BELIEF SHAPING IN NONCOOPERATIVE COMMUNICATION AND CONTROL SYSTEMS THROUGH STRATEGIC SIGNALING

BY

MUHAMMED O. SAYIN

DISSERTATION

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Electrical and Computer Engineering
in the Graduate College of the
University of Illinois at Urbana-Champaign, 2019

Urbana, Illinois

Doctoral Committee:

Professor Tamer Başar, Chair
Professor Bruce Hajek
Associate Professor Cedric Langbort
Professor Venugopal V. Veeravalli

ABSTRACT

In this dissertation, we analyze the interaction between intelligent and selfish agents in non-cooperative environments with a specific focus on the transmission of some private information among them. We seek to quantify the ability of informed agents to shape the uninformed (rational) agents' beliefs about the private information through signals crafted strategically even when the uninformed agents construct their beliefs with awareness of how the messages were crafted. Through the quantification of this ability, our goal is to introduce strategic information transmission to applications in cyber and cyber-physical systems as a deception-as-defense mode of operation. It is worth noting that transparency in the signals sent provides robustness against advanced adversaries that can learn/discover the signaling strategy. Due to the versatility of the Gaussian distribution, we first formulate derivation of the optimal signaling strategies for Gauss Markov information in dynamic communication settings. We formulate an equivalent semi-definite program instead of addressing this problem over the original infinite-dimensional strategy spaces. We show that the optimal signaling strategies are linear within the general class of measurable policies when the agents have different quadratic cost measures. This formulation brings in the possibility of adopting strategic information transmission in dynamic control systems based on the common theme of communication and control settings. In this context, we introduce a robust sensor design framework and compute the associated sensor outputs to provide resiliency in linear-quadratic-Gaussian control systems against advanced attackers with malicious and unknown control objectives. In order to extend these results to distributions other than Gaussian, we have address the problem of optimal hierarchical signaling for a general class of square integrable multivariate distributions. Again instead of addressing the problem directly over the original strategy spaces, we have formulated an equivalent linear optimization problem over the cone of completely positive matrices when the underlying state space is finite. The ability to compute the optimal signaling strategies for large finite state spaces enables us to address the signaling problem approximately also for continuous distributions. We also provide analytical guarantees on the level of accuracy for the approximation. Finally, we discuss some of the future research directions on belief shaping through strategic signaling.

To my beloved family and wife, for their love and support.

ACKNOWLEDGMENTS

I was very fortunate to be advised by Professor Tamer Başar during my Ph.D. studies. It is my great pleasure to thank him for his prompt and continued support. His strong work ethic and unlimited excitement for impactful research will continue to guide me throughout my academic life. My gratitude extends also to the other members of my dissertation committee: Professor Bruce Hajek, Professor Cedric Langbort, and Professor Venugopal Veeravalli.

I am very grateful to have a chance to conduct research in such a friendly, respectful, and stress-free environment. Special thanks to all of my fellow group mates Khaled, Aneeq, Kaiqing, Erik, and Angie.

I also would like to express my gratitude to Professor Suleyman S. Kozat, my Master's thesis advisor at Bilkent University, who introduced me to the beauty of the academic research environment.

Last but not least, I would like to thank my family and beloved wife for their continuous support.

The research in this dissertation 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.

TABLE OF CONTENTS

1

INTRODUCTION AND MOTIVATION

> *The triumph of persuasion over force is the sign of a civilized society.*
>
> – Mark Skousen

Around five centuries ago, discovery of ignorance, i.e., believing that no one can know everything that is important, was a breaking point for scientific research, and as a result today's technological wisdom has arisen [1]. There is always an entire world of important information to be discovered. However, only some could have access to (or discover) new important information, e.g., based on their effort, while there will be others who would desperately need this information in order to improve their decisions. Axiomatically, there will always be someone who knows what we do not know (yet relevant to important for us), and vice versa. This inevitable distributed nature of information and its substantial *importance* can lead to *manipulation* of the decisions by the information providers.

Human history is full of such manipulations: Authorities holding the will of certain ideologies or religions (we can consider them as the information providers) could have controlled masses even to the extent of wasting their own lives *willingly* [1]. The key distinction is the willingness in their actions rather than them being controlled by force since the masses had perceived the engineered phenomenon as the absolute truth by heart. However, the issue is still not over in today's world. Indeed, it is far more prevailing because of the tremendous amount of information that is available out there, and the world is as tightly networked as ever. Some scholars even view today as the era of big data [2]. And we are developing trust in the power of informed decisions more and more as we are always observing its repeatedly proven empirical effectiveness. However, this trust makes the informed decisions vulnerable against manipulations, e.g., deception.

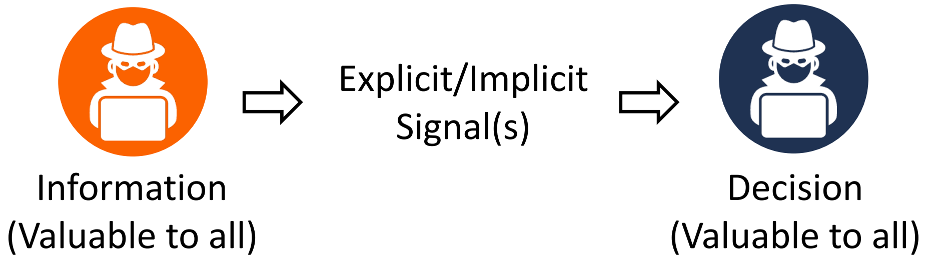


Figure 1.1: The interaction between an information provider and a decision maker through explicit or implicit signal(s) while the information and the decision are valuable to both.

There are various definitions of deception. Depending on the specific definition at hand, the analysis or the related applications vary.

Definition. We say that an informed agent (or the signal the agent crafts) is **deceptive** if he/she shapes that information of interest private to him/her strategically in order to control the perception of the uninformed agents toward his/her own benefit by *removing*, *changing*, or *adding content*.

Indeed, our ability to infer information from correlated phenomena enables us to generalize this signaling model to settings where there is no explicit signaling or physical messages, but we can still infer certain information based on observed actions.

Definition. We say that an action taker (or the associated action) is **deceptive** if he/she takes the actions strategically to control the others' inference about information of interest private to him/her in the direction of his/her own benefit.

In either case, the information should have value for both sides so that the informed agent could deceive the other agent(s), and the decisions should be valuable to both sides so that the informed agent could have incentive to manipulate the decisions. Figure 1.1 provides an illustration of the strategic information flow between informed and uninformed agents.

In noncooperative environments with asymmetry of information, the interaction between informed and uninformed agents can turn into a game where the agents select their strategies according to their selfish objectives while taking into account the fact that the other agent would also have selected his/her strategy[1] according to his/her selfish, possibly different, objective.

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

Correspondingly, such an interaction between the informed and uninformed agents can be analyzed under a game-theoretic solution concept. Note that there is a main distinction between incentive compatible deception model and deception model with policy commitment.

Definition. We say that a deception model is **incentive compatible** if neither the informed nor the uninformed agent(s) have any incentive to deviate from their strategies unilaterally.

The associated solution concept here is the Nash equilibrium [3]. Existence of a Nash equilibrium is not guaranteed in general. Furthermore, even if it exists, there may be multiple Nash equilibria. Without certain commitments, none of the equilibria may actually be realized or in case one has been realized, it is not a priori certain as to which of the multiple equilibria was the one realized, since different ones could be favorable to different players.

Definition. We say that in a deception model, there is **policy commitment** if either the informed agent or the uninformed agent commits to play a certain strategy beforehand and the other agent reacts to it, being aware of the committed strategy.

The associated solution concept is the Stackelberg equilibrium, where one of the players leads the game by announcing his/her committed strategy [3]. Existence of a Stackelberg equilibrium is not guaranteed in general, e.g., over non-compact strategy spaces. However, if it exists, all the equilibria would lead to the same game outcome for the leader of the game since the leader could have always selected the favorable one among them. We also note that if there is a favorable outcome for the leader in the incentive compatible model, the leader has the freedom to commit to that policy in the latter model. Correspondingly, the leader would be at an advantage by acting first to commit to play according to a certain strategy even though the result may not be incentive compatible.

Game theoretical analysis of deception has attracted substantial interest in various disciplines, including economics and engineering fields. In the following subsections, we review the literature in these disciplines with respect to deception models involving incentive compatibility and policy commitment.

1.1 Economics Literature

The scheme of the type introduced above, called strategic information transmission, was introduced in a seminal paper [4] by V. Crawford and J. Sobel. This paper has attracted substantial attention due to the wide range of relevant applications from economics and political science to philosophy and biology. J. Sobel surveys these applications across various disciplines in [5]. In the model adopted in [4], there are two agents, and the informed agent's objective function includes a commonly known (deterministic) bias term different from the uninformed agent's objective. That bias term can be viewed as the misalignment factor in-between the two objectives. For the incentive compatible model, the authors have shown that all equilibria are partition equilibria, where the informed agent controls the resolution of the information shared via certain quantization schemes, under certain assumptions on the objective functions (satisfied by quadratic objectives), and the assumption that the information of interest is drawn from a distribution with bounded support.

Following this inaugural introduction of the strategic information transmission framework, also called *cheap talk* due to the costless communication over an ideal channel, different settings, have been studied extensively such as

- Single sender and multiple receivers [6, 7]
- Multiple senders and single receiver [8–10]
- Repeated games [11]
- Multidimensional information [10]
- Unbounded state and lying cost [12]
- Certifiable information [13]
- Dynamic information transmission over finite horizon [14]

Different from the original setting in [4], some of these settings, e.g., [10, 12–14], could lead to full revelation of the information at an equilibrium. In [10], the author has shown that when there are multiple senders, the receiver could exploit the aligned part of different senders to recover the underlying information fully. Similarly, when the state is multidimensional, the receiver can ensure that even a single sender shares the information truthfully at certain dimensions in an equilibrium [10]. Furthermore, truthful information revelation could also be observed at an equilibrium when the sender faces a cost of lying, which can grow unboundedly as shown in [12]; when the certifiable information makes the messages state-contingent as shown in [13]; and when the dynamic interactions of the players align their incentives together as shown in [14].

More recently, in [15], the authors have proposed to use a deception model with policy commitment, called "Bayesian persuasion". Different from the setting in [4], here the sender cannot distort or conceal information once the signal realization is known, which can be viewed as the sender revealing and committing to the signaling rule in addition to the corresponding signal realization. For information of interest drawn from a compact metric space, the authors have provided necessary and sufficient conditions for the existence of a strategic signal that can benefit the informed agent, and characterized the corresponding optimal signaling rule through a geometrical interpretation.

Following the introduction of Bayesian persuasion, the problem has been analyzed under various settings, such as

- Multiple senders and single receiver [16, 17]
- Single sender and multiple receivers [18]
- Dynamic environments [19]
- Costly persuasion [20]

A detailed review of these studies could be found in the survey [21]. Furthermore, in [22], the author has shown the optimality of linear signaling rules for multivariate Gaussian information of interest and with quadratic objective functions.

1.2 Engineering Literature

There exist various engineering applications depending on the definition of deception. Reference [23] provides a taxonomy of these studies with a specific focus on security. Obfuscation techniques to hide valuable information, e.g., via externally introduced noise [24–26] can also be viewed as deception based defense. As an example, in [24], the authors have provided a browser extension that can obfuscate a user's real queries by including automatically fabricated queries to preserve privacy. Here, however, we specifically focus on signaling-based deception applications, in which we craft the information available to adversaries to control their perception rather than corrupting it. In line with the browser extension example, our goal is to persuade the query trackers to perceive the user behavior in a certain fabricated way rather than limiting their ability to learn the actual user behavior.

In computer security, various (heuristic) deception techniques, e.g., honeypots and honey nets, are prevalent to make the adversary perceive a honey-system as the real one or a real system as a honey-one [27]. Several studies, e.g., [28], have analyzed honeypots within the framework of binary signaling games by abstracting the complexity of crafting a real system to be perceived as a honeypot (or crafting a honeypot to be perceived as a real system) to binary signals. However, here, our goal is to address the optimal way to craft the underlying information of interest with a continuum support, e.g., a Gaussian state.

The recent study [29] addresses strategic information transmission of multivariate Gaussian information over an additive Gaussian noise channel for quadratic misaligned cost functions and identifies the conditions where the signaling rule attaining a Nash equilibrium can be a linear function. Recall that for the scalar case, when there is no noisy channel in-between, all the equilibria are partition equilibria, implying that all the signaling rules attaining a Nash equilibrium are nonlinear except babbling equilibrium, where the informed agent discloses no information [4]. Two other recent studies [30] and [31] address strategic information transmission for the scenarios where the bias term is not common knowledge of the players and the solution concept is Stackelberg equilibrium rather than Nash equilibrium. They have shown that the Stackelberg equilibrium could be attained by linear signaling rules under certain conditions, different from the partition equilibria in the incentive compatible cheap talk model [4]. In [31], the authors have studied strategic sensor networks for multivariate Gaussian information of interest and with myopic quadratic objective functions in dynamic environments and by restricting the receiver's strategies to affine functions. In [30], for jointly Gaussian scalar private information and bias variable, the authors have shown that optimal sender strategies are linear functions within the general class of measurable policies for misaligned quadratic cost functions when there is an additive Gaussian noise channel and hard power constraint on the signal, i.e., when it is no longer cheap talk.

Although strategic signaling has attracted significant attention in various fields due to its compelling applications in noncooperative multi-agent environments, we still have important but not yet explored problems. In this dissertation, we seek to address some of these issues within the theme of deception and security with a specific application point of view in cyber and cyber-physical systems. We specifically seek to introduce strategic information transmission to cyber or cyber-physical systems as a deception-as-defense mode of operation, explained below. Particularly, strategic information transmission can play a key role in multi-agent non-cooperative environments as well as in cooperative ones, where certain (uninformed) agents could have been compromised by certain adversaries. In such scenarios, informed agents can signal strategically to the uninformed ones in case they could have been compromised. Furthermore, deceiving an adversary to act, or attack the system in a way aligned with the system's goals can be viewed as being too optimistic due to the very definition of adversary. However, an adversary can also be viewed as a selfish decision maker seeking to satisfy a certain malicious objective, which may not necessarily be completely conflicting with the system's objective. This now leads to the following notion of "deception-as-defense".

Definition. We say that an informed agent engages in a **deception-as-defense** mode of operation if he/she crafts the information of interest strategically before sharing with an uninformed (malicious) agent in order to persuade him/her (without any explicit enforcement) to act in line with the aligned part of the objective as much as possible without taking into account the misaligned part.

We re-emphasize that this approach differs from the approaches that seek to raise suspicion on the information of interest to sabotage the adversaries' malicious objectives. Sabotaging the adversaries' malicious objectives may not necessarily be the best option for the informed agent unless the objectives are completely opposite of each other. In this latter case, the deception-as-defense framework actually ends up seeking to sabotage the adversaries' malicious objectives.

We also note that this approach differs from lying, i.e., the scenario where the informed agent provides totally different information (correlated or not) *as if* it is the information of interest. Lying could be effective, as expected, as long as the uninformed agent trusts the legitimacy of the information provided. However, in non-cooperative environments, this could turn into a game where the uninformed agent becomes aware of the possibility of lying. This correspondingly raises suspicion on the legitimacy of the shared information and could end up sabotaging the adversaries' malicious objectives rather than controlling their perception of the information of interest.

Once a defense mechanism has been widely deployed, this can cause the advanced adversaries to learn the defense policy in the course of time. Correspondingly, the solution concept of policy commitment model can address this possibility in the deception-as-defense framework in a robust way if the defender commits to a certain policy that takes into account the best reaction of the adversaries that are aware of the policy. Furthermore, the transparency of the signal sent via the committed policy generates a trust-based relationship in-between the sender and the receiver, which is powerful to persuade the receiver to make certain decisions inadvertently without any explicit enforcement by the sender. Therefore, we focus on deception models with policy commitment. We call it hierarchical signaling in order to distinguish it from the general setting of strategic information transmission.

Due to the versatility of the Gaussian distribution in engineering applications, we mostly address (multivariate) Gaussian signaling under various scenarios:

- Dynamic environments over finite or infinite horizon [32–36]
- Noisy environments [37, 38]
- Linear-quadratic-Gaussian (LQG) control [34, 38–41]
- Single sender and multiple receivers [38]

Reference [42] provides an overview of these results. Furthermore, we have also addressed the problem of optimal hierarchical signaling for a general class of distributions in [43] under static settings, and in [36] under dynamic settings with, however, the receiver restricted to using linear estimates. In this dissertation, we provide an overview of these contributions with a specific focus on dynamic Gaussian signaling, robust sensor design, and signaling for general distributions.

1.3 Dynamic Gaussian Signaling

In [22], the author has shown the optimality of linear signaling strategies within the general class of measurable policies in an analytical form for multivariate Gaussian distributions over a single-stage information flow. Its extension to multi-stage information flow necessitates balancing the trade-off between deceiving at a current stage and preserving the capacity to deceive at future stages when the receiver has perfect recall. Furthermore, such an extension could bring the strategic information transmission into the framework of dynamic control systems. To this end, we seek to address dynamic Gaussian signaling under various scenarios, including signaling over finite or infinite horizon, signaling of degenerate Gaussian information, and signaling with noisy or partial measurements.

Over a finite horizon, for a discrete-time Gauss-Markov process, and when the sender and the receiver have misaligned quadratic objectives, in [34], we have shown the optimality of linear signaling rules within the general class of measurable policies and provided a semi-definite program (SDP) to compute the optimal policies numerically. Also in [34], we have formulated the optimal linear signaling rule in a non-cooperative LQG control setting when the sensor and the controller have known misaligned control objectives. In [35], we have shown the optimality of linear signaling in the settings where the underlying Gaussian distribution is degenerate. Furthermore, in [36], we have shown that there exists a solution if the players have discounted quadratic cost measures over infinite horizon and formulated the linear signaling rules that can lead to optimal performance for the sender approximately with any desired level of accuracy. For Gaussian information, under the restriction that the sender can use linear-plus-noise signaling strategies only, we have also formulated the optimal signaling strategies in the settings where there exists an additive Gaussian noise channel [37] and the sender has access to a noisy version of the underlying information [38].

1.4 Robust Sensor Design

As a deception-as-defense mode of operation in cyber-physical systems, we seek to restrain the actions of the attackers (with control objectives) by controlling their perceptions about the underlying state. To this end, we can use the asymmetry of information in favor of resiliency, and design the sensor outputs strategically against the possibility of undetected attacks on the system. In [39] and in the ensuing studies [40, 41], we have introduced the secure sensor design framework, where we have addressed the optimal linear signaling rule again in a non-cooperative LQG setting when the sensor and private-type controller have misaligned control objectives in a Bayesian setting, i.e., the distribution over the private type of the controller is known. In [38], we have addressed optimal linear robust signaling in a non-Bayesian setting, where the distribution over the private type of the controller is not known, and provided a comprehensive formulation by considering also the cases where the sensor could have partial or noisy information on the signal of interest and relevance.

1.5 Signaling for General Distributions

Within the hierarchical signaling framework, optimal signaling strategy has been formulated in [22] for Gaussian distributions. In [15], the authors have developed a geometrical interpretation to address the problem for distributions over finite state spaces with fairly small sizes. For larger state spaces, they have characterized the specific settings where we can deduce whether the sender can benefit via strategic signaling or not. However, its computation for general settings, e.g., for relatively large state spaces, has remained open. Therefore, in this dissertation, we have sought to address the problem of optimal hierarchical signaling for a general class of multivariate square integrable distributions.

In [36], we have shown that all the results obtained for Gaussian, e.g., optimality of linear signaling within the general class of measurable policies, hold also for distributions other than Gaussian if the receiver has bounded rationality by using linear estimates only. However, if the receiver is (unboundedly) rational, the problem is much more challenging. To address it, in [43], we have first addressed the problem for finite state spaces by formulating an equivalent linear optimization problem over the cone of completely positive matrices. Even though the equivalent problem and its dual turn out to be not tractable because of the difficulty the convex cones present, the equivalence established has enabled us to use the existing computational tools to solve this class of cone programs approximately with any desired level of accuracy. Furthermore, for continuous distributions, we have obtained theoretical guarantees on the approximation level of the proposed solution concept when it is applied to a discretized version of the underlying information, e.g., through a given quantization scheme.

1.6 Organization

We organize the dissertation as follows. In Chapter 2, we analyze how a deceptive information provider can shape Gauss-Markov information in order to control a decision maker's perception in dynamic environments. In Chapter 3, we introduce a deception-as-defense mode of operation for linear-quadratic-Gaussian systems, to enhance their resiliency against multiple attackers with misaligned control objectives. In Chapter 4, we address the problem of optimal hierarchical signaling for a general class of distributions. Chapter 5 summarizes the contributions of the dissertation and discusses future research directions in the topical areas covered by the dissertation. Appendices A-C provide technical proofs for Chapters 2-4.

1.7 Notation

For an ordered set of parameters, e.g., $x_1, \dots, x_n$, we define $x_{k:l} \coloneqq x_k, \dots, x_l$, where $1 \leq k \leq l \leq n$. For a vector x and a matrix A, x' and A' denote their transposes; further $\|x\|$ and $\|A\|_2$ denote the Euclidean (L^2) norms of the vector x and the matrix A, respectively. For a matrix A, $\mathrm{Tr}\{A\}$ denotes its trace. We denote the identity and zero matrices with the associated dimensions by I and O, respectively. $A \otimes B$ denotes the Kronecker product of the matrices A and B.

For positive semi-definite matrices A and B, $A \geq B$ means that $A-B$ is also a positive semi-definite matrix. $\mathbb{S}^m$ (or $\mathbb{S}^m_+$) denotes the set of symmetric (or positive semi-definite) matrices of dimensions m-by-m while $\mathbb{R}^{n\times m}_+$ (or $\mathbb{R}^{n\times m}_{++}$) denotes the set of n-by-m matrices with non-negative (or positive) entries.

We denote random variables by bold lowercase letters, e.g., $\boldsymbol{x}$. For a random variable $\boldsymbol{x}$, $\hat{\boldsymbol{x}}$ is another random variable corresponding to its posterior belief conditioned on certain random variables that will be apparent from the context. For a random vector, e.g., $\boldsymbol{x}$, $\mathrm{cov}\{\boldsymbol{x}\}$ denotes the corresponding covariance matrix. $\mathcal{N}(0,.)$ denotes the multivariate Gaussian distribution with zero mean and designated covariance.

2

DYNAMIC GAUSSIAN SIGNALING

Half a truth is often a great lie.

– Benjamin Franklin

In[1] the era of smart devices, we have various systems having enhanced processing and efficient communication capabilities. Even though information exchange is generally useful in cooperative multi-agent networks, where each agent has the same goal, such as in consensus networks, diversification in smart systems brings about inevitable mismatches in the objectives of different agents. This then leads to noncooperative game formulations for smart systems in the disclosure of information [4, 22, 30, 44]. As an example, a trajectory controller can drive a tracking system to a desired path, different from the tracker's actual intent, by controlling the disclosed information [33].

To this end, consider the scenario of a sender ($\mathcal{P}_S$) having access to some information and a receiver ($\mathcal{P}_R$) needing this information to be able to take a particular action, impacting both $\mathcal{P}_S$ and $\mathcal{P}_R$. In the classical communication setting, $\mathcal{P}_S$ seeks to transmit this information in the best possible way, leading to a full cooperation between him/her and $\mathcal{P}_R$, toward mitigating the channel's impact on the transmitted signals. However, even if there exists an ideal (perfect) channel between $\mathcal{P}_S$ and $\mathcal{P}_R$, if their objectives differ, absolute transparency of the disclosed information is not a reasonable action for $\mathcal{P}_S$ in general [4, 22, 30, 44]. In a hierarchical game, also known as Stackelberg game, [3], $\mathcal{P}_R$ reacts after $\mathcal{P}_S$'s disclosure of information. Therefore, in strategic settings, where objectives differ, $\mathcal{P}_S$ develops strategies to control the transparency of the disclosed information. Originally, a scheme of this type, called strategic information transmission, was introduced in a seminal paper by V. Crawford and J. Sobel [4], and attracted substantial attention in

[1] We acknowledge that the content of this chapter appears in [34] and the copyright owner has provided permission for reprint.

the economics and engineering literatures due to the wide range of relevant applications.

Recently, strategic information transmission in hierarchical signaling games (where there is a hierarchy in the announcement of the strategies) has attracted substantial interest in various disciplines, including control theory [31, 33, 45], information theory [30, 46], and economics [15, 22]. In [31], the authors have studied strategic sensor networks for Gaussian variables and with myopic quadratic objective functions, i.e., the players construct strategies just for the current stage irrespective of the length of the horizon, by restricting the receiver strategies to affine functions. Reference [33] has addressed the optimality of linear sender strategies within the general class of policies for myopic quadratic objectives. In [29, 45], the authors have shown that for scalar parameters, quadratic cost functions, and a commonly known bias parameter, the hierarchical game formulation can be converted into a team problem. Reference [30] has shown that linear sender strategies achieve the equilibrium within the general class of policies even with additive Gaussian noise channels. In [22], the author has demonstrated the optimality of linear sender strategies also for the multivariate Gaussian information, and with quadratic cost functions. In [15], the authors have provided a geometrical interpretation of the optimal signaling strategies for general information parameters.

In addition to the mismatched objectives in a communication system, the signaling game setting can also be considered as a dynamic deception game [47–49], where a player aims to deceive the other player, say victim, such that the victim's perception about an underlying phenomenon and correspondingly the victim's reaction is controlled in a desirable way. Hence, this approach brings about new security and resilience applications for cyber-physical systems that are vulnerable to cyber attacks, e.g., power grids, transportation systems, and cloud networks [50–52]. In particular, turning the problem around, new defense mechanisms can be developed aiming to arouse attackers' suspicion on compromised information or to deceive attackers to take certain actions. Additionally, the resulting scheme would be advantageous to the defender, i.e., sender in the strategic communication scheme, in terms of his/her objectives due to the hierarchical structure, and therefore would be more preferable for security related scenarios.

A recent Verizon Data Breach Investigation Report (DBIR) [53] shows that millions of people have been affected by and a substantial amount of financial loss has occurred due to cyber attacks. Furthermore, many of the attacks are either unreported or not yet discovered by the victim. Importantly, in 93% of the attacks, the attackers can infiltrate into the system within minutes and even seconds, and in 68% of the attacks the attackers exfiltrate the system within days [53]. Therefore, if attackers succeed in infiltrating into the system, an additional layer of defense based on dynamic deception can play a vital role for the security of the system [54]. The experiment conducted in blue (defender) and red (attacker) teams from Lockheed Martin [55] is an illustrative example of the effectiveness of deception strategies even when the confidential information has been compromised.

Now, coming to the specifics of this chapter, we obtain here equilibrium achieving sender strategies in hierarchical (i.e., Stackelberg [3]) multi-stage signaling games with finite horizon, where hierarchically $\mathcal{P}_S$ is the leader such that his/her strategies are known by (and enforced on) $\mathcal{P}_R$. We show that memoryless linear sender strategies and linear receiver strategies can yield multi-stage equilibrium with finite horizon for general quadratic objective functions and multivariate Gaussian processes evolving according to first-order auto-regressive models. This extends the result for the optimality of linear strategies shown in [22] to dynamic settings. We point out that in the dynamic settings, in addition to the mismatches between the objectives, $\mathcal{P}_S$ should also control the transparency of the disclosed information due to impact of the actions on future stages. At each stage, $\mathcal{P}_S$ faces a trade-off in terms of the current stage and all other future stages of the game while controlling the transparency of the disclosed information, and should develop strategies in a comprehensive manner over the horizon.

After obtaining equilibrium achieving policies in the multi-stage strategic communication game, we extend the results to noncooperative strategic control, where sensor and controller of a dynamic system have different objectives. As an example, the controller aims to drive the system to a desired path based on the sensor outputs, while the sensor designs the sensor outputs to deceive the controller so that the system is driven to a path different from the controller's actual intent. Such a scheme can have important applications in resilience of cyber-physical systems under adversarial attacks. Even though attackers have infiltrated into the controller and gained access to control the system, the damage could be minimized via the strategic sensor outputs. Furthermore, the sensors of the system could also be infiltrated into by the attackers, which can annihilate the proposed defense mechanism via a shortcut to the state realization if the sensors's policies could be controlled remotely. In order to mitigate that, we consider the scenario where the sensor's signaling rules are *selected beforehand* to minimize the expected loss and *fixed* (can be time-variant, yet not controlled) during the operation. We provide an algorithm to compute the optimal linear sensor signaling rules for Gauss-Markov processes controlled by the controller with any measurable control rule[2] numerically with global optimality guarantees.

Particularly, the proposed formulation can be considered as a passive defense strategy that can be incorporated along with active defense strategies [54]. Consider the scenarios, where infiltration detection mechanisms (an active defense mechanism) have detected adversarial infiltration into the controller of the cyber-physical system and characterized the control objective of the adversary. And there is certain necessary time before disabling the access of the attacker to the controller. For that time interval, which can be considered as the time horizon in our formulation, the system can switch to the proposed passive defense mode, where the sensor outputs have been constructed to minimize the damage due to the attack. We emphasize that no information will be shared with the attacker except the sensor's outputs (which can also be non-informative). Importantly, *the defender will not provide his/her strategy as to how the sensor's outputs are constructed to the attacker.* However, the problem still can be considered as a Stackelberg game, where the sensor is the leader, because this is a passive defense mechanism that does not depend on the actual realizations, i.e., the sensor seeks to minimize the expected cost, and the attacker, having access to the system, can be aware of the switch to this passive defense mode and correspondingly can know how the sensor outputs will have been constructed.

The main contributions and conclusions of this chapter are as follows:

- We study dynamic hierarchical Gaussian signaling games with finite horizon for general quadratic cost functions and general class of measurable policies.

- We formulate a functional minimization problem whose solutions correspond to the equilibrium achieving signaling rules, and we characterize

[2] For linear signaling rules, the optimal control rules are also linear [56].

the solutions through a finite dimensional optimization problem bounding the original problem from below.

- We show that *linear* sender and receiver signaling rules can yield the equilibrium for arbitrary (finitely many) number of stages within the general class of measurable policies.

- We show that in multi-stage case, the sub-games at each-stage are not decoupled and cannot be considered as single-stage games, where the innovation part of the state is to be disclosed.

- We geometrically observe that linear strategies for Gaussian information can achieve the equilibrium within the general class of measurable policies because uncorrelatedness implies independence.

- Correspondingly, the proposed method, to characterize the solution via lower bound, may not compute the optimal strategies for arbitrary distributions in general unless, e.g., the receivers' strategies are restricted to linear functions.

- We also argue that Gaussian distribution is the *best* distribution serving the deceptive sender's objectives.

- We extend the results to controlled Gauss-Markov processes and provide an algorithm to compute optimal linear sensor strategies numerically with global optimality guarantees in noncooperative control scenarios.

The chapter is organized as follows: In Section 2.1, we provide the problem description. In Section 2.2, we introduce and analyze strategic communication scenario, and we provide the equilibrium achieving policies in Section 2.3. In Section 2.4, we highlight intriguing properties of hierarchical signaling games. We analyze strategic communication in noncooperative control scenarios in Section 2.5. We provide numerical examples for different noncooperative communication and control scenarios in Section 2.6. We conclude the chapter in Section 2.7 with several remarks.

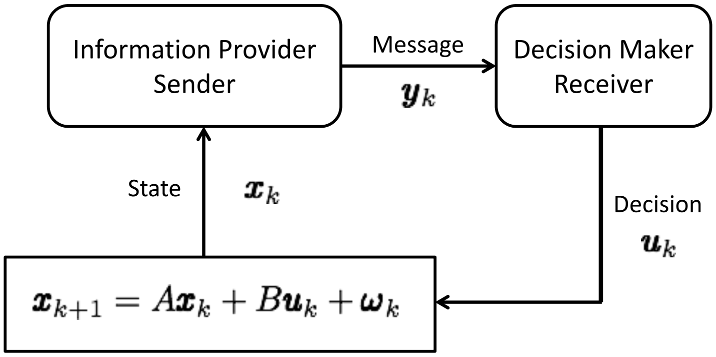


Figure 2.1: multi-stage signaling game model.

2.1 Problem Formulation

Consider a controlled stochastic system described by the following state equation[3]:

$$\boldsymbol{x}_{k+1} = A\boldsymbol{x}_k + B\boldsymbol{u}_k + \boldsymbol{w}_k, \tag{2.1}$$

for $k = 1, \ldots, n$, where[4] $A \in \mathbb{R}^{p \times p}$, $B \in \mathbb{R}^{p \times t}$, $\boldsymbol{x}_1 \sim \mathcal{N}(0, \Sigma_1)$. The additive noise process $\{\boldsymbol{w}_k\}$ is a white Gaussian vector process, e.g., $\boldsymbol{w}_k \sim \mathcal{N}(0, \Sigma_w)$, and is independent of the initial state $\boldsymbol{x}_1$. The closed-loop control vector $\boldsymbol{u}_k \in \mathbb{R}^t$ is given by

$$\boldsymbol{u}_k = \gamma_k(\boldsymbol{y}_{[1,k]}), \tag{2.2}$$

where $\gamma_k(\cdot)$ is a Borel measurable function from $\mathbb{R}^{pk}$ to $\mathbb{R}^t$. The message signal $\boldsymbol{y}_k \in \mathbb{R}^p$ is given by

$$\boldsymbol{y}_k = \eta_k(\boldsymbol{x}_{1:k}), \tag{2.3}$$

where $\eta_k(\cdot)$ is a Borel measurable function from $\mathbb{R}^{pk}$ to $\mathbb{R}^p$. We assume that the auto-covariance matrices Σ_1 and Σ_w are all positive definite.

As seen in Fig. 2.1, we have two agents: Sender ($\mathcal{P}_S$) and Receiver ($\mathcal{P}_R$), who select signaling rules under different objectives. For stage k, $\mathcal{P}_S$ selects the signaling rule $\eta_k(\cdot)$ from the policy space Ω_k, which is the set of all Borel measurable functions from $\mathbb{R}^{kp}$ to $\mathbb{R}^p$, i.e., $\eta_k \in \Omega_k$, such that $\boldsymbol{y}_k = \eta_k(\boldsymbol{x}_{1:k})$ almost everywhere over $\mathbb{R}^p$. On the other side, $\mathcal{P}_R$ selects the signaling rule

[3] The provided derivations can be extended to time-variant cases rather routinely. And the derivations can also be extended to the non-zero mean case in a straightforward way.

[4] We assume that the matrix A is non-singular.

$\gamma_k(\cdot)$ from the policy space Γ_k, which is the set of all Borel measurable functions from $\mathbb{R}^{kp}$ to $\mathbb{R}^t$, i.e., $\gamma_k \in \Gamma_k$, such that $\boldsymbol{u}_k = \gamma_k(\boldsymbol{y}_{1:k})$ almost everywhere over $\mathbb{R}^t$. $\mathcal{P}_S$ and $\mathcal{P}_R$ have different quadratic finite horizon cost functions[5] $J_S(\eta_{1:n}, \gamma_{1:n})$ and $J_R(\eta_{1:n}, \gamma_{1:n})$, respectively, while each signaling rule implicitly depends on the other. In the following, we introduce a hierarchical equilibrium concept for the signaling rules with respect to these cost functions, J_S and J_R. Particularly, we consider the situation where there is a hierarchy between the agents in the announcement of the policies such that $\mathcal{P}_S$ leads the game by announcing and sticking to his/her policies beforehand and $\mathcal{P}_R$ reacts to those policies accordingly. We can model such a scheme as a Stackelberg game between the players [3] such that the leader, i.e., $\mathcal{P}_S$, chooses his signaling rule based on the corresponding best response of the follower, i.e., $\mathcal{P}_R$.

Due to the hierarchy, $\mathcal{P}_R$'s signaling rule γ_k can depend on $\mathcal{P}_S$'s signaling rules $\eta_{1:k}$. In order to explicitly show the dependence on $\mathcal{P}_S$'s policies, henceforth, we denote $\mathcal{P}_R$'s policies by[6] $\gamma_k(\eta_{1:k})$, i.e., $\gamma_k(\eta_{1:k})(\boldsymbol{y}_k) := \gamma_k(\boldsymbol{y}_{1:k})$. Then, for each n-tuple of policies $\eta_k \in \Omega_k$, $k = 1, \ldots, n$, we let $\Pi_R(\eta_{[1,n]})$ be the reaction set of $\mathcal{P}_R$, as a subset of $\times_{k=1}^{n} \Gamma_k$. For finite-horizon objectives, we have

$$\Pi_R(\eta_{[1,n]}) := \arg \min_{\substack{\gamma_k \in \Gamma_k,\\ k=1,\ldots,n}} J_R(\eta_{1:n}; \gamma_{1:n}(\eta_{1:n})),$$

where $\gamma_{1:n}(\eta_{1:n}) := \{\gamma_1(\eta_1), \ldots, \gamma_n(\eta_{1:n})\}$. In the following sections, when we provide the objective functions for the associated scenarios explicitly, we will also show that Π_R is an equivalence class such that all $\gamma_{1:n}^* \in \Pi_R$ lead to the same random variable $\boldsymbol{u}_k^*$ almost surely under certain convexity assumptions. Therefore, the pair of signaling rules $(\eta_{1:n}^*, \gamma_{1:n}^*)$ attains the multi-stage Stackelberg equilibrium provided that

$$\eta_{1:n}^* = \arg \min_{\substack{\eta_k \in \Omega_k,\\ k=1,\ldots,n}} J_S\big(\eta_{1:n}; \gamma_{1:n}^*(\eta_{1:n})\big), \tag{2.4a}$$

$$\gamma_{1:n}^*(\eta_{1:n}) = \arg \min_{\substack{\gamma_k \in \Gamma_k,\\ k=1,\ldots,n}} J_R(\eta_{1:n}; \gamma_{1:n}(\eta_{1:n})). \tag{2.4b}$$

Remark. We note that the hierarchical equilibrium (2.4) implies that $\mathcal{P}_S$'s

[5] We provide these functions explicitly in the following sections in noncooperative communication and control scenarios.

[6] Without loss of generality, we can also consider that $\gamma_k(\eta_{1:n}) = \gamma_k(\eta_{1:k})$.

signaling rules do not depend on the realizations of the random variables and all of them can be selected beforehand since they also do not depend on $\mathcal{P}_R$'s signaling rules. Such an equilibrium formulation, where $\mathcal{P}_S$ strategies do not depend on the actual realizations, i.e., where $\mathcal{P}_S$ does not have access to the realizations, is essential for the cyber-security related applications in order to avoid shortcuts that can cancel the proposed defense mechanism once the attacker also infiltrates into $\mathcal{P}_S$. Furthermore, $\mathcal{P}_S$ should anticipate $\mathcal{P}_R$'s reaction to any selected strategy since even if $\mathcal{P}_S$ might have incentive to come up with another policy based on $\mathcal{P}_R$'s policy, any change in $\mathcal{P}_S$'s policy would also imply a change in $\mathcal{P}_R$'s policy accordingly due to the hierarchy.

In the following sections, we analyze the equilibrium achieving signaling rules in noncooperative communication and control scenarios.

2.2 Dynamic Gaussian Signaling in Communication Systems

Here, we consider a strategic communication scenario, which is a special case of (2.1), where $B = O$ such that state $\{\boldsymbol{x}_k\}$ is an exogenous process rather than a controlled process. Following this, we use the results obtained to characterize the equilibrium achieving linear signaling rules for the original case (2.1), i.e., in a noncooperative control scenario. The underlying state, now, is a Markov process (not necessarily stationary) evolving according to first-order auto-regressive model:

$$\boldsymbol{x}_{k+1} = A\boldsymbol{x}_k + \boldsymbol{w}_k, \quad k = 1, \dots, n \tag{2.5}$$

and at stage-k, state $\boldsymbol{x}_k$ is a zero-mean Gaussian random vector with auto-covariance matrix Σ_k, which is given by the following recursion: $\Sigma_k = A\Sigma_{k-1}A' + \Sigma_w$ for $k = 2, \dots, n$. Note that if $\mathcal{P}_S$ and $\mathcal{P}_R$ have the same cost functions, the best signaling rule of $\mathcal{P}_S$ can be direct information disclosure, i.e., $\eta_k(\boldsymbol{x}_{1:k}) = \boldsymbol{x}_k$ almost everywhere over $\mathbb{R}^p$, since there is a perfect channel between the agents. However, when $\mathcal{P}_S$ and $\mathcal{P}_R$'s cost functions are different, direct information disclosure may not be in $\mathcal{P}_S$'s best interest.

Consider the situation where $\mathcal{P}_S$ and $\mathcal{P}_R$ have the following quadratic finite horizon cost functions, for $j = S, R$, respectively:

$$J_j(\eta_{1:n};\gamma_{1:n}) = \mathbb{E}\left\{\sum_{k=1}^{n} \|Q_{j,k}\boldsymbol{x}_k + R_{j,k}\boldsymbol{u}_k\|^2\right\}, \tag{2.6}$$

where $Q_{j,k} \in \mathbb{R}^{r\times p}$ and $R_{j,k} \in \mathbb{R}^{r\times t}$. Note that $\boldsymbol{u}_k = \gamma_k(\eta_{1:k})(\boldsymbol{y}_{1:k})$ while $\boldsymbol{y}_l = \eta_l(\boldsymbol{x}_{1:l})$ almost surely. We assume that $R'_{R,k}R_{R,k}$ is positive definite, i.e., $R_{R,k}$ is full rank, for all $k = 1,\dots,n$. Then, there is a linear relationship between the best R policies γ_k^* and the posterior

$$\hat{\boldsymbol{x}}_k := \mathbb{E}\{\boldsymbol{x}_k|\boldsymbol{y}_{1:k}\}$$

almost everywhere over $\mathbb{R}^p$. Since $B = O$, by (2.6) for $j = R$, γ_k only impacts the sub-cost function at stage-k, i.e., $\mathbb{E}\{\|Q_{R,k}\boldsymbol{x}_k + R_{R,k}\boldsymbol{u}_k\|^2\}$. Correspondingly, given $\eta_{1:k}$, the best $\mathcal{P}_R$ strategy is given by

$$\gamma_k^*(\eta_{1:k}) = \arg\min_{\gamma_k\in\Gamma_k} \mathbb{E}\left\{\|Q_{R,k}\boldsymbol{x}_k + R_{R,k}\gamma_k(\eta_{1:k})(\boldsymbol{y}_{1:k})\|^2\right\}$$

and by the positive definiteness assumption on $R'_{R,k}R_{R,k} \succ O$, we have

$$\gamma_k^*(\eta_{1:k})(\boldsymbol{y}_{1:k}) = -(R'_{R,k}R_{R,k})^{-1}R'_{R,k}Q_{R,k}\hat{\boldsymbol{x}}_k,$$

almost everywhere over $\mathbb{R}^p$, which also implies that $Pi_R(\eta_{1:n})$ is a singleton.

Example 2.1. This noncooperative communication formulation between $\mathcal{P}_S$ and $\mathcal{P}_R$ also covers the schemes where there exist two separate exogenous processes such that, e.g., [33],

$$\underbrace{\begin{bmatrix}\boldsymbol{z}_{k+1}\\ \boldsymbol{\theta}_{k+1}\end{bmatrix}}_{=\boldsymbol{x}_{k+1}} = \underbrace{\begin{bmatrix}A_z & \\ & A_\theta\end{bmatrix}}_{=A}\underbrace{\begin{bmatrix}\boldsymbol{z}_k\\ \boldsymbol{\theta}_k\end{bmatrix}}_{=\boldsymbol{x}_k} + \underbrace{\begin{bmatrix}\boldsymbol{\omega}_k\\ \boldsymbol{\nu}_k\end{bmatrix}}_{=\boldsymbol{w}_k}. \tag{2.7}$$

$\mathcal{P}_R$ aims to track the process $\{\boldsymbol{z}_k\}$ through the disclosed information $\boldsymbol{y}_k$ while $\mathcal{P}_S$ wants $\mathcal{P}_R$'s decision $\boldsymbol{u}_k$ to track a linear combination of $\boldsymbol{z}_k$ and a bias parameter $\boldsymbol{\theta}_k$, e.g., $\boldsymbol{z}_k + D_k\boldsymbol{\theta}_k$. In particular, the cost functions are in this case given by

$$c_S(\eta_{1:n};\gamma_{1:n}) = \mathbb{E}\left\{\sum_{k=1}^{n} \|\boldsymbol{z}_k + D_k\boldsymbol{\theta}_k - \boldsymbol{u}_k\|^2\right\} \tag{2.8}$$

$$c_R(\eta_{1:n};\gamma_{1:n}) = \mathbb{E}\left\{\sum_{k=1}^{n} \|\boldsymbol{z}_k - \boldsymbol{u}_k\|^2\right\} \tag{2.9}$$

such that in (2.6) for $j = S, R$, $Q_{S,k} = \begin{bmatrix} I & D_k \end{bmatrix}$, $Q_{R,k} = \begin{bmatrix} I & O \end{bmatrix}$, and $R_{S,k} = R_{R,k} = -I$ for $k = 1,\dots,n$.

Corresponding to $\mathcal{P}_R$'s best reactions, $\mathcal{P}_S$ seeks policies η_k^* which minimize the expected cost over $\eta_k \in \Omega_k$. Particularly, the optimization problem faced by $\mathcal{P}_S$ is given by

$$\min_{\substack{\eta_k \in \Omega_k,\\ k=1,\dots,n}} \sum_{k=1}^{n} \mathbb{E}\left\{\|Q_{S,k}\boldsymbol{x}_k - R_{S,k}(R'_{R,k}R_{R,k})^{-1}R'_{R,k}Q_{R,k}\,\hat{\boldsymbol{x}}_k\|^2\right\}. \tag{2.10}$$

Note that (2.10) is a functional optimization problem, where $\mathcal{P}_S$ seeks to find n functions among all Borel measurable functions from $\mathbb{R}^{kp}$ to $\mathbb{R}^p$, for $k = 1,\dots,n$. In order to find these functions, we first aim to formulate an optimization problem over finite dimensional spaces that bounds the original functional optimization problem (2.10) from below. The objective in (2.10) is a quadratic function of $\boldsymbol{x}_k$ and $\hat{\boldsymbol{x}}_k$, and in the following we show that the cost function (2.10) can be written in terms of the second-order moments of $\boldsymbol{x}_k$ and $\hat{\boldsymbol{x}}_k$:

$$\begin{aligned}&\mathbb{E}\left\{\|Q_{S,k}\boldsymbol{x}_k - R_{S,k}(R'_{R,k}R_{R,k})^{-1}R'_{R,k}Q_{R,k}\,\hat{\boldsymbol{x}}_k\|^2\right\}\\ &\quad = \mathbb{E}\left\{\boldsymbol{x}'_k Q'_{S,k}Q_{S,k}\boldsymbol{x}_k\right\} - 2\mathbb{E}\left\{\hat{\boldsymbol{x}}'_k\Lambda'_k Q_{S,k}\boldsymbol{x}_k\right\} + \mathbb{E}\left\{\hat{\boldsymbol{x}}'_k\Lambda'_k\Lambda_k\hat{\boldsymbol{x}}_k\right\},\end{aligned}$$

where $\Lambda_k := R_{S,k}(R'_{R,k}R_{R,k})^{-1}R'_{R,k}Q_{R,k}$. Note that the first term on the right-hand side does not include $\hat{\boldsymbol{x}}_k$, and therefore does not depend on $\mathcal{P}_S$'s signaling rules. For the second term, we have

$$\begin{aligned}\mathbb{E}\{\hat{\boldsymbol{x}}'_k\Delta\boldsymbol{x}_k\} &\overset{(a)}{=} \mathbb{E}\{\mathbb{E}\{\hat{\boldsymbol{x}}'_k\Delta\boldsymbol{x}_k|\boldsymbol{y}_{1:k}\}\}\\ &\overset{(b)}{=} \mathbb{E}\{\hat{\boldsymbol{x}}'_k\Delta\mathbb{E}\{\boldsymbol{x}_k|\boldsymbol{y}_{1:k}\}\} \overset{(c)}{=} \mathbb{E}\{\hat{\boldsymbol{x}}'_k\Delta\hat{\boldsymbol{x}}_k\},\end{aligned} \tag{2.11}$$

where Δ is an arbitrary deterministic matrix with associated dimensions. The equality (a) is due to the law of iterated expectations; (b) holds because

$\hat{\boldsymbol{x}}_k$ is σ-$\boldsymbol{y}_{1:k}$ measurable; and (c) is due to $\hat{\boldsymbol{x}}_k = \mathbb{E}\{\boldsymbol{x}_k|\boldsymbol{y}_{1:k}\}$. Therefore,

$$\begin{aligned} 2\mathbb{E}\left\{\hat{\boldsymbol{x}}_k'\Lambda_k'Q_{S,k}\boldsymbol{x}_k\right\} &= \mathbb{E}\left\{\hat{\boldsymbol{x}}_k'(\Lambda_k'Q_{S,k} + Q_{S,k}'\Lambda_k)\boldsymbol{x}_k\right\} \\ &= \mathbb{E}\left\{\hat{\boldsymbol{x}}_k'(\Lambda_k'Q_{S,k} + Q_{S,k}'\Lambda_k)\hat{\boldsymbol{x}}_k\right\}. \end{aligned} \tag{2.12}$$

Then, we can re-write the optimization problem (2.10) as

$$\min_{\substack{\eta_k\in\Omega_k,\\ k=1,\ldots,n}} \sum_{k=1}^{n} \mathbb{E}\{\hat{\boldsymbol{x}}_k'V_k\hat{\boldsymbol{x}}_k\}, \tag{2.13}$$

where

$$V_k := \Lambda_k'\Lambda_k - \Lambda_k'Q_{S,k} - Q_{S,k}'\Lambda_k. \tag{2.14}$$

As an example, for Example 2.1, we have $V_k := \begin{bmatrix} -I & -D_k \\ -D_k & O \end{bmatrix}$.

We point out that in Reference [22], the author addresses multidimensional information disclosure for the single-stage case. To this end, he constructs a Semi-Definite Programming (SDP) problem as a bound on sender's objective function (named utility function in [22]) and shows that linear strategies for Gaussian parameters can achieve this bound. Here, we employ a similar approach to extend these results to the dynamic settings by addressing the question of whether the linear strategies are still optimal within the general class of policies or not.

The first-order moment of $\hat{\boldsymbol{x}}_k$ is

$$\begin{aligned} \mathbb{E}\{\hat{\boldsymbol{x}}_k\} &= \mathbb{E}\{\mathbb{E}\{\boldsymbol{x}_k|\boldsymbol{y}_{1:k}\}\} \\ &= \mathbb{E}\{\boldsymbol{x}_k\} = 0 \end{aligned} \tag{2.15}$$

by the law of iterated expectations. We define the covariance matrix of $\hat{\boldsymbol{x}}_k$, namely the posterior covariance, as $H_k := \mathbb{E}\{(\hat{\boldsymbol{x}}_k - \mathbb{E}\{\hat{\boldsymbol{x}}_k\})(\hat{\boldsymbol{x}}_k - \mathbb{E}\{\hat{\boldsymbol{x}}_k\})'\} = \mathbb{E}\{\hat{\boldsymbol{x}}_k\hat{\boldsymbol{x}}_k'\}$. We note that for multivariate Gaussian variables, the mean is well defined, which implies that $\hat{\boldsymbol{x}}_k$ exists by the Radon-Nikodym theorem [57]. Furthermore, being multivariate Gaussian, the state parameter is integrable, i.e., $\mathbb{E}\{|\boldsymbol{x}_k|\} < \infty$, hence $\hat{\boldsymbol{x}}_k$ is finite almost surely, which implies that $H_k = \mathbb{E}\{\hat{\boldsymbol{x}}_k\hat{\boldsymbol{x}}_k'\}$ also exists.

The following lemma provides a lower bound for the minimization problem in (2.13).

Lemma 2.1. *There exists a semi-definite programming (SDP) problem bounding the minimization problem* (2.13) *from below and given by*[7]

$$\min_{\substack{S_k \in \mathbb{S}^p,\\ k=1,\dots,n}} \sum_{k=1}^{n} \operatorname{Tr}\{V_k S_k\} \tag{2.16}$$

subject to $\Sigma_j \geq S_j \geq AS_{j-1}A'$ for $j = 1,\dots,n$, and $S_0 = O$.

Proof. The proof is provided in Appendix A.1. The key point is that at stage-k, the covariance of the posterior, i.e., H_k, is bounded from above by the case when we disclose the information fully, i.e., Σ_k, and is bounded from below by the case when we disclose no information yet $\mathcal{P}_R$ can still infer $\boldsymbol{x}_k$ based on all previously sent signals $\boldsymbol{y}_{1:k-1}$. □

We point out that (2.16) is indeed an SDP problem [58]. There exist effective computational tools to solve SDP problems numerically, e.g., through CVX, a package for specifying and solving convex programs [59, 60]. However, closed-form solutions can rarely be obtained [58]. Therefore, in order to solve (2.16) analytically, we develop a different approach and characterize the solutions without computing them explicitly. The following theorem characterizes the solution of (2.16) for an arbitrary (but finite) number of stages.

Theorem 2.2. *There exist symmetric idempotent matrices $P_k \in \mathbb{S}^p$, for $k = 1,\dots,n$, such that*

$$S_k^* = AS_{k-1}^*A' + (\Sigma_k - AS_{k-1}^*A')^{1/2} P_k (\Sigma_k - AS_{k-1}^*A')^{1/2}, \tag{2.17}$$

for $k = 1,\dots,n$ (with $S_0^* = O$), attains the global minimum of (2.16).

Proof. We first point out that the constraint set in (2.16), i.e.,

$$\Psi := \left\{ (S_1,\dots,S_n) \in \mathbb{S}^p \times \dots \times \mathbb{S}^p \,\middle|\, \bigwedge_k \{S_k \in \Psi_k(S_{k-1})\} \right\}, \tag{2.18}$$

where $\Psi_k(S_{k-1}) := \{S_k \in \mathbb{S}^p \mid \Sigma_k \geq S_k \geq AS_{k-1}A'\}$, is convex. To show this, consider n-tuples of symmetric matrices $(M_1,\dots,M_n) \in \mathbb{S}^p \times \dots \times \mathbb{S}^p$ and $(N_1,\dots,N_n) \in \mathbb{S}^p \times \dots \times \mathbb{S}^p$ such that both $(M_1,\dots,M_n)$ and $(N_1,\dots,N_n)$

[7] $\mathbb{S}^p$ denotes the set of symmetric $p \times p$ matrices.

are in the constraint set Ψ. Then, Ψ is a convex set if, and only if, for any $t \in [0,1]$, the linear combination

$$\begin{aligned}(E_1,\dots,E_n) :&= t(M_1,\dots,M_n) + (1-t)(N_1,\dots,N_n)\\ &= (tM_1 + (1-t)N_1,\dots,tM_n + (1-t)N_n) \in \Psi.\end{aligned}$$

Since $\Sigma_1 \geq M_1 \geq O$ and $\Sigma_1 \geq N_1 \geq O$, we have

$$\Sigma_1 \geq tM_1 + (1-t)N_1 \geq O,$$

and $E_1 = tM_1 + (1-t)N_1 \in \Psi_1(O)$. Suppose that $E_j \in \Psi_j(E_{j-1})$ for $j = 1,\dots,k-1$. Since $\Sigma_k \geq M_k \geq AM_{k-1}A'$, $\Sigma_k \geq N_k \geq AN_{k-1}A'$, and $E_{k-1} = tM_{k-1} + (1-t)N_{k-1}$, we obtain

$$\Sigma_k \geq tM_k + (1-t)N_k \geq AE_{k-1}A',$$

and $E_k = tM_k + (1-t)N_k \in \Psi_k(E_{k-1})$. By induction, we conclude that the convex combination $(E_1,\dots,E_n) \in \Psi$ and therefore Ψ is a convex set. Note that since the objective function in (2.16) is linear in $S_1,\dots,S_n$ (not a zero function) and the constraint set is non-empty compact (since Ψ is a Cartesian product of the closed and bounded sets $\Psi_k(S_{k-1})$) and convex, the global minimum can be attained at the *extreme points* of Ψ.[8]

Next, we formulate the extreme points of Ψ. To this end, for given $S_{-k} := \{S_1,\dots,S_{k-1},S_{k+1},\dots,S_n\}$, we introduce the sub-constraint set:

$$\begin{aligned}\Phi_k(S_{-k}) := \big\{S_k \in \mathbb{S}^p \mid \Sigma_k \geq S_k \geq AS_{k-1}A'\\ \wedge\ A^{-1}S_{k+1}(A')^{-1} \geq S_k \geq AS_{k-1}A'\big\},\end{aligned} \tag{2.19}$$

for each $k = 1,\dots,n$, where we set $S_0 = O$ and $S_{n+1} = A\Sigma_n A' + \Sigma_w$. We consider that the sub-constraint set $\Phi_k(S_{-k}) = \varnothing$ is empty if $\Sigma_k - AS_{k-1}A'$ or $A^{-1}S_{k+1}(A')^{-1} - AS_{k-1}A'$ are not positive semi-definite. Then, the following lemma provides a necessary condition for the extreme points of Ψ in terms of these sub-constraint sets (2.19).

Lemma 2.3. *If an n-tuple $(E_1,\dots,E_n) \in \Psi$ is an extreme point of Ψ, then*

[8] An extreme point of a convex set is a point that cannot be written as a convex combination of any other points in the interior of the set.

for each $k = 1, \dots, n$, $E_k \in \Phi_k(E_{-k})$ is an extreme point of $\Phi_k(E_{-k})$.

Proof. The proof can be shown via contradiction and is provided in Appendix A.2. □

Now, we seek to obtain the extreme points through the necessary conditions provided in Lemma 2.3. Let $(S_1^*, \dots, S_n^*) \in \Psi$ be an extreme point of Ψ. Then, the element S_n^* should be an extreme point of $\Phi_n(S_{-n}^*)$. To this end, consider arbitrary $S_1, \dots, S_n$. Then, in stage-n, the sub-constraint set $\Phi_n(S_{-n})$ is given by

$$\Phi_n(S_{-n}) = \{S_n \in \mathbb{S}^p | \Sigma_n \geq S_n \geq AS_{n-1}A'\}$$

since we set $S_{n+1} = A\Sigma_n A' + \Sigma_w$ and

$$A^{-1}(A\Sigma_n A' + \Sigma_w)(A')^{-1} = \Sigma_n + A^{-1}\Sigma_w(A')^{-1} \succ \Sigma_n.$$

We note that for each $k = 1, \dots, n$, if $\Sigma_k \geq S_k$, then the matrix $\Sigma_{k+1} - AS_kA'$ is positive definite because

$$\Sigma_{k+1} - AS_kA' = A\Sigma_kA' + \Sigma_w - AS_kA' = A(\Sigma_k - S_k)A' + \Sigma_w$$

and $\Sigma_w \succ O$ by definition. Then, if $\Sigma_{n-1} \geq S_{n-1}$, we have $\Sigma_n \succ AS_{n-1}A'$ and the following transformation:

$$F_n(S_n) := (\Sigma_n - AS_{n-1}A')^{-1/2}(S_n - AS_{n-1}A')(\Sigma_n - AS_{n-1}A')^{-1/2} \tag{2.20}$$

such that F_n maps the sub-constraint set $\Phi_n(S_{-n})$ to

$$F_n(\Phi_n(S_{-n})) = \{P \in \mathbb{S}^p | I \geq P \geq O\}. \tag{2.21}$$

The following lemma characterizes the extreme points of the convex set $\Phi := \{P \in \mathbb{S}^p \mid I \geq P \geq O\}$.

Lemma 2.4. *A point P_e in Φ is an extreme point if, and only if, P_e is a symmetric idempotent matrix.*

Proof. The proof can be shown via contradiction and is provided in Appendix A.3. □

We note that under bijective affine transformation of a convex set, the extreme points are mapped to the extreme points of the transformed set [61]. Since $F_n(\cdot)$ is a bijective affine transformation, $P_o \in \Phi$ is an extreme point of Φ if, and only if, $F_n^{-1}(P_o) \in \Phi_n(S_{-n})$ is an extreme point of $\Phi_n(S_{-n})$. Therefore, if $\Sigma_{n-1} \geq S_{n-1}$, the extreme points of $\Phi_n(S_{-n})$ are given by

$$S_n^* = AS_{n-1}A' + (\Sigma_n - AS_{n-1}A')^{1/2} P_n (\Sigma_n - AS_{n-1}A')^{1/2},$$

where P_n is a symmetric idempotent matrix.

For stage-$(n-1)$, we have the sub-constraint set:

$$\begin{aligned}\Phi_{n-1}(S_{-(n-1)}) = \{&S_{n-1} \in \mathbb{S}^p | \Sigma_{n-1} \geq S_{n-1} \geq AS_{n-2}A' \\ &\wedge A^{-1}S_n(A')^{-1} \geq S_{n-1} \geq AS_{n-2}A'\}.\end{aligned}$$

We point out that if $S_{n-1} \in \Phi_{n-1}(S_{-(n-1)})$, we have $\Sigma_{n-1} \geq S_{n-1}$. Then, setting $S_n = S_n^*$, we obtain

$$\begin{aligned}\Phi_{n-1}(S_{-(n-1)}) = \{&S_{n-1} \in \mathbb{S}^p | \Sigma_{n-1} \geq S_{n-1} \geq AS_{n-2}A' \\ &\wedge S_{n-1} + \Delta \geq S_{n-1} \geq AS_{n-2}A'\},\end{aligned}$$

where

$$\Delta := A^{-1}(\Sigma_n - AS_{n-1}A')^{1/2} P_n (\Sigma_n - AS_{n-1}A')^{1/2}(A')^{-1} \geq O.$$

Therefore, if S_n is an extreme point of $\Phi_n(S_{-n})$, the sub-constraint set $\Phi_{n-1}(S_{-(n-1)})$ can be written as

$$\Phi_{n-1}(S_{-(n-1)}) = \{S_{n-1} \in \mathbb{S}^p | \Sigma_{n-1} \geq S_{n-1} \geq AS_{n-2}A'\}.$$

Correspondingly, if $\Sigma_{n-2} \geq S_{n-2}$, the extreme points of $\Phi_{n-1}(S_{-(n-1)})$ are given by

$$S_{n-1}^* = AS_{n-2}A' + (\Sigma_{n-1} - AS_{n-2}A')^{1/2} P_{n-1} (\Sigma_{n-1} - AS_{n-2}A')^{1/2},$$

where P_{n-1} is also a symmetric idempotent matrix. Since $\Sigma_{n-1} \geq S_{n-1}^*$, setting $S_{n-1} = S_{n-1}^*$, we have

$$S_n^* = AS_{n-1}^*A' + (\Sigma_n - AS_{n-1}^*A')^{1/2} P_n (\Sigma_n - AS_{n-1}^*A')^{1/2}.$$

Following identical steps, we obtain that any extreme point $(S_1^*, \ldots, S_n^*)$ of Ψ should satisfy (2.17). □

In the next section, we address the tightness of the bound (2.16), i.e., whether the minimum of the lower bound can be achieved through certain sender policies or not.

2.3 Optimality of Linear Signaling Rules

Even though Theorem 2.2 characterizes the necessary and sufficient conditions for the minimizing arguments of the SDP problem (2.16), it still does not provide the solutions explicitly. However, as we will show next, these results have important consequences in the characterization of equilibrium achieving signaling rules for the original optimization problem (2.13). In particular, sender strategies that can be constructed to yield posterior covariances in (2.17) can minimize the lower bound (2.16), and therefore can minimize the main objective function (2.13).

The following theorem says that for *any* solution of (2.16), say $S_1^*, \ldots, S_n^*$, there exist certain deterministic matrices $L_k \in \mathbb{R}^{p \times p}$ for $k = 1, \ldots, n$, such that the memoryless linear disclosure policies

$$\eta_k(\boldsymbol{x}_{1:k}) = L_k' \boldsymbol{x}_k, \tag{2.22}$$

almost everywhere over $\mathbb{R}^p$, result in $H_1 = S_1^*, \ldots, H_n = S_n^*$. In particular, by minimizing the lower bound on $\mathcal{P}_S$'s objective function, the memoryless linear sender policies (2.22) yield the multi-stage Stackelberg equilibrium within the general class of measurable policies.

Theorem 2.5. *Let* $S_1^*, \ldots, S_n^*$ *be a solution of the SDP problem* (2.16) *and* $P_1, \ldots, P_n$ *be the corresponding symmetric idempotent matrices in* (2.17)*. Let* P_k*,* $k = 1, \ldots, n$*, have the eigen decompositions:* $P_k = U_k \Lambda_k U_k'$*. Then, for*

$$L_k = (\Sigma_k - A S_{k-1}^* A')^{-1/2} U_k \Lambda_k, \tag{2.23}$$

memoryless linear sender strategies (2.22) *yield the multi-stage equilibrium* (2.13) *within the general class of policies.*

Proof. Say that $\mathcal{P}_S$ employs memoryless linear policies as in (2.22) for some deterministic combination of matrices $L_1, \ldots, L_n \in \mathbb{R}^{p\times p}$. Correspondingly, the posteriors $\hat{\boldsymbol{x}}_k = \mathbb{E}\{\boldsymbol{x}_k | \boldsymbol{y}_{1:k}\} = \mathbb{E}\{\boldsymbol{x}_k | L_1'\boldsymbol{x}_1, \ldots, L_k'\boldsymbol{x}_k\}$ are given by[9]

$$\begin{aligned}\hat{\boldsymbol{x}}_1 =& \Sigma_1 L_1 (L_1'\Sigma_1 L_1)^\dagger L_1' \boldsymbol{x}_1 && (2.24)\\ \hat{\boldsymbol{x}}_k =& A\hat{\boldsymbol{x}}_{k-1} + (\Sigma_k - AH_{k-1}A')L_k(L_k'(\Sigma_k - AH_{k-1}A')L_k)^\dagger\\ &\times L_k'(\boldsymbol{x}_k - A\hat{\boldsymbol{x}}_{k-1}) \text{ for } k \geq 2. && (2.25)\end{aligned}$$

Next, we seek to compute $H_k = \mathbb{E}\{\hat{\boldsymbol{x}}_k\hat{\boldsymbol{x}}_k'\}$, for $k = 1, \ldots, n$. By (2.24), we obtain $H_1 = \Sigma_1 L_1 (L_1'\Sigma_1 L_1)^\dagger L_1'\Sigma_1$ since $\mathbb{E}\{\boldsymbol{x}_1\boldsymbol{x}_1'\} = \Sigma_1$, and for a matrix M and its pseudo-inverse $M^\dagger$, we have $M^\dagger M M^\dagger = M$. By (2.25), for H_2, we have a cross-term $\mathbb{E}\{\hat{\boldsymbol{x}}_1(\boldsymbol{x}_2 - A\hat{\boldsymbol{x}}_1)'\}$, which can be written as

$$\begin{aligned}\mathbb{E}\{\hat{\boldsymbol{x}}_1(\boldsymbol{x}_2 - A\hat{\boldsymbol{x}}_1)'\} &= \mathbb{E}\{\hat{\boldsymbol{x}}_1\boldsymbol{x}_2'\} - \mathbb{E}\{\hat{\boldsymbol{x}}_1\hat{\boldsymbol{x}}_1'\}A' && (2.26)\\ &= H_1A' - H_1A' = O, && (2.27)\end{aligned}$$

due to the law of iterated expectations such that $\mathbb{E}\{\hat{\boldsymbol{x}}_1\boldsymbol{x}_2'\} = \mathbb{E}\{\mathbb{E}\{\hat{\boldsymbol{x}}_1\boldsymbol{x}_2'|\boldsymbol{y}_1\}\} = \mathbb{E}\{\hat{\boldsymbol{x}}_1\mathbb{E}\{\boldsymbol{x}_2'|\boldsymbol{y}_1\}\} = \mathbb{E}\{\hat{\boldsymbol{x}}_1\hat{\boldsymbol{x}}_1'\}A'$. Then, (2.25), for $k \geq 2$, leads to

$$\begin{aligned}H_k = &AH_{k-1}A' + (\Sigma_k - AH_{k-1}A')L_k\\ &\times (L_k'(\Sigma_k - AH_{k-1}A')L_k)^\dagger L_k'(\Sigma_k - AH_{k-1}A'). && (2.28)\end{aligned}$$

Let $C_1 := \Sigma_1^{1/2}L_1$ and $C_k := (\Sigma_k - AH_{k-1}A')^{1/2}L_k$ for $k = 2, \ldots, n$, such that $H_1 = \Sigma_1^{1/2}C_1(C_1'C_1)^\dagger C_1'\Sigma_1^{1/2}$, and for $k \geq 2$,

$$\begin{aligned}H_k = &AH_{k-1}A' + (\Sigma_k - AH_{k-1}A')^{1/2}\\ &\times C_k(C_k'C_k)^\dagger C_k'(\Sigma_k - AH_{k-1}A')^{1/2}. && (2.29)\end{aligned}$$

Note that $C_k(C_k'C_k)^\dagger C_k'$, for $k = 1, \ldots, n$, is a symmetric idempotent matrix and the posterior covariances $H_1, \ldots, H_n$ have identical expressions as in (2.17). If the symmetric idempotent matrices P_k for $k = 1, \ldots, n$ corresponding to the minimizers of the SDP problem (2.16) have the eigen decompositions: $P_k = U_k\Lambda_kU_k'$, we can set $C_k = U_k\Lambda_k$ for $k = 1, \ldots, n$, such that $C_k(C_k'C_k)^\dagger C_k' = P_k$. In particular, setting $L_1 = \Sigma_1^{-1/2}U_1\Lambda_1$ and

[9] We take the pseudo inverse of the matrices since they can be singular if the associated matrix L_k has a rank smaller than p. For example, at stage-k, $\mathcal{P}_S$ can disclose no information $\eta_k(\boldsymbol{x}_{1:k}) = 0$.

Table 2.1: A description to compute equilibrium achieving sender policies in strategic communication.

```
Algorithm 2.1: Strategic Communication
SDP Problem:
    Compute $V_k$, $\forall k$, by (2.14).
    Solve the SDP problem (2.16) through a numerical toolbox
      and obtain the solution $S_k^*$, $\forall k$.
Equilibrium achieving policies:
    Compute the corresponding idempotent matrices $P_k$,$\forall k$,
      by using the solution $S_k^*$, $\forall k$, and (2.17).
    Compute the eigen decompositions: $P_k = U_k \Lambda_k U_k'$.
    Compute $L_k$, $\forall k$, by using $S_{k-1}^*, U_k, \Lambda_k$, and (2.23).
```

$L_k = (\Sigma_k - AS_{k-1}^* A')^{-1/2} U_k \Lambda_k$, we obtain $H_k = S_k^*$ for $k = 1, \ldots, n$. Hence, the memoryless linear signaling rules (2.22) can minimize the main objective function (2.13) within the general class of measurable policies. □

In Table 2.1, we provide a description to compute the equilibrium achieving sender policies based on Lemma 2.1, and Theorems 2.2 and 2.5. We note that for linear sender signaling rules, the corresponding equilibrium achieving receiver signaling rules are also linear since the underlying state is Gaussian. Therefore, linear sender and receiver signaling rules can achieve the equilibrium also in multi-stage hierarchical Gaussian signaling games.

2.4 Intriguing Properties of Gaussian Signaling

In this section, we list several intriguing remarks related to the proposed hierarchical signaling scheme:

Uniqueness of the Solution: In addition to the memoryless linear sender strategies in Theorem 2.5, any signaling rule leading to the same posteriors can yield the equilibrium. As an example, if $\boldsymbol{y}_k = L_k' \boldsymbol{x}_k$ for $k = 1, \ldots, n$ achieves the equilibrium, then $\tilde{\boldsymbol{y}}_1 = \boldsymbol{y}_1$ and $\tilde{\boldsymbol{y}}_k = \boldsymbol{y}_k - \mathbb{E}\{\boldsymbol{y}_k | \boldsymbol{y}_{1:k-1}\}$ for $k = 2, \ldots, n$

lead to the same posteriors, i.e., $\mathbb{E}\{\boldsymbol{x}_k|\tilde{\boldsymbol{y}}_{1:k}\} = \mathbb{E}\{\boldsymbol{x}_k|\boldsymbol{y}_{1:k}\}$ for $k = 1, \ldots, n$, therefore yield the equilibrium. Note that $\tilde{\boldsymbol{y}}_{1:n}$ is a whitened version of $\boldsymbol{y}_{1:n}$, i.e., $\tilde{\boldsymbol{y}}_k$'s are pair-wise independent of each other.

Inter-stage Coupling: In general, when $\mathcal{P}_S$ and $\mathcal{P}_R$ have different cost functions, signaling rules: $\eta_k(\boldsymbol{x}_{1:k}) = K_k'(\boldsymbol{x}_k - \mathbb{E}\{\boldsymbol{x}_k|\boldsymbol{x}_{1:k-1}\})$, for certain matrices $K_k \in \mathbb{R}^{p\times p}$ (where $\boldsymbol{x}_k - \mathbb{E}\{\boldsymbol{x}_k|\boldsymbol{x}_{1:k-1}\} = \boldsymbol{w}_{k-1}$ is the innovation in the state process) do not lead to the equilibrium, contrary to the case when they have the same cost functions. In particular, in the multi-stage case, the sub-games at each stage are not decoupled and cannot be considered as a single-stage game as if the innovation part of the state is going to be disclosed. As an example, let $\Sigma_1 = O$ such that $\boldsymbol{x}_2 = \boldsymbol{w}_1$; then $\boldsymbol{y}_2 = K_2'\boldsymbol{w}_1$ and $\boldsymbol{y}_3 = K_3'\boldsymbol{w}_2$. This implies that

$$\begin{aligned} H_2 &= \Sigma_w K_2 (K_2'\Sigma_w K_2)^\dagger K_2'\Sigma_w \\ H_3 &= A H_2 A' + \Sigma_w K_3 (K_3'\Sigma_w K_3)^\dagger K_3'\Sigma_w. \end{aligned}$$

However, by Theorem 2.2, the corresponding S_k's are

$$\begin{aligned} S_2 &= \Sigma_2^{1/2} P_2 \Sigma_2^{1/2} = \Sigma_w^{1/2} P_2 \Sigma_w^{1/2}, \\ S_3 &= A S_2 A' + (\Sigma_3 - A S_2 A')^{1/2} P_3 (\Sigma_3 - A S_2 A')^{1/2}. \end{aligned}$$

We can set K_2 such that $H_2 = S_2$; however, $H_3 = S_3$ requires that

$$\begin{aligned} \Sigma_w^{1/2} K_3 (K_3'\Sigma_w K_3)^\dagger K_3'\Sigma_w^{1/2} = \Sigma_w^{-1/2} &(\Sigma_3 - A S_2 A')^{1/2} \\ &\times P_3 (\Sigma_3 - A S_2 A')^{1/2} \Sigma_w^{-1/2}. \end{aligned} \tag{2.30}$$

Note that the left-hand side of (2.30) is a symmetric idempotent matrix, however, the right-hand side is not necessarily an idempotent matrix.

Applicability to Noisy Observations: The results would hold if the message space was larger than p since it would also lead to the same constraint set Ψ (2.18). However, the derivations would not carry over if $\mathcal{P}_S$ had access to noisy version of the state instead of the actual state. As an example, consider the situation where $\mathcal{P}_S$ has access to $\boldsymbol{s}_k = C\boldsymbol{x}_k + \boldsymbol{v}_k$, where $C \in \mathbb{R}^{p\times p}$ and $\{\boldsymbol{v}_k \sim \mathcal{N}(0, \Sigma_v)\}$ is an independent white Gaussian noise process. Then,

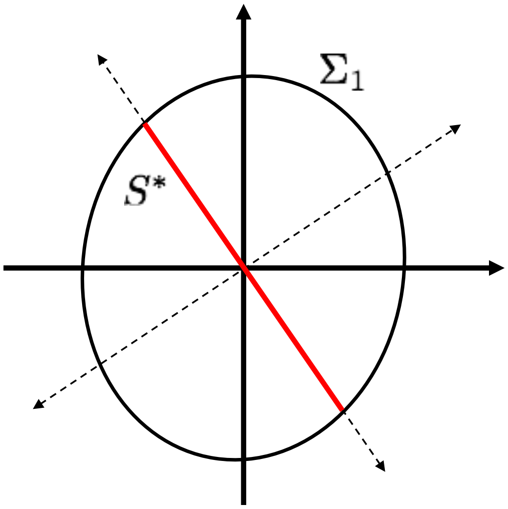


Figure 2.2: Illustration of Σ_1 and S^* for $n = 2$.

for $\boldsymbol{y}_k = K_k'\boldsymbol{s}_k$, the posteriors would be given by

$$\begin{aligned}\hat{\boldsymbol{x}}_1 &= \Sigma_1 C' L_1 (L_1' C \Sigma_1 C' L_1 + \underbrace{L_1' \Sigma_v L_1})^\dagger L_1' \boldsymbol{s}_1 \\ \hat{\boldsymbol{x}}_k &= A\hat{\boldsymbol{x}}_{k-1} + (\Sigma_k - AH_{k-1}A')C'L_k \\ &\times \left[L_k' C(\Sigma_k - AH_{k-1}A')C'L_k + \underbrace{L_k'\Sigma_v L_k}\right]^\dagger L_k'(\boldsymbol{s}_k - CA\hat{\boldsymbol{x}}_{k-1})\end{aligned}$$

and due to the underbraced term, $(\Sigma_k - AH_{k-1}A')^{-1/2}(H_k - AH_{k-1}A')(\Sigma_k - AH_{k-1}A')^{-1/2}$ would not lead to a symmetric idempotent matrix, contrary to (2.29).

Applicability to Different Dimensional Signals: For the single-stage case, i.e., $n = 1$, as in [22], the lower bound (2.16) is given by

$$\min_{S \in \mathbb{S}^p} \operatorname{Tr}\{V_1 S\} \tag{2.31}$$

subject to $\Sigma_1 \succeq S \succeq O$. And the optimizer is given by

$$S^* = \Sigma_1^{1/2} Q_- Q_-' \Sigma_1^{1/2}, \tag{2.32}$$

where $Q_- = \begin{bmatrix} q_1 & \cdots & q_m \end{bmatrix}$ and $q_j \in \mathbb{R}^p$, $j = 1, \ldots, m$, are the eigenvectors of $\Sigma_1^{1/2} V_1 \Sigma_1^{1/2}$ corresponding to negative eigenvalues. This also implies that in the multi-stage case, i.e., $n > 1$, the rank of L_k is bounded from above by the number of negative eigenvalues of V_k due to Sylvester's law of inertia [62].

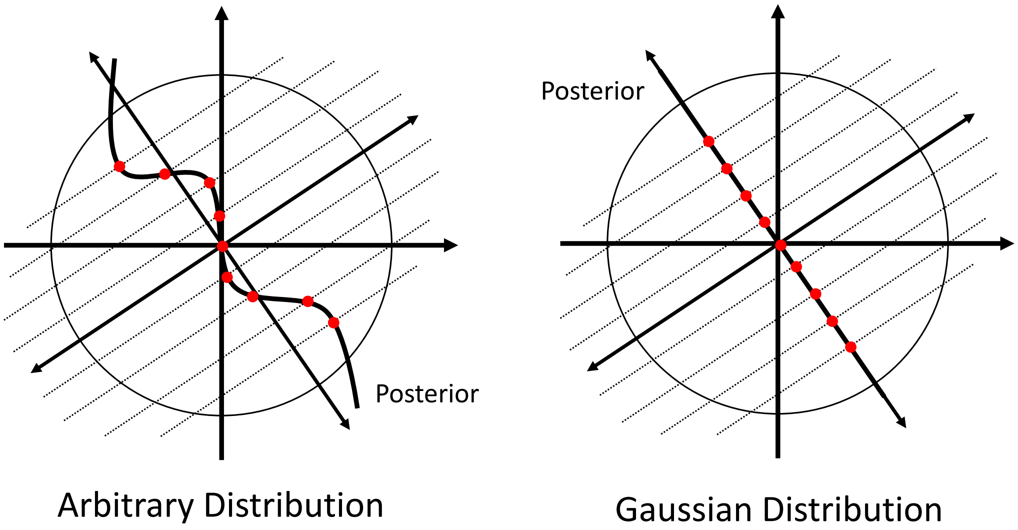
Applicability to Different Information Models: For the single-stage case, the optimal signaling rule can be computed analytically and is given by [22]

$$\eta(\boldsymbol{x}_1) = Q'\Sigma_1^{-1/2}\boldsymbol{x}_1, \tag{2.33}$$

almost everywhere over $\mathbb{R}^p$, where $Q = \begin{bmatrix} Q_- & O_{p\times(p-m)} \end{bmatrix}$. When we take a closer look at (2.32) for $p = 2$, we observe that the signal should not be informative in a certain direction (e.g., the direction of the eigenvector of $\Sigma_1^{1/2}V_1\Sigma_1^{1/2}$ associated with positive eigenvalue) while it should be fully informative another direction (e.g., the direction of the eigenvector associated with negative eigenvalue), which has also been illustrated in Fig. 2.2. Then, the optimal signaling rule for Gaussian information case, i.e., (2.33), is just a projection of the information onto the direction (expected to be fully informative) through a linear signaling rule. Since the signals in the orthogonal directions[10] are uncorrelated with each other and they are jointly Gaussian, the orthogonality implies that they are independent of each other. Correspondingly, any information on one of them, e.g., vertical direction, does not provide any information about the other, e.g., horizontal direction, since the posterior conditioned on independent information is just the same with the posterior without conditioning on any information. However, this is not the case for arbitrary information models, e.g., other than Gaussian, since uncorrelatedness does not imply independence in general.

In particular, Fig. 2.3 illustrates this for $p = 2$ and when the underlying coordinates, i.e., $\mathbb{R}^p$, have been transformed linearly such that $\Sigma_1 = I$ over the new coordinates. We seek to design the signaling rule such that the signal is fully informative in the left-tilted direction while not informative in the right-tilted direction. The projection onto the left-tilted direction is fully informative in that direction. However, such a projection implies that the realized information can be at any point on the line passing through the projection, and parallel to the right-tilted direction according to the underlying distribution. For the Gaussian case, the corresponding posterior is just on the left-tilted direction since $\Sigma_1 = I$. However, for arbitrary distributions, the posterior conditioned on the parallel lines may not be on the left-tilted direction, as seen in Fig. 2.3, and any deviation of the posterior from the left-tilted direction implies that the projection-based signaling is

[10] Note that they have zero-mean at those directions.



Arbitrary Distribution

Gaussian Distribution

Figure 2.3: For $p = 2$, we show how informative the signal is in the other direction if the signal is the projection of the realization on the left-tilted direction for arbitrary distribution (on the left sub-figure) and Gaussian distribution (on the right sub-figure) while $\Sigma_1 = I$. Particularly, the projection implies that the realization could be at any point on the line passing through the projection, and parallel to the right-tilted direction. Conditioned on that, the posterior (marked with red dots) may not be on the left-tilted direction, i.e., the projection can also be informative on the right-tilted direction for arbitrary distributions.

also informative on the right-tilted direction. Therefore, the covariance of the posterior, i.e., $\mathbb{E}\{\hat{\boldsymbol{x}}_1\hat{\boldsymbol{x}}_1'\}$, would not be equal to the solution of the lower bound (2.32) through such a linear (or indeed any) signaling rule for arbitrary distributions in general.

Optimality of Gaussian Information for Deception: What we have observed above also implies that Gaussian distribution is the *best* distribution serving deceptive $\mathcal{P}_S$'s objective since the lower bound is not necessarily tight for other distributions. Additionally, if $\mathcal{P}_R$'s policies are restricted to linear functions, then the proposed approach also computes the optimal signaling rule for arbitrary distributions, since uncorrelatedness yields linear independence.

In the next section, we compute the optimal linear signaling rules in noncooperative control scenarios, e.g., $B \neq O$ in (2.1).

2.5 Dynamic Gaussian Signaling in Control Systems

Returning back to the general scenario (2.1), we now consider the situation where $\mathcal{P}_S$ and $\mathcal{P}_R$ have the following quadratic finite horizon cost functions, for $j = S, R$, respectively:

$$J_j = \mathbb{E}\left\{\sum_{k=1}^{n} \boldsymbol{x}'_{k+1} Q_{j,k+1} \boldsymbol{x}_{k+1} + \boldsymbol{u}'_k R_{j,k} \boldsymbol{u}_k\right\}, \tag{2.34}$$

where $Q_{j,k+1} \in \mathbb{R}^{p\times p}$ are positive semi-definite and $R_{j,k} \in \mathbb{R}^{t\times t}$ are positive definite.

For discrete-time linear Gaussian stochastic systems and in *scalar* settings, if the measurement signals and the control inputs can be constructed within the class of general policies, and there exists an additive white Gaussian noise (AWGN) channel between the sensor and the controller, reference [63] has shown that in the simultaneous (or cooperative) design, the optimal performance in terms of quadratic cost functions can be obtained through linear control inputs, and measurement signals which are linear in the innovation in the state. However, the linear measurement signals may not be optimal for the multidimensional cases in general. Furthermore, again in a cooperative setting, reference [64] has formulated the joint sensor and controller design problem over a perfect channel when there exists additive (privacy-preservation induced) information-theoretic cost of communication in addition to the quadratic control cost similar to (2.34). And the authors have addressed the problem when the sensor's policies are restricted to a linear structure and provided an SDP-based algorithm to compute the optimal strategies [64].

Remark. We note that this stochastic control problem entails non-classical information in the general settings, where $\mathcal{P}_S$ selects signaling rules within the general class of measurable policies, since $\mathcal{P}_S$'s signaling rules are functions of the actual state (correspondingly the control inputs) and both players can exploit this via triggering-based threat strategies in this *noncooperative* dynamic setting [3, 65]. Correspondingly, optimality of linear sender strategies is still an open problem, and linearity may or may not hold within the general class of strategies.

However, here, we restrict $\mathcal{P}_S$'s signaling rules to memoryless linear strategies as in [64] and in the following, we provide an SDP-based efficient algorithm to compute the optimal sender strategies numerically with global optimality guarantees. Particularly, $\mathcal{P}_S$ selects η_k^ℓ from the space of all linear functions from $\mathbb{R}^p$ to $\mathbb{R}^p$, denoted by Ω^ℓ, such that the signal $\boldsymbol{y}^\ell = \eta_k^\ell(\boldsymbol{x}_k)$ almost everywhere over $\mathbb{R}^p$. Correspondingly, there exist certain matrices $L_k \in \mathbb{R}^{p\times p}$ such that $\boldsymbol{y}_k^\ell = L_k'\boldsymbol{x}_k$ almost everywhere over $\mathbb{R}^p$. We note that $\mathcal{P}_R$ still selects his/her strategies from Γ_k, $k = 1,\dots,n$.

The above is a general framework for noncooperative game formulations between $\mathcal{P}_S$ and $\mathcal{P}_R$, which permits analysis of the equilibrium achieving signaling rules in the most general form. By adjusting the matrices, it is possible to generate many different examples of stochastic control/game problems in strategic environments.

Example 2.2. As one example, there can be two separate controlled stochastic processes:

$$\underbrace{\begin{bmatrix} \boldsymbol{z}_{k+1} \\ \boldsymbol{\theta}_{k+1} \end{bmatrix}}_{=\boldsymbol{x}_{k+1}} = \underbrace{\begin{bmatrix} A_z & \\ & A_\theta \end{bmatrix}}_{=A} \underbrace{\begin{bmatrix} \boldsymbol{z}_k \\ \boldsymbol{\theta}_k \end{bmatrix}}_{=\boldsymbol{x}_k} + \underbrace{\begin{bmatrix} B_z \\ B_\theta \end{bmatrix}}_{=B} \boldsymbol{u}_k + \underbrace{\begin{bmatrix} \boldsymbol{\omega}_k \\ \boldsymbol{\nu}_k \end{bmatrix}}_{=\boldsymbol{w}_k}.$$

$\mathcal{P}_R$ seeks to drive $\boldsymbol{z}_k$ into his/her desired path, but the control variable $\boldsymbol{u}_k$ has also impact on the state $\boldsymbol{\theta}_k$ and $\mathcal{P}_S$ designs the measurement signals so that $\boldsymbol{\theta}_k$ is driven into his own desired path not in line with $\mathcal{P}_R$'s actual intent. In particular, in the objective functions, $Q_{S,k} = \begin{bmatrix} O & O \\ O & Q_{\theta,k} \end{bmatrix}$ and $Q_{R,k} = \begin{bmatrix} Q_{z,k} & O \\ O & O \end{bmatrix}$ and $\mathcal{P}_R$ seeks to minimize

$$\mathbb{E}\left\{\sum_{k=1}^{n} \boldsymbol{z}_{k+1}' Q_{z,k+1} \boldsymbol{z}_{k+1} + \boldsymbol{u}_k' R_{R,k} \boldsymbol{u}_k\right\}, \tag{2.35}$$

while $\mathcal{P}_S$ seeks to minimize

$$\mathbb{E}\left\{\sum_{k=1}^{n} \boldsymbol{\theta}_{k+1}' Q_{\theta,k+1} \boldsymbol{\theta}_{k+1} + \boldsymbol{u}_k' R_{S,k} \boldsymbol{u}_k\right\}.$$

Example 2.3. Another special case is one where while $\mathcal{P}_R$ seeks to drive $\boldsymbol{z}_k$ into his/her desired path, $\mathcal{P}_S$ wants $\boldsymbol{z}_k$ to track an exogenous process $\boldsymbol{\theta}_k$, i.e., $B_\theta = O$. Then, $\mathcal{P}_S$'s cost function is given by

$$\sum_{k=1}^{n} (\boldsymbol{z}_{k+1} - D_{k+1}\boldsymbol{\theta}_{k+1})' Q_{\theta,k+1} (\boldsymbol{z}_{k+1} - D_{k+1}\boldsymbol{\theta}_{k+1}) + \boldsymbol{u}_k' R_{S,k} \boldsymbol{u}_k$$

and this corresponds to $Q_{S,k} = \begin{bmatrix} I \\ -D_k' \end{bmatrix} Q_{\theta,k} \begin{bmatrix} I & -D_k \end{bmatrix}$ in (2.34), while $\mathcal{P}_R$'s cost function is given by (2.35).

In order to address the hierarchical signaling in noncooperative control scenarios, rather routinely by completing the squares [63], for $j = S, R$, we can write (2.34) as

$$\sum_{k=1}^{n} \mathbb{E}\{\boldsymbol{x}_{k+1}' Q_{j,k+1} \boldsymbol{x}_{k+1} + \boldsymbol{u}_k' R_{j,k} \boldsymbol{u}_k\} = \sum_{k=1}^{n} \mathbb{E}\left\{\|\boldsymbol{u}_k + K_{j,k}\boldsymbol{x}_k\|_{\Delta_{j,k}}^2\right\} + \Delta_{j,0}, \tag{2.36}$$

where[11] $K_{j,k} = \Delta_{j,k}^{-1} B' \tilde{Q}_{j,k+1} A$, $\Delta_{j,k} = B' \tilde{Q}_{j,k+1} B + R_{j,k}$,

$$\begin{aligned} \tilde{Q}_{j,k} &= Q_{j,k} + A'(\tilde{Q}_{j,k+1} - \tilde{Q}_{j,k+1} B \Delta_{j,k}^{-1} B' \tilde{Q}_{j,k+1}) A \\ \tilde{Q}_{j,n+1} &= Q_{j,n+1},\ \Delta_{j,0} = \mathrm{Tr}\{\tilde{Q}_{j,1}\Sigma_1\} + \sum_{k=1}^{n} \mathrm{Tr}\{\tilde{Q}_{j,k+1}\Sigma_w\}, \end{aligned} \tag{2.37}$$

and set $Q_{j,1} = O$. Then, through a routine change of variables,

$$\sum_{k=1}^{n} \mathbb{E}\left\{\|\boldsymbol{u}_k + K_{j,k}\boldsymbol{x}_k\|_{\Delta_{j,k}}^2\right\} = \sum_{k=1}^{n} \mathbb{E}\left\{\|\boldsymbol{u}_{j,k} + K_{j,k}\boldsymbol{x}_k^o\|_{\Delta_{j,k}}^2\right\}, \tag{2.38}$$

where $\boldsymbol{u}_{j,k} = \boldsymbol{u}_k + K_{j,k} B \boldsymbol{u}_{k-1} + \ldots + K_{j,k} A^{k-2} B \boldsymbol{u}_1$ and

$$\boldsymbol{x}_{k+1}^o = A\boldsymbol{x}_k^o + \boldsymbol{w}_k. \tag{2.39}$$

Remark. In the cooperative settings, (2.38) would imply that the optimal control can be computed via the solution for the sub-cost function $\mathbb{E}\{\|\boldsymbol{u}_{R,k} + K_{R,k}\boldsymbol{x}_k^o\|_{\Delta_{R,k}}^2\}$. As an example, we would have $\boldsymbol{u}_{R,1}^* = -K_{R,1}\mathbb{E}\{\boldsymbol{x}_1^o | \boldsymbol{y}_1^\ell\}$ and $\boldsymbol{u}_{R,2}^* = -K_{R,2}\mathbb{E}\{\boldsymbol{x}_2^o | \boldsymbol{y}_1^\ell, \boldsymbol{y}_2^\ell\}$, and correspondingly, the optimal control inputs would be given by $\boldsymbol{u}_1^* = \boldsymbol{u}_{R,1}^*$ and $\boldsymbol{u}_2^* = \boldsymbol{u}_{R,2}^* - K_{R,1}\boldsymbol{u}_{R,1}^*$, almost everywhere over $\mathbb{R}^t$. However, in the noncooperative settings, even though the control-free process $\{\boldsymbol{x}_k^o\}$ is independent of how the control inputs $\boldsymbol{u}_k$'s are constructed, the sensor outputs $\boldsymbol{y}_k^\ell$ depend on the state $\boldsymbol{x}_k$ and correspondingly on the previous control inputs $\boldsymbol{u}_{1:k-1}$. Therefore, while constructing the control inputs in the noncooperative settings, $\mathcal{P}_R$ should also consider their impact on the future stages, as also pointed out in the remark above.

However, the following lemma shows that $\mathcal{P}_R$ cannot influence how $\mathcal{P}_S$

[11] The assumption $R_{j,k} \succ O$ ensures that $\Delta_{j,k}$ is non-singular.

selects his/her linear signaling rules strategically.

Lemma 2.6. *For a controlled Gauss-Markov process $\{\boldsymbol{x}_k\}$ evolving according to* (2.1) *and the control-free state $\{\boldsymbol{x}_k^o\}$ evolving according to* (2.39)*, we have*

$$\mathbb{E}\{\boldsymbol{x}_k^o | L_1'\boldsymbol{x}_1, \ldots, L_k'\boldsymbol{x}_k\} = \mathbb{E}\{\boldsymbol{x}_k^o | L_1'\boldsymbol{x}_1^o, \ldots, L_k'\boldsymbol{x}_k^o\}, \tag{2.40}$$

where $L_j \in \mathbb{R}^{p\times p}$, $j = 1, \ldots, k$.

Proof. By (2.39), the linear signaling rule yields

$$L_k'\boldsymbol{x}_k = L_k'\boldsymbol{x}_k^o + \underbrace{L_k'B\boldsymbol{u}_{k-1} + \ldots + L_k'A^{k-2}B\boldsymbol{u}_1}, \tag{2.41}$$

almost everywhere over $\mathbb{R}^p$, where the under-braced term is σ-$\boldsymbol{y}_{1:k-1}^{\ell}$ measurable for all $k = 1, \ldots, n$, which implies (2.40). However, this would not necessarily be the case for nonlinear signaling rules in general since the previous control inputs could *limit* the informativeness of the current signal. □ □

Based on Lemma 2.6, the problem faced by $\mathcal{P}_S$, i.e., (2.38), is just a strategic information disclosure problem. Therefore, after some algebra, similar to the lines followed in Section 2.2, the problem can also be written as an affine function of $H_k^o := \mathbb{E}\{\hat{\boldsymbol{x}}_k^o(\hat{\boldsymbol{x}}_k^o)'\}$, where $\hat{\boldsymbol{x}}_k^o := \mathbb{E}\{\boldsymbol{x}_k^o | \boldsymbol{y}_{1:k}^{\ell}\}$, as follows:

$$\min_{\substack{\eta_k\in\Omega_k,\\ k=1,\ldots,n}} \sum_{k=1}^{n} \mathrm{Tr}\{V_k^o H_k^o\} + \Xi_o, \tag{2.42}$$

for certain symmetric deterministic matrices $V_k^o \in \mathbb{R}^{p\times p}$, $k = 1, \ldots, n$, which are given by

$$V_k^o := \Xi_{k,k} + \sum_{l=k+1}^{n} \Xi_{k,l}A^{l-k} + (A^{l-k})'\Xi_{l,k}, \tag{2.43}$$

and $\Xi_{k,l}$ is the corresponding $p \times p$ sub-block of Ξ, which is given by

$$\Xi := T_S'\Delta_S T_S - T_S'\Delta_S K_S - K_S'\Delta_S T_S \tag{2.44}$$

$$\Xi_o := \mathrm{Tr}\{\Sigma^o K_S'\Delta_S K_S\} + \Delta_{S,0}, \tag{2.45}$$

where $\Sigma^o := \mathbb{E}\{\boldsymbol{x}^o(\boldsymbol{x}^o)'\}$, $\boldsymbol{x}^o := \begin{bmatrix} \boldsymbol{x}_n^o & \cdots & \boldsymbol{x}_1^o \end{bmatrix}'$, $T_S := \Phi_S \Phi_R^{-1} K_R$, and

$$\Phi_j := \begin{bmatrix} I & K_{j,n}B & K_{j,n}AB & \cdots & K_{j,n}A^{n-2}B \\ & I & K_{j,n-1}B & \cdots & K_{j,n-1}A^{n-3}B \\ & & I & \cdots & K_{j,n-2}A^{n-4}B \\ & & & \ddots & \\ & & & & I \end{bmatrix}, \tag{2.46}$$

$$K_j := \begin{bmatrix} K_{j,n} & & \\ & \ddots & \\ & & K_{j,1} \end{bmatrix}, \Delta_j := \begin{bmatrix} \Delta_{j,n} & & \\ & \ddots & \\ & & \Delta_{j,1} \end{bmatrix}, \tag{2.47}$$

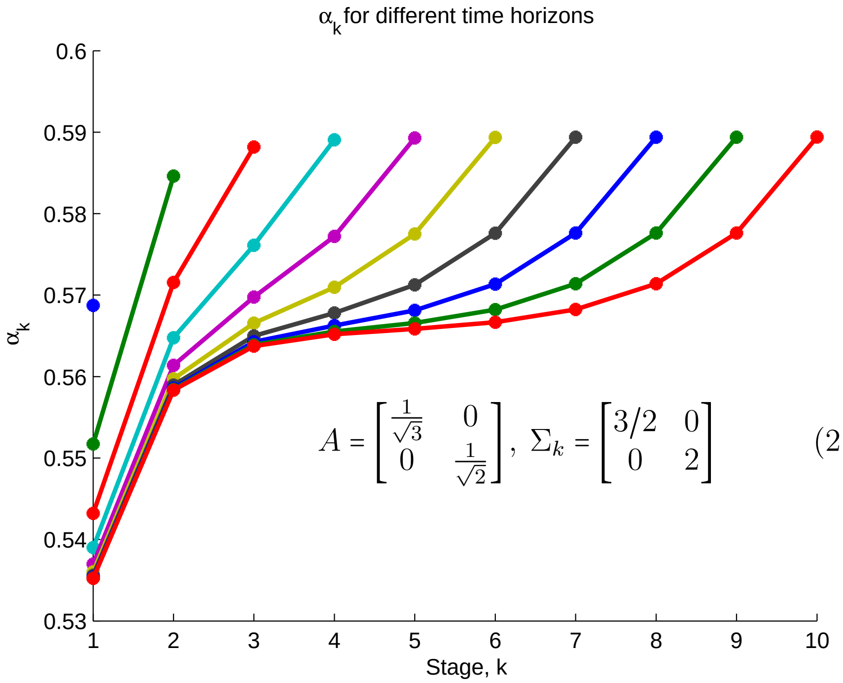
for $j = S, R$. Then, Theorems 2.2 and 2.5 show that given V_k's, we can compute the optimal linear signaling rules via Algorithm 2.1. In the following corollary of these theorems, we recap the results.

Corollary 2.7. *We can compute the optimal linear signaling rules in non-cooperative control settings by computing* (2.43) *based on* (2.37) *and* (2.44)-(2.47)*, and then applying Algorithm 2.1 for* (2.42)*.*

2.6 Illustrative Examples

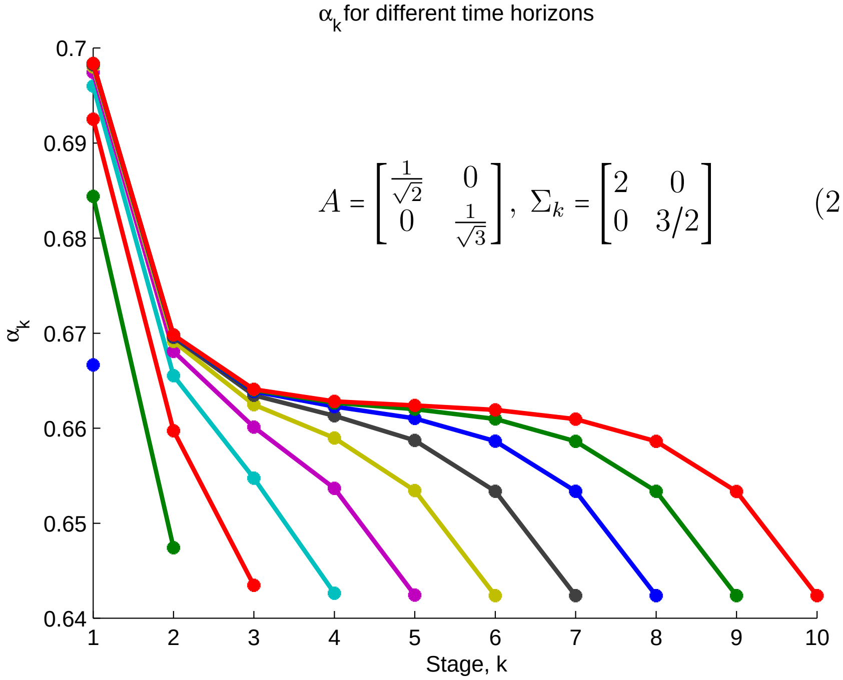
As numerical illustrations of Algorithm 2.1, we consider Example 2.1 in strategic communication formulation with cost functions (2.8) and (2.9), where $\boldsymbol{z}_k \in \mathbb{R}$, $\boldsymbol{\theta}_k \in \mathbb{R}$, and $D_k = 1$. We consider two different scenarios: Scenario 1, where the process $\{\boldsymbol{z}_k\}$ is relatively more colored, i.e., more correlated in time, than the process $\{\boldsymbol{\theta}_k\}$, and Scenario 2, where the process $\{\boldsymbol{\theta}_k\}$ is more colored. To this end, we set Σ_k and A as in (2.48) and (2.49), introduced as parts of Figs. 2.4 and 2.5, respectively, which yields that the underlying state process $\{\boldsymbol{x}_k \in \mathbb{R}^2\}$ is stationary and $\Sigma_w = I$.

We can compute the equilibrium achieving sender policies via Algorithm 2.1. After the computation, we observe that the resulting weight matrices $L_k \in \mathbb{R}^{2\times 2}$, $\forall k$, have rank 1, and indeed have a column that is full of zeros. Therefore, we can consider that at stage k, $\mathcal{P}_S$ sends practically a scalar which is a linear combination of $\boldsymbol{z}_k$ and $\boldsymbol{\theta}_k$ to R. Additionally, we can scale that sent signal by multiplying it with a certain constant such that the weight



$$A = \begin{bmatrix} \frac{1}{\sqrt{3}} & 0 \\ 0 & \frac{1}{\sqrt{2}} \end{bmatrix}, \ \Sigma_k = \begin{bmatrix} 3/2 & 0 \\ 0 & 2 \end{bmatrix} \tag{2.48}$$

Figure 2.4: Scenario 1: the process $\{\boldsymbol{z}_k\}$ is relatively less colored, i.e., less correlated in time, than the process $\{\boldsymbol{\theta}_k\}$.



$$A = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{3}} \end{bmatrix}, \ \Sigma_k = \begin{bmatrix} 2 & 0 \\ 0 & 3/2 \end{bmatrix} \tag{2.49}$$

Figure 2.5: Scenario 2: the process $\{\boldsymbol{z}_k\}$ is relatively more colored.

$$A = \begin{bmatrix} \frac{1}{\sqrt{3}} & 0 \\ 0 & \frac{1}{\sqrt{2}} \end{bmatrix}, \ B = \begin{bmatrix} 2 \\ -\frac{1}{2} \end{bmatrix}, \ \Sigma_k^o = \begin{bmatrix} 3/2 & 0 \\ 0 & 2 \end{bmatrix} \qquad (2.50)$$

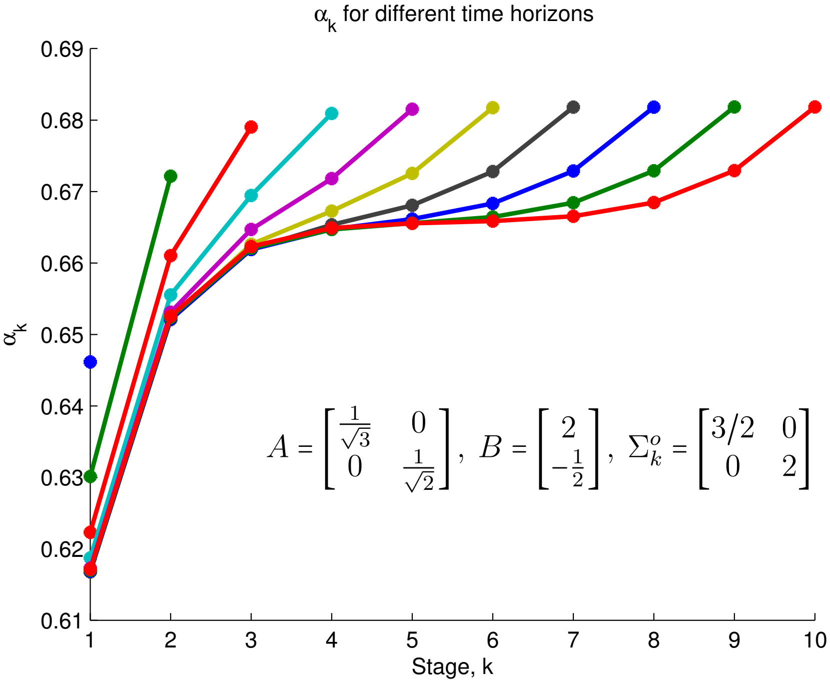
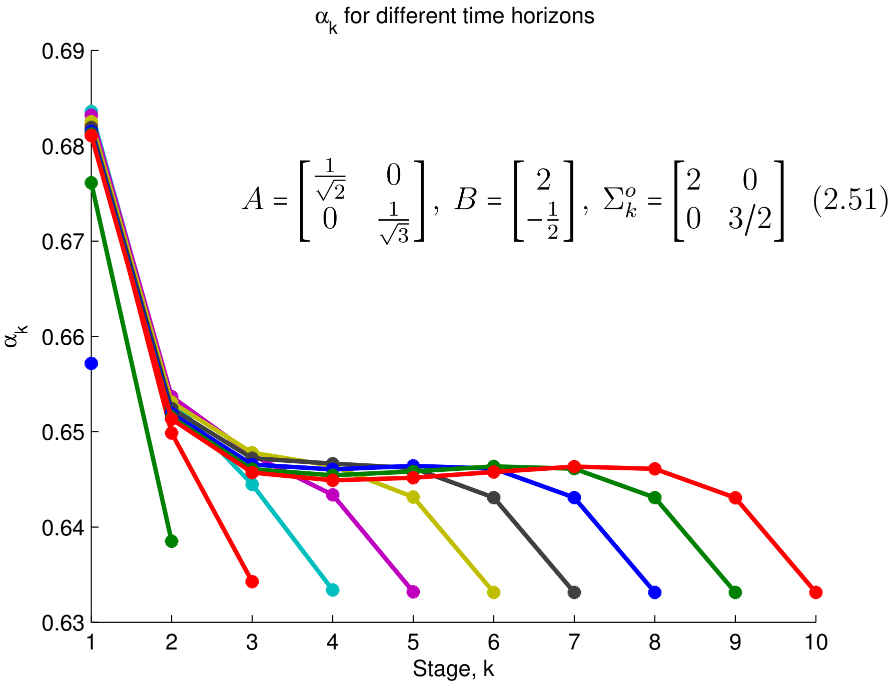


Figure 2.6: Scenario 3: the process $\{\boldsymbol{z}_k\}$ is relatively less colored in noncooperative control.

of $\boldsymbol{z}_k$ in the message is just 1. In particular, the sent signal can be written as $\boldsymbol{y}_k = \boldsymbol{z}_k + \alpha_k \boldsymbol{\theta}_k$ for a certain constant $\alpha_k \in \mathbb{R}$. In Figs. 2.4 and 2.5, we plot the time evolution of α_k for different time horizons, e.g., $n = 1, \dots, 10$, in the Scenarios 1 and 2, respectively. We observe that the weight of $\boldsymbol{z}_k$ and $\boldsymbol{\theta}_k$ increases or decreases in time depending on their relative correlatedness in time. As an example, in Scenario 1, the process $\{\boldsymbol{\theta}_k\}$ is relatively more colored than the process $\{\boldsymbol{z}_k\}$ and the weight of $\boldsymbol{\theta}_k$, i.e., α_k, in the sent messages increases in time compared to the weight of $\boldsymbol{z}_k$, i.e., 1. Additionally, the pattern that the weight α_k draws as the length of time horizon grows provides an insight for the equilibrium achieving sender policies for stationary state processes in infinite time horizon, e.g., after a transient phase, the weights could reach a steady state value as $n \to \infty$.

Furthermore, we also consider Example 2.3 within the noncooperative control formulation, where $\boldsymbol{z}_k \in \mathbb{R}$, $\boldsymbol{\theta}_k \in \mathbb{R}$, and $D_k = 1$. Different from the previous illustrative examples, here, $B = \begin{bmatrix} 2 \\ -1/2 \end{bmatrix}$ and similar to Scenarios 1 and 2, we consider two new scenarios: Scenario 3, where the process $\{\boldsymbol{z}_k\}$ is relatively more colored than the process $\{\boldsymbol{\theta}_k\}$, and Scenario 4, where the process



$$A = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{3}} \end{bmatrix}, \; B = \begin{bmatrix} 2 \\ -\frac{1}{2} \end{bmatrix}, \; \Sigma_k^o = \begin{bmatrix} 2 & 0 \\ 0 & 3/2 \end{bmatrix} \quad (2.51)$$

Figure 2.7: Scenario 4: the process $\{\boldsymbol{z}_k\}$ is relatively more colored in noncooperative control.

$\{\boldsymbol{\theta}_k\}$ is more colored. To this end, we set $Q_{\theta,k} = Q_{z,k} = R_{S,k} = R_{R,k} = 1$, and A, B, and Σ_k^o as in (2.50) and (2.51), introduced as parts of Figs. 2.6 and 2.7, respectively, which yields that the underlying control-free state process $\{\boldsymbol{x}_k \in \mathbb{R}^2\}$, introduced in (2.39), is stationary and $\Sigma_w = I$. Similar to Scenarios 1 and 2, we also observe that all the optimal weight matrices $L_k \in \mathbb{R}^{2\times 2}$ have rank 1 and $\mathcal{P}_S$ practically sends a scalar variable. Therefore, in Figs. 2.6 and 2.7, we plot the change of α_k within various time horizons, where $\boldsymbol{y}_k = \boldsymbol{z}_k + \alpha_k \boldsymbol{\theta}_k$. We also note that the evolution of α_k is very much also dependent on B in addition to the relative colorfulness of the processes $\{\boldsymbol{z}_k\}$ and $\{\boldsymbol{\theta}_k\}$.

2.7 Concluding Remarks

In this chapter, we have addressed the existence and characterization of the equilibrium achieving sender strategies in hierarchical signaling games with finite horizon, for quadratic objective functions and multivariate Gaussian processes. Our main conclusion has been that linear sender and receiver strategies can yield the equilibrium within the general class of policies in strategic communication scenarios. This settles an open question on the structure of equilibrium achieving policies in dynamic strategic information transmission within a Stackelberg game framework. We have observed that independence of uncorrelated Gaussian parameters plays a significant role in the optimality of linear signaling rules. Furthermore, Gaussian distribution is the best distribution serving the deceptive sender's objectives. We have also provided algorithms to compute optimal linear strategies numerically with global optimality guarantees in noncooperative communication and control scenarios.

Some future directions of research on this topic include characterization of the equilibrium achieving strategies in closed forms, and analysis of equilibrium under information-regularization constraints.

3

ROBUST SENSOR DESIGN

Always mystify, mislead and surprise the enemy, if possible.
– General Thomas J. "Stonewall" Jackson

Cyber connectedness of physical systems makes them vulnerable against cyber attacks which could have undesirable physical outcomes, e.g., damages [66,67]. Different from the vulnerability of computer systems in a cyber network, cyber connectedness of physical systems brings in new and distinct security challenges due to the inherent physical dynamics. Cyber attacks can be very strategic while disturbing the system to achieve a certain malicious goal and therefore they differ from external disturbances that can be modeled, e.g., statistically or within certain bounds, for robust control system design. Cyber attacks can be advanced and very target specific by learning the system's dynamics and tuning their attack specific to the underlying system and the existing defensive measures for success and stealthiness. To cite a recent occurrence of such an event, in 2014, Dragonfly Malware intervened the operation of many cyber-physical, e.g., process control, systems in energy and pharmaceutical industries across the world over a long period of time without being detected [68]. Therefore, it is crucial that we develop novel security mechanisms against such attackers for the security of cyber-physical systems.

Prior Literature In a physical system, advance attackers can seek to evade detection mechanisms by manipulating the physical signals used by the detectors. For example, in [69], the authors have introduced false data injection attacks, where the attackers can inject data into the sensor outputs, in the context of state estimation, and characterized undetectable attacks. The ensuing studies mainly focused on characterizing the vulnerabilities of control systems against such evasive attacks and designing counter measures to be able to detect them. In [70], the authors have introduced replay attacks where the attacker records and replays the sensor outputs when the system is at steady state since they are expected to be similar. As a counter measure, an independent signal can be injected into the control input to detect such attacks at the expense of degradation in control performance [70, 71]. In [72, 73], the authors have characterized the reachable set that an evasive attacker can drive the system by injecting data into sensor outputs and control inputs jointly.

Within deterministic control scenarios, in [74], the authors have analyzed open-loop stealthy attacks, and proposed to add new measurements as a counter measure, as in [70]. In [75], the authors have formulated the limitations of monitoring-based detection mechanisms against false data injection and replay attacks. In [76], the authors have proposed decoding schemes to estimate the state based on sensor outputs while a subset of them could have been under attack. The attackers can also have adversarial control objectives. In [77, 78], the authors have analyzed such attacks, where the attacker seeks to drive the state of the system according to his adversarial goal evasively by manipulating sensor outputs and control inputs jointly. In [79], the authors have analyzed optimal attack strategies to maximize the quadratic cost of a system with linear Gaussian dynamics without being detected. In [80], the authors have proposed linear encoding schemes for sensor outputs of an LQG system in order to enhance detectability of false data injection attacks while the encoding matrix is assumed oblivious to the attackers.

Motivation We address, in this chapter, primarily the following two questions: “If we have already designed the sensor outputs, in a non-Bayesian setting, to what extent would we have secured the system against multiple type advanced and evasive attackers who can bypass/hijack the defensive measures to fulfill a certain malicious control objective?” And “what would be the best affine sensor outputs that can deceive such attackers about the underlying state of the system so that their actions/attacks would not lead to any degradation?” We consider attackers who have malicious control objectives misaligned with the normal operation of the system, but not completely opposite of it as in the framework of a zero-sum game. This implies that there is a part of the malicious objective that is benign. Correspondingly, the attacker would be acting in line with the normal operation of the system with respect to the aligned part of his objective. Our motivation is to restrain the attacker’s abilities so that he/she will not act along the misaligned part of the objectives while taking actions in line with the aligned part. To this end, we propose to design the information available to an attacker strategically since the attacker would be making decisions to fulfill a malicious objective based on the information available to him/her. By designing the sensor outputs strategically, our goal is to control the attacker's perception about the underlying system, and correspondingly to persuade the attacker (without any explicit enforcement) to fulfill the aligned part of the objectives as much as possible without fulfilling the misaligned part.

We have partially addressed this challenge in Chapter 2 in non-cooperative communication settings. For a discrete-time Gauss-Markov process, and when the sender and the receiver have misaligned quadratic objectives, we have shown the optimality of linear signaling rules within the general class of measurable policies and provided an algorithm to compute the optimal policies numerically. This chapter differs from Chapter 2 in the sense that it addresses optimal linear plus noise signaling for the scenarios where the distribution over the private type of the controller is not known. Furthermore here we provide a comprehensive formulation by considering also the cases where the sensor could have partial or noisy information on the signal of interest and relevance. Further details on this will be given next as part of our description of the main contributions of this work, as well as throughout the chapter.

Contributions of This Chapter To obtain explicit results, we specifically consider systems with linear Gaussian dynamics and quadratic control objectives, which have various industrial applications [79] from manufacturing processes to aerospace control. We consider the possibility of adversarial intervention by multiple advanced and evasive attackers across control networks. The attackers have different long-term control objectives. Due to the stochastic nature of the problem, i.e., due to the presence of state noise, any open-loop control strategy of an attacker could not drive the system along his desired path effectively. Therefore, regardless of whether the controller has an adversarial objective or not, it has to generate a closed-loop control input using the designed sensor outputs. We also consider the scenarios where the advanced attackers could learn the relationship between the sensor output and the state, i.e., the designed signaling rule, in order to avoid any obscurity based defense, which can be bypassed once the advanced attacker learns the information in obscurity. This implies that the interaction between the sensor and the attackers could be modeled as a hierarchical dynamic game [3], where the sensor leads the game by announcing its strategy in advance. Therefore, while designing the sensor outputs, we should consider the possibility of malicious or benign control inputs and defend against the worst possible distribution over them.

Specifically, we seek to determine optimal *affine* sensor strategies for controlled Gauss-Markov processes, where the sensor can have partial or noisy measurements. We only consider affine signaling rules, since under such rules our setting entails a classical information model, whereas without such a structural restriction on the signaling rules, the underlying model features a non-classical information due to the asymmetry of information between the players and the dynamic interaction through closed-loop feedback signals. The follower, i.e., the attacker, has a private type while the distribution over the types is not known by the leader, i.e., the sensor. Our goal is to defend against the worst possible distribution over these types. To this end, we provide an equivalent problem faced by the sensor in terms of the covariance of the posterior estimate of the (control-free) state by formulating necessary and sufficient conditions on that covariance matrix. This new equivalent problem is linear in the optimization argument with a compact and convex constraint set.

We emphasize that what we have is an exact equivalence relation. Based on this exact equivalence relation, we can provide an offline algorithm to compute the optimal affine sensor strategies. In particular, in order to determine the best signaling rule against multiple types of attackers, we introduce additional constraints on the equivalent problem, which implies that the equivalence in optimality is not a sufficient condition in that respect. We had noted earlier for multiple attack types with *known* distribution over them that the optimum can be attained at the extreme points of the constraint set [39, 40] since the equivalent problem is linear in the optimization argument and the constraint set is compact and convex [81]. And, further the corresponding covariance matrices could be attained through certain *linear* signaling rules, where the sensor does not introduce any additional independent noise. However, when we defend against multiple types of attackers with the worst possible distribution over them as here, the new problem imposes additional linear constraints on the equivalent problem. With these new constraints, even though the optimum will be attained at the extreme points of this modified constraint set, there can be cases where the optimum may be attained only at non-extreme points of the original constraint set before the modification. Such covariance matrices could be attained through certain linear-plus-noise signaling rules.

We now list the main contributions of this chapter as follows:

- We introduce a robust sensor design agent that can craft the measurements sent to the noiseless communication network in order to defend against *multiple* advanced and evasive attackers with long-term control objectives that are *misaligned* with the normal operation of the system.
- We show the optimality of *memoryless* signaling rules within the general class of signaling rules with complete/bounded memory when the sensor has access to the underlying state of the system.
- We show that the optimal signaling rule dictates the sensor to possibly introduce additive independent noise into the sensor outputs if there are multiple types of attackers.
- We extend the results to the cases where the sensor has partial or *noisy* information on the signal of interest and relevance.

The chapter is organized as follows: In Section 3.1, we formulate the robust sensor design game. In Section 3.2, we analyze the equilibrium of the robust sensor design game under perfect measurements. In Section 3.3, we extend the results to the cases where there are partial or noisy measurements. In Section 3.4, we examine numerically the performance of the proposed scheme for various scenarios. We conclude the chapter in Section 3.5 with several remarks and possible research directions.

3.1 Problem Formulation

Consider a cyber-physical control system, seen in Fig. 3.1, whose underlying state dynamics and sensor measurements are described, respectively, by:

$$\boldsymbol{x}_{k+1} = A\boldsymbol{x}_k + B\boldsymbol{u}_k + \boldsymbol{w}_k, \tag{3.1}$$

$$\boldsymbol{y}_k = C\boldsymbol{x}_k + \boldsymbol{v}_k, \tag{3.2}$$

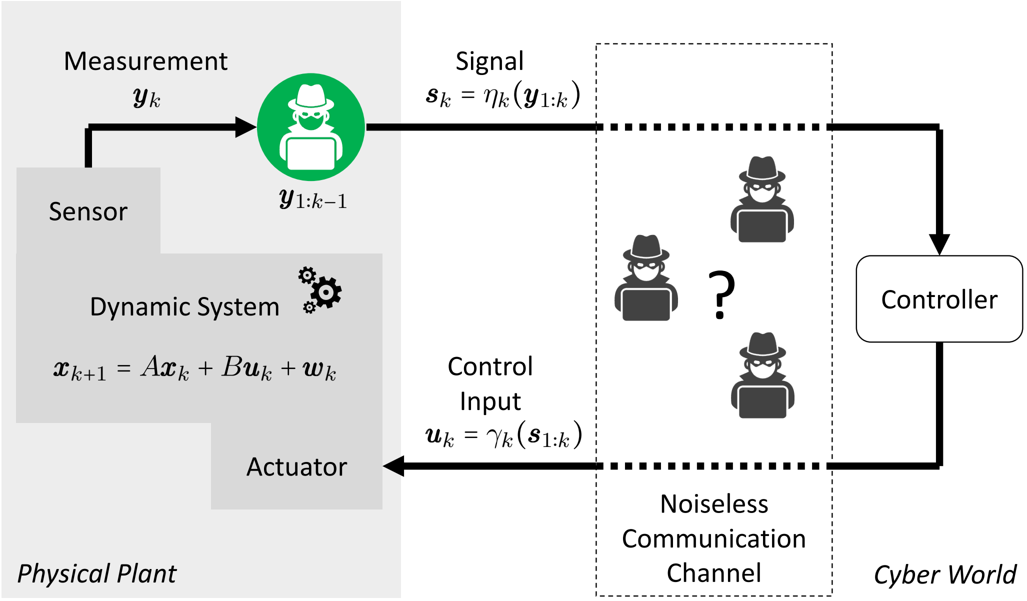


Figure 3.1: Cyber-physical systems equipped with sensor design component in the physical part as a deceptive defense mechanism against advanced evasive attackers who can intervene through the noiseless communication channel, e.g, controller area network (CAN bus) in a vehicle.

for $k = 1,\ldots,\kappa$, where[1] $A \in \mathbb{R}^{m\times m}, B \in \mathbb{R}^{m\times r}$, and $C \in \mathbb{R}^{m\times m}$, and the initial state $\boldsymbol{x}_1 \sim \mathcal{N}(0,\Sigma_1)$. The additive state and measurement noise sequences $\{\boldsymbol{w}_k\}$ and $\{\boldsymbol{v}_k\}$, respectively, are white Gaussian vector processes, i.e., $\boldsymbol{w}_k \sim \mathcal{N}(0,\Sigma_w)$ and $\boldsymbol{v}_k \sim \mathcal{N}(0,\Sigma_v)$; and are independent of the initial state $\boldsymbol{x}_1$ and of each other. As seen in Fig. 3.1, the signal $\boldsymbol{s}_k \in \mathbb{R}^m$, which can be different from the measurement $\boldsymbol{y}_k \in \mathbb{R}^m$, is given by the affine signaling rule:

$$\boldsymbol{s}_k = \eta_k(\boldsymbol{y}_{1:k}) \tag{3.3}$$

$$= L'_{k,k}\boldsymbol{y}_k + \ldots + L'_{k,1}\boldsymbol{y}_1 + \boldsymbol{n}_k, \tag{3.4}$$

where $L_{k,j} \in \mathbb{R}^{m\times m}$, $j = 1,\ldots,k$, can be any deterministic matrix, and $\boldsymbol{n}_k \sim \mathcal{N}(0,\Theta_k)$ is independent of every other parameter. Let Υ_k denote the set of such affine signaling rules from $\mathbb{R}^{mk}$ to $\mathbb{R}^m$, i.e., $\eta_k \in \Upsilon_k$. Furthermore, the closed-loop control input $\boldsymbol{u}_k \in \mathbb{R}^r$, which is constructed by the controller

[1] Even though we consider time invariant matrices A, B, and C, for notational simplicity, the provided results could be extended to time-variant cases rather routinely. Furthermore, we consider all the random parameters to have zero mean; however, the derivations can be extended to non-zero mean case in a straightforward way.

located in the cyber-part of the system, is given by

$$\boldsymbol{u}_k = \gamma_k(\boldsymbol{s}_{1:k}), \tag{3.5}$$

almost everywhere over $\mathbb{R}^r$, where $\gamma_k(\cdot)$ can be any Borel measurable function from $\mathbb{R}^{mk}$ to $\mathbb{R}^r$. Let Γ_k denote the set of all Borel measurable functions from $\mathbb{R}^{mk}$ to $\mathbb{R}^r$, i.e., $\gamma_k \in \Gamma_k$.

Particularly, the dynamic system, measurement system, and actuators are located in the physical part while the controller is located in the cyber part through a connection over a noiseless communication channel. However, the connectivity over the channel is vulnerable to cyber attacks. We consider the scenarios where advanced and evasive attackers can intervene through the channel by injecting malicious control inputs to drive the underlying state according to a malicious long-term control objective and can bypass or hijack the detection-based defensive measures. Our goal is to produce defense against such advanced evasive attacks by *crafting* the attacker's perceptions about the underlying state of the system strategically so that their actions/attacks would not be harmful (to the extent possible) and would be along the desired objectives. To this end, we introduce a robust-secure-sensor-design component, denoted by $\mathcal{P}_S$, in the physical plant that gets the sensor measurement $\boldsymbol{y}_k$ as an input and constructs the signal $\boldsymbol{s}_k$, given by (3.3), and feeds this signal to the noiseless communication channel. Even if there is an attacker intervening over the channel, that attacker can only access that signal $\boldsymbol{s}_k$ related to the underlying state of the system.

Remark (Sensor Placement). Note that if the signal $\boldsymbol{s}_k$ is memoryless, then $\boldsymbol{s}_k \in \mathbb{R}^m$ can be written as

$$\begin{aligned} \boldsymbol{s}_k &= \underbrace{L'_{k,k}C}\,\boldsymbol{x}_k + \underbrace{L'_{k,k}\boldsymbol{v}_k + \boldsymbol{n}_k} \\ &= \tilde{C}_k\boldsymbol{x}_k + \boldsymbol{t}v_k, \end{aligned}$$

where $\boldsymbol{t}v_k \sim \mathcal{N}(0, L'_{k,k}\Sigma_v L_{k,k} + \Theta_k)$, such that $\tilde{C}_k \in \mathbb{R}^{m\times m}$ is the gain matrix in the measurement while $\boldsymbol{t}v_k$ is the white Gaussian measurement noise. Therefore, the optimal signaling rules $\eta^*_{1:\kappa}$ can provide a guideline to engineer (or designer) the placement of the physical sensors to monitor the underlying state of the system securely or to assess the resiliency against attacks with long-term control objectives.

The normal operation of the system, i.e., when there is no adversarial intervention by the attackers, is a stochastic control setting, where the controller, denoted by $\mathcal{P}_C$, constructs the control inputs $\boldsymbol{u}_k \in \Gamma_k$ to minimize a finite horizon quadratic cost function given by

$$\mathbb{E}\left\{\sum_{k=1}^{\kappa} \|\boldsymbol{x}_{k+1}\|_Q^2 + \|\boldsymbol{u}_k\|_R^2\right\}, \tag{3.6}$$

where[2] $Q \in \mathbb{S}^m$ is positive-semi definite and $R \in \mathbb{S}_+^r$ is positive definite. $\mathcal{P}_S$ selects the signaling rule $\eta_{1:\kappa}$ to minimize the same cost function with $\mathcal{P}_C$, i.e., (3.6), as a team. And if there were no possibility for an adversarial intervention, $\mathcal{P}_S$ could be as informative as disclosing the measurement directly to $\mathcal{P}_C$ since there is no cost for the disclosed information over the noiseless communication channel. However, as seen in Fig. 3.1, there can be advanced and evasive adversarial interventions in the noiseless communication channel between the dynamic system and $\mathcal{P}_C$. We particularly consider multiple (finitely many) types of attackers who can inject malicious closed-loop control inputs with long-term control objectives. Let type-α attacker's cost function be given by

$$\mathbb{E}\left\{\sum_{k=1}^{\kappa} \|\boldsymbol{x}_{k+1}\|_{Q_\alpha}^2 + \|\boldsymbol{u}_k\|_{R_\alpha}^2\right\}, \tag{3.7}$$

where $Q_\alpha \in \mathbb{S}^m$ is positive semi-definite and $R_\alpha \in \mathbb{S}^r$ is positive-definite.

Example 3.1 (A Special Case). The attacker objective (3.7) also covers the special cases where the attacker seeks to regularize the underlying state $\{\boldsymbol{x}_k\}$ around an external process, e.g., $\{\boldsymbol{z}_k^\alpha\}$, rather than the zero vector. To this end, we can consider the augmented state vector $\begin{bmatrix}\boldsymbol{x}_k' & (\boldsymbol{z}_k^\alpha)'\end{bmatrix}'$ and set the associated weight matrix in the regularization, i.e., Q_α in (3.7), accordingly.

Since our aim is to defend against advanced and evasive attackers, we consider the scenarios where there exists a hierarchy between the defender, i.e., $\mathcal{P}_S$, and the attackers such that each type of attacker is aware of $\mathcal{P}_S$'s signaling rules $\eta_{1:\kappa}$ by testing and learning the system's dynamics once they are deployed publicly. Different from [34,39,40], in this chapter, $\mathcal{P}_S$ does not know the underlying distribution governing the attackers' types and seeks

[2] For notational simplicity, we consider time-invariant Q and R. However, the results provided could be extended to the general time-variant case rather routinely.

to defend against the worst possible distribution. Particularly, $\mathcal{P}_S$ designs the secure sensor outputs such that $\mathcal{P}_S$'s cost is minimized in expectation with respect to the worst possible *true* distribution of types within a robust setting.

Remark (Game-theoretic View)*.* This can be viewed as a game, where $\mathcal{P}_S$ designs the signaling rule $\eta_{1:\kappa}$ within a hierarchical setting, where the controllers, $\mathcal{P}_C$ with different benign/malicious types, and the adversary ($\mathcal{P}_A$), determining the distribution of types, are aware of the signaling rules. Therefore, $\mathcal{P}_S$ anticipates reactions of different types of controllers and the worst possible distribution over those types while selecting the signaling rule $\eta_{1:\kappa}$ to minimize (3.6).

3.1.1 Game Model

We consider a game with three players: $\mathcal{P}_S$, $\mathcal{P}_C$, and $\mathcal{P}_A$. $\mathcal{P}_C$ can have different private types. Let Ω denote the finite set of all (benign/malicious) controller types. Correspondingly, depending on the type $\omega \in \Omega$, $\mathcal{P}_C$ selects the control rule $\gamma_k^\omega \in \Gamma_k$. $\mathcal{P}_S$ designs the signaling rule $\eta_{1:\kappa}$ to minimize the expected cost, where the expectation is taken over all the randomness (due to the initial state, and state and measurement noises), and the distribution of types, determined by $\mathcal{P}_A$. Let $p := \{p_\omega\}_{\omega \in \Omega}$ denote the probabilities of types $\omega \in \Omega$. Then, type-ω $\mathcal{P}_C$'s, $\mathcal{P}_S$'s, and $\mathcal{P}_A$'s cost functions are given by

$$U_C^\omega(\eta_{1:\kappa}, \gamma_{1:\kappa}^\omega) = \mathbb{E}\left\{ \sum_{k=1}^{\kappa} \|\boldsymbol{x}_{k+1}^\omega\|_{Q_\omega}^2 + \|\gamma_k^\omega\big(\eta_k(\boldsymbol{y}_{1:k}^\omega), \dots, \eta_1(\boldsymbol{y}_1^\omega)\big)\|_{R_\omega}^2 \right\} \tag{3.8}$$

$$U_S(\eta_{1:\kappa}, \{\gamma_{1:\kappa}^\omega\}, p) = \sum_{\omega \in \Omega} p_\omega \mathbb{E}\left\{ \sum_{k=1}^{\kappa} \|\boldsymbol{x}_{k+1}^\omega\|_Q^2 + \|\gamma_k^\omega\big(\eta_k(\boldsymbol{y}_{1:k}^\omega), \dots, \eta_1(\boldsymbol{y}_1^\omega)\big)\|_R^2 \right\} \tag{3.9}$$

$$U_A(\eta_{1:\kappa}, \{\gamma_{1:\kappa}^\omega\}, p) = -U_S(\eta_{1:\kappa}, \{\gamma_{1:\kappa}^\omega\}, p), \tag{3.10}$$

respectively, where we represent the dependence of the state on the controller's type, ω, due to the control input in the state recursion (3.1) explicitly through $\boldsymbol{x}_k^\omega$ (and the signal $\boldsymbol{y}_k^\omega$) instead of $\boldsymbol{x}_k$ (and $\boldsymbol{y}_k$). Then, the robust sensor design game is defined as follows:

Definition (Robust Sensor Design Game). The robust sensor design game

$$\mathcal{G} := \big(\Upsilon_{1:\kappa}, \Gamma_{1:\kappa}, \Delta^{|\Omega|}, \boldsymbol{x}_1, \boldsymbol{w}_{1:\kappa}, \boldsymbol{v}_{1:\kappa}, U_C^{\omega}(\cdot), U_S(\cdot), U_A(\cdot)\big) \tag{3.11}$$

is a Stackelberg game [3] between $\mathcal{P}_S$, $\mathcal{P}_C$, and $\mathcal{P}_A$, where $\mathcal{P}_S$ is the leader while $\mathcal{P}_C$ and $\mathcal{P}_A$ are the followers, reacting to the leader's announced strategies. $\mathcal{P}_C$'s type is drawn according to $\mathcal{P}_A$'s action $p \in \Delta^{|\Omega|}$ and his/her strategy space is Γ_k at stage k. $\mathcal{P}_S$'s strategy space is Υ_k at each stage k and $\mathcal{P}_A$'s action space is the simplex $\Delta^{|\Omega|}$. Objectives of $\mathcal{P}_C$, $\mathcal{P}_S$, and $\mathcal{P}_A$ are given by (3.8), (3.9) and (3.10), respectively. The tuple of strategies $(\eta_{1:\kappa}^*, \{\gamma_{1:\kappa}^{\omega *}\}_{\omega\in\Omega}, p^*)$ attains the Stackelberg equilibrium provided that

$$\eta_{1:\kappa}^* = \operatorname*{argmin}_{\substack{\eta_k\in\Upsilon_k\\ k=1,\dots,\kappa}} U_S\big(\eta_{1:\kappa}, \{\gamma_{1:\kappa}^{\omega *}(\eta_{1:\kappa})\}_{\omega\in\Omega}, p^*(\eta_{1:\kappa})\big) \tag{3.12a}$$

$$\gamma_{1:\kappa}^{\omega *}(\eta_{1:\kappa}) = \operatorname*{argmin}_{\substack{\gamma_k^{\omega}\in\Gamma_k\\ k=1,\dots,\kappa}} U_C^{\omega}\big(\eta_{1:\kappa}, \gamma_{1:\kappa}^{\omega}(\eta_{1:\kappa})\big), \tag{3.12b}$$

$$p^*(\eta_{1:\kappa}) = \operatorname*{argmin}_{p\in\Delta^{|\Omega|}} U_A\big(\eta_{1:\kappa}, \{\gamma_{1:\kappa}^{\omega *}(\eta_{1:\kappa})\}_{\omega\in\Omega}, p(\eta_{1:\kappa})\big) \tag{3.12c}$$

where, with abuse of notation, we denote type-ω $\mathcal{P}_C$'s strategy γ_k^{ω} by $\gamma_k^{\omega}(\eta_{1:k})$ to show the dependence of type-ω $\mathcal{P}_C$'s strategies on $\mathcal{P}_S$'s signaling rules due to the hierarchy, explicitly, and we define $\gamma_{1:\kappa}^{\omega}(\eta_{1:\kappa}) := \{\gamma_1^{\omega}(\eta_1), \dots, \gamma_{\kappa}^{\omega}(\eta_{1:\kappa})\}$.

Remark (Uniqueness of Follower Reactions). The reaction set of type-ω $\mathcal{P}_C$ is an equivalence class such that all $\gamma_{1:\kappa}^{\omega *}$ in the reaction set lead to the same control input $\boldsymbol{u}_k^{\omega *}$ almost surely under certain convexity assumptions, e.g., $R_{\omega} \succ O$ is positive-definite, which will be shown in detail in Section 3.2. Furthermore, the reaction set of $\mathcal{P}_A$ is also an equivalence class due to the zero-sum relation between the cost functions U_S and U_A.

Remark (Decoupled Follower Objectives). Given $\mathcal{P}_S$'s signaling rule, $\mathcal{P}_C$'s objective U_C^{ω}, for $\omega \in \Omega$, is *decoupled* from the other follower $\mathcal{P}_A$'s action while $\mathcal{P}_A$'s objective U_A depends on different type $\mathcal{P}_C$'s strategies. Therefore, this can be viewed as a sequential optimization between the two followers, where firstly $\mathcal{P}_C$ selects his/her strategy optimizing his/her objective (3.8) given the leader's strategy, and then $\mathcal{P}_A$ takes action corresponding to the leader's strategy and the $\mathcal{P}_C$'s optimal reaction to optimize his/her objective (3.10).

3.2 Robust Sensor Design in LQG Control

We first assume, in this section, that $\mathcal{P}_S$ has access to perfect measurements, i.e., $\boldsymbol{y}_k = \boldsymbol{x}_k$ for $k = 1, \ldots, \kappa$; the general noisy/partial measurements case will be addressed later in Section 3.3. Then, given $p \in \Delta^{|\Omega|}$, $\mathcal{P}_S$ faces the following optimization probably

$$\min_{\substack{\eta_k \in \Upsilon_k \\ k=1,\ldots,\kappa}} U_S(\eta_{1:\kappa}, \{\gamma^{\omega *}_{1:\kappa}(\eta_{1:\kappa})\}_{\omega\in\Omega}, p), \tag{3.13}$$

where $\gamma^{\omega *}_{1:\kappa}(\eta_{1:\kappa})$ is given by (3.12b). This is a highly nonlinear and non-convex problem. However, the following theorem provides an equivalent semi-definite programming (SDP) problem, which is not limited to equivalence in optimality as in Chapter 2, so that we can address the equilibrium for the robust sensor design game $\mathcal{G}$ in a compact way.

Theorem 3.1 (Equivalence Result)**.** *Let the convex and compact set* Ψ *be defined as*

$$\Psi := \left\{ (S_k \in \mathbb{S}^m)_{k=1}^{\kappa} \,|\, \Sigma_k^o \geq S_k \geq A S_{k-1} A', k = 1, \ldots, \kappa, S_0 = O \right\}, \tag{3.14}$$

where $\Sigma_k^o \in \mathbb{S}^m$ *is the covariance matrix of the control-free process:*

$$\boldsymbol{x}^o_{k+1} = A \boldsymbol{x}^o_k + \boldsymbol{w}_k \text{ and } \boldsymbol{x}^o_1 = \boldsymbol{x}_1, \tag{3.15}$$

i.e., $\boldsymbol{x}^o_k \sim \mathcal{N}(0, \Sigma^o_k)$ *and*[3] $\Sigma^o_k := \mathbb{E}\{\boldsymbol{x}^o_k (\boldsymbol{x}^o_k)'\}$. *Then, given* $p \in \Delta^{|\Omega|}$, *for any signaling rule* $\eta_k \in \Upsilon_k$, *for* $k = 1, \ldots, \kappa$, *there exists* $S_{1:\kappa} \in \Psi$ *such that*

$$U_S(\eta_{1:\kappa}, \{\gamma^{\omega *}_{1:\kappa}(\eta_{1:\kappa})\}_{\omega\in\Omega}, p) = \sum_{k=1}^{\kappa} \operatorname{Tr}\left\{ S_k \left(\sum_{\omega\in\Omega} p_\omega V_k(\omega) \right) \right\} + v_o, \tag{3.16}$$

where $V_{1:\kappa}(\omega)$ *and* v_o *are deterministic parameters that do not depend on* $S_{1:\kappa}$ *and derived in Appendix B.2. Furthermore, for any* $S_{1:\kappa} \in \Psi$, *there exists a signaling rule* $\eta_{1:\kappa}$ *such that*

$$\sum_{k=1}^{\kappa} \operatorname{Tr}\left\{ S_k \left(\sum_{\omega\in\Omega} p_\omega V_k(\omega) \right) \right\} + v_o = U_S(\eta_{1:\kappa}, \{\gamma^{\omega *}_{1:\kappa}(\eta_{1:\kappa})\}_{\omega\in\Omega}, p). \tag{3.17}$$

Proof. The proof proceeds as follows: $i)$ we first show that the optimization

[3] Note that $\Sigma^o_k = A \Sigma^o_{k-1} A' + \Sigma_w$.

function can be written as a linear function of the covariance of the posterior control-free state, i.e.,

$$H_k := \operatorname{cov}\{\mathbb{E}\{\boldsymbol{x}_k^o | \boldsymbol{s}_{1:k}\}\}, \tag{3.18}$$

for $k = 1, \ldots, \kappa$; *ii*) we then identify the necessary condition on $H_{1:\kappa}$, which is indeed the constraint set Ψ, i.e., $H_{1:\kappa} \in \Psi$; and finally *iii*) we show that the constraint set Ψ is also a sufficient condition for $H_{1:\kappa}$ since any point in Ψ can be attained through certain linear plus noise signaling rule. We now provide details of each of these steps.

Step i) Our first goal is to isolate the underlying state from the control input by completing the squares in the cost functions and through change of variables, which yields the result that given positive semi-definite $Q_\omega \in \mathbb{S}^m$ and positive definite $R_\omega \in \mathbb{S}^r$ corresponding to the type-ω controller, we have

$$\mathbb{E}\left\{\sum_{k=1}^{\kappa} \|\boldsymbol{x}_{k+1}\|_{Q_\omega}^2 + \|\boldsymbol{u}_k\|_{R_\omega}^2\right\} = \sum_{k=1}^{\kappa} \mathbb{E}\left\{\|\boldsymbol{u}_k^o + K_k^\omega \boldsymbol{x}_k^o\|_{\Delta_k^\omega}^2\right\} + \Delta_0^\omega, \tag{3.19}$$

where $K_k^\omega \in \mathbb{R}^{r\times m}, \Delta_k^\omega \in \mathbb{S}_+^m$, for $k = 1, \ldots, \kappa$, and $\Delta_0^\omega \in \mathbb{R}$ are derived in Appendix B.1; and $\{\boldsymbol{x}_k^o\}$ is the control-free process defined in (3.15) and

$$\boldsymbol{u}_k^o = \boldsymbol{u}_k + K_k^\omega B \boldsymbol{u}_{k-1} + \ldots + K_k^\omega A^{k-2} B \boldsymbol{u}_1. \tag{3.20}$$

Remark (Optimality of Linear Signaling Rules). Different from the cooperative settings, (3.19) does *not* imply that the optimal transformed control input is $\boldsymbol{u}_k^o = -K_k^\omega \mathbb{E}\{\boldsymbol{x}_k^o | \boldsymbol{s}_{1:k}\}$ since $\boldsymbol{s}_k$ depends on previous control inputs $\boldsymbol{u}_{1:k-1}$, as also pointed out in Chapter 2. Therefore, we cannot claim optimality of linear signaling rules within the general class of all measurable policies.

However, for affine signaling rules, e.g., $\boldsymbol{s}_k = L'_{k,k}\boldsymbol{x}_k + \ldots + L'_{k,1}\boldsymbol{x}_1 + \boldsymbol{n}_k$, we have

$$\begin{aligned}&\mathbb{E}\{\boldsymbol{x}_k^o | L'_{1,1}\boldsymbol{x}_1 + \boldsymbol{n}_1, \cdots, L'_{k,k}\boldsymbol{x}_k + \ldots + L'_{k,1}\boldsymbol{x}_1 + \boldsymbol{n}_k\}\\ &\quad = \mathbb{E}\{\boldsymbol{x}_k^o | L'_{1,1}\boldsymbol{x}_1^o + \boldsymbol{n}_1, \cdots, L'_{k,k}\boldsymbol{x}_k^o + \ldots + L'_{k,1}\boldsymbol{x}_1^o + \boldsymbol{n}_k\},\end{aligned} \tag{3.21}$$

which holds since the signal $\boldsymbol{s}_l$ for $l = 1, \ldots, k$ can be written as

$$\begin{aligned} L'_{l,l}\boldsymbol{x}_l + \ldots + L'_{l,1}\boldsymbol{x}_1 + \boldsymbol{n}_l &= L'_{l,l}\boldsymbol{x}^o_l + \ldots + L'_{l,1}\boldsymbol{x}^o_1 + \boldsymbol{n}_l \\ &+ \Big\{L'_{l,l}B\boldsymbol{u}_{l-1} + \ldots + (L'_{l,l}A^{l-2} + \ldots + L'_{l,2})B\boldsymbol{u}_1\Big\}, \end{aligned} \tag{3.22}$$

where the term in-between $\{\cdot\}$ is σ-$\boldsymbol{s}_{1:l-1}$ measurable since the control input is given by (3.5). This yields that the optimal transformed control input is given by $\boldsymbol{u}^o_k = -K^\omega_k \mathbb{E}\{\boldsymbol{x}^o_k|\boldsymbol{s}_{1:k}\}$ since $\mathbb{E}\{\boldsymbol{x}^o_k|\boldsymbol{s}_{1:k}\}$ does not depend on $\boldsymbol{u}_{1:k}$. Then, the corresponding optimal (original) control input $\boldsymbol{u}^*_k$ can be computed based on (3.20) and $\boldsymbol{u}^*_k$ is linear in $\mathbb{E}\{\boldsymbol{x}^o_k|\boldsymbol{s}_{1:k}\}$ while $\mathbb{E}\{\boldsymbol{x}^o_k|\boldsymbol{s}_{1:k}\}$ does not depend on the type of the controller.

Remark (Versatility of the Control Objectives)*.* The result in Step *i*) would also hold if the controllers have objectives (other than (3.8)), e.g., additional certain soft constraints, leading to optimal control inputs that are linear functions of $\mathbb{E}\{\boldsymbol{x}^o_k|\boldsymbol{s}_{1:k}\}$.

Due to the linearity of the controllers' reactions in $\mathbb{E}\{\boldsymbol{x}^o_k|\boldsymbol{s}_{1:k}\}$, the quadratic objective (3.19) can be written as

$$\sum_{k=1}^{\kappa} \mathrm{Tr}\left\{H_k\left(\sum_{\omega\in\Omega} p_\omega V_k(\omega)\right)\right\} + v_o, \tag{3.23}$$

where $V_{1:\kappa}(\omega) \in \mathbb{S}^m$, for $\omega \in \Omega$, and $v_o \in \mathbb{R}$ are derived in Appendix B.2.

Step ii) The covariance of the posterior control-free state $H_k \in \mathbb{S}^m$ can be in-between two extremes: Σ^o_k corresponding to full disclosure of the state, i.e., $\boldsymbol{s}_k = \boldsymbol{x}_k$; and $\mathbb{E}\{\mathbb{E}\{\boldsymbol{x}^o_k|\boldsymbol{s}_{1:k-1}\}\mathbb{E}\{\boldsymbol{x}^o_k|\boldsymbol{s}_{1:k-1}\}'\} = AH_{k-1}A'$ corresponding to sharing nothing, i.e., $\boldsymbol{s}_k = 0$. The inequality

$$\Sigma^o_k \geq H_k \geq AH_{k-1}A' \tag{3.24}$$

follows from the following covariance matrices:

$$\begin{aligned} \mathrm{cov}\{\boldsymbol{x}^o_k - \mathbb{E}\{\boldsymbol{x}^o_k|\boldsymbol{s}_{1:k}\}\} &= \Sigma^o_k - H_k \geq O, \\ \mathrm{cov}\{\mathbb{E}\{\boldsymbol{x}^o_k|\boldsymbol{s}_{1:k}\} - \mathbb{E}\{\boldsymbol{x}^o_k|\boldsymbol{s}_{1:k-1}\}\} &= H_k - AH_{k-1}A' \geq O, \end{aligned}$$

since for arbitrary random variables $\boldsymbol{a}$ and $\boldsymbol{b}$,

$$\mathbb{E}\{\boldsymbol{a}\mathbb{E}\{\boldsymbol{a}|\boldsymbol{b}\}\} = \mathbb{E}\{\mathbb{E}\{\boldsymbol{a}|\boldsymbol{b}\}\mathbb{E}\{\boldsymbol{a}|\boldsymbol{b}\}\}.$$

We then arrive at (3.16) based on (3.24).

Step iii) In order to show (3.17), we will be using the following lemma from [35] to address the cases when $\Sigma_k^o - A\Sigma_{k-1}^o A' = \Sigma_w \geq O$ can be singular.

Lemma 3.2 (Lemma 3 in [35]). *If we can partition a positive semi-definite matrix into blocks such that a block at the diagonal is a zero matrix, then we have*

$$\begin{bmatrix} A & B \\ B' & O \end{bmatrix} \geq O \Leftrightarrow A \geq O \text{ and } B = O. \tag{3.25}$$

Based on Lemma 3.2, the following lemma shows that any point in Ψ can be attained by a certain affine signaling rule.

Lemma 3.3 (Sufficiency Result). *Consider any $S_{1:\kappa} \in \Psi$, and let*

$$\Sigma_k^o - AS_{k-1}A' = \bar{U}_k \begin{bmatrix} \bar{\Lambda}_k & O \\ O & O \end{bmatrix} \bar{U}_k'$$

be the eigen-decomposition such that $\bar{\Lambda}_k \succ O$. Let

$$T_k := \begin{bmatrix} \bar{\Lambda}_k^{1/2} & O \end{bmatrix} \bar{U}_k'(S_k - AS_{k-1}A')\bar{U}_k \begin{bmatrix} \bar{\Lambda}_k^{1/2} \\ O \end{bmatrix} \tag{3.26}$$

have the eigen-decomposition $T_k = U_k\Lambda_k U_k'$ with eigenvalues, e.g.,[4] *$\lambda_{k,i} \in [0,1]$ for $i = 1,\dots,t_k$, where $t_k = \operatorname{rank}\{\Sigma_k^o - AS_{k-1}A'\}$. Then, there exists a memoryless affine signaling rule*

$$\boldsymbol{y}_k = L_k'\boldsymbol{x}_k + \boldsymbol{n}_k, \textit{ for } k = 1,\dots,\kappa, \tag{3.27}$$

where $\boldsymbol{n}_k \sim \mathcal{N}(0,\Theta_k)$ and $\Theta_k = \operatorname{diag}\{\theta_{1,1}^2,\dots,\theta_{1,t_k}^2\}$, L_k is given by

$$L_k = \bar{U}_k \begin{bmatrix} \bar{\Lambda}_k^{-1/2} U_k \Lambda_k^o & O \\ O & O \end{bmatrix} \tag{3.28}$$

where $\Lambda_k^o := \operatorname{diag}\{\lambda_{1,1}^o,\dots,\lambda_{1,t_k}^o\}$ and

$$\frac{(\lambda_{k,i}^o)^2}{(\lambda_{k,i}^o)^2 + \theta_{k,i}^2} = \lambda_{k,i} \in [0,1], \forall\, i = 1.\dots,t_k, \tag{3.29}$$

[4] We do not assume that its eigenvalues are necessarily in $[0,1]$. But actually, they turn out to be in $[0,1]$.

which leads to $S_{1:\kappa} = H_{1:\kappa}$.

Proof. The proof follows by induction. If $S_{1:\kappa} \in \Psi$, then $S_1 \in \mathbb{S}^m$ satisfies

$$\Sigma_1^o \succeq S_1 \succeq O, \tag{3.30}$$

where $\Sigma_1^o \succeq O$ can be singular. Let $\Sigma_k^o = \bar{U}_1 \begin{bmatrix} \bar{\Lambda}_1 & O \\ O & O \end{bmatrix} \bar{U}_1'$ be the eigen-decomposition such that $\bar{\Lambda}_1 \succ O$. Then, we have

$$\begin{bmatrix} \bar{\Lambda}_1 & O \\ O & O \end{bmatrix} \succeq \bar{U}_1' S_1 \bar{U}_1 \succeq O, \tag{3.31}$$

which implies that

$$\begin{bmatrix} \bar{\Lambda}_1 & O \\ O & O \end{bmatrix} - \begin{bmatrix} M_{1,1} & M_{1,2} \\ M_{2,1} & M_{2,2} \end{bmatrix} \succeq O, \tag{3.32}$$

where we let $\bar{U}_1' S_1 \bar{U}_1 = \begin{bmatrix} M_{1,1} & M_{1,2} \\ M_{2,1} & M_{2,2} \end{bmatrix}$ be the corresponding partitioning. Note that since $\bar{U}_1' S_1 \bar{U}_1 \succeq O$, we have $M_{2,2} \succeq O$ [62]. However, the bottom-right block of the positive semi-definite matrix (the whole term) on the left-hand side of the inequality (3.32), i.e., $-M_{2,2}$, must also be a positive semi-definite matrix, which implies $O \succeq M_{2,2}$. Therefore we have $M_{2,2} = O$ and Lemma 3.2 yields that there exists a symmetric matrix $T_1 \in \mathbb{S}^{t_1}$, where $t_1 := \text{rank}\{\Sigma_1^o\}$, such that

$$S_1 = \bar{U}_1 \begin{bmatrix} \bar{\Lambda}_1^{1/2} T_1 \bar{\Lambda}_1^{1/2} & O \\ O & O \end{bmatrix} \bar{U}_1'. \tag{3.33}$$

Note that there exists a bijective relation between $S_1 \in \mathbb{S}^m$ and $T_1 \in \mathbb{S}^{t_1}$. Furthermore, (3.30) and (3.33) imply that

$$I \succeq T_1 \succeq O, \tag{3.34}$$

and $T_1 \in \mathbb{S}^m$ has eigenvalues in the closed interval $[0,1]$ since the eigenvalues of I, i.e., the vector $\mathbf{1} \in \mathbb{R}^{t_1}$, weakly majorizes the eigenvalues of T_1 from below [62]. Let $T_1 = U_1 \Lambda_1 U_1'$ be the eigen-decomposition and $\lambda_{1,1}, \ldots, \lambda_{1,t_1} \in [0,1]$ be the associated eigenvalues.

Furthermore, consider the affine signaling rule $\boldsymbol{s}_1 = L_1' \boldsymbol{x}_1 + \boldsymbol{n}_1$, where $\boldsymbol{n}_1 \sim \mathcal{N}(0, \Theta_1)$ is independent of all the other parameters. Then, the covariance of the posterior control-free state is given by

$$H_1 = \Sigma_1^o L_1 (L_1' \Sigma_1^o L_1 + \Theta_1)^\dagger L_1' \Sigma_1^o. \tag{3.35}$$

If we set $L_1 = \bar{U}_1 \begin{bmatrix} \bar{\Lambda}_1^{-1/2} U_1 \Lambda_1^o & O \\ O & O \end{bmatrix}$ and $\Theta_1 \geq O$ such that

$$\Lambda_1^o := \begin{bmatrix} \lambda_{1,1}^o & & \\ & \ddots & \\ & & \lambda_{1,t_1}^o \end{bmatrix}, \Theta_1 := \begin{bmatrix} \theta_{1,1}^2 & & \\ & \ddots & \\ & & \theta_{1,t_1}^2 \end{bmatrix} \tag{3.36}$$

and

$$\frac{(\lambda_{1,i}^o)^2}{(\lambda_{1,i}^o)^2 + \theta_{1,i}^2} = \lambda_{1,i} \in [0,1], \text{ for } i = 1, \dots, t_1, \tag{3.37}$$

then, we would obtain $H_1 = S_1$ exactly.

Suppose that $H_j = S_j$ for $j < k$. Then, $S_k \in \mathbb{S}^m$ satisfies

$$\Sigma_k^o \geq S_k \geq A S_{k-1} A', \tag{3.38}$$

which is equivalent to

$$\Sigma_k^o \geq S_k \geq A H_{k-1} A'. \tag{3.39}$$

Correspondingly, $\Sigma_k^o - A H_{k-1} A' \geq O$ can be singular. Let $\Sigma_k^o - A H_{k-1} A' = \bar{U}_k \begin{bmatrix} \bar{\Lambda}_k & O \\ O & O \end{bmatrix} \bar{U}_k'$ be the eigen-decomposition such that $\bar{\Lambda}_k \succ O$. Then, we have

$$\begin{bmatrix} \bar{\Lambda}_k & O \\ O & O \end{bmatrix} \geq \bar{U}_k' (S_k - A H_{k-1} A') \bar{U}_k \geq O \tag{3.40}$$

and correspondingly Lemma 3.2 yields that there exists a symmetric matrix $T_k \in \mathbb{S}^{t_k}$, where $t_k := \operatorname{rank}\{\Sigma_k^o - A H_{k-1} A'\}$, such that

$$S_k = A H_{k-1} A' + \bar{U}_k \begin{bmatrix} \bar{\Lambda}_k^{1/2} T_k \bar{\Lambda}_k^{1/2} & O \\ O & O \end{bmatrix} \bar{U}_k'. \tag{3.41}$$

Furthermore, (3.39) and (3.41) yield that

$$I \geq T_k \geq O, \tag{3.42}$$

which implies that $T_k \in \mathbb{S}^{t_k}$ has eigenvalues in the closed interval $[0,1]$. Let $T_k = U_k \Lambda_k U_k'$ be the eigen decomposition and $\lambda_{k,1}, \ldots, \lambda_{k,t_k} \in [0,1]$ be the associated eigenvalues.

Furthermore, for the affine signaling rule $\boldsymbol{s}_k = L_k' \boldsymbol{x}_k + \boldsymbol{n}_k$, where $\boldsymbol{n}_k \sim \mathcal{N}(0, \Theta_k)$ is independent of all the other parameters, the covariance of the posterior control-free state is given by

$$H_k = AH_{k-1}A' + (\Sigma_k^o - AH_{k-1}A')L_k \tag{3.43}$$

$$\times (L_k(\Sigma_k^o - AH_{k-1}A')L_k + \Theta_k)^\dagger L_k'(\Sigma_k^o - AH_{k-1}A'), \tag{3.44}$$

which follows since

$$\begin{aligned}\text{cov}\{\mathbb{E}\{\boldsymbol{x}_k^o | \boldsymbol{s}_{1:k}\}\} = {} & \text{cov}\{\mathbb{E}\{\boldsymbol{x}_k^o | \boldsymbol{s}_{1:k-1}\}\} \\ & + \text{cov}\{\mathbb{E}\{\boldsymbol{x}_k^o | \boldsymbol{s}_k - \mathbb{E}\{\boldsymbol{s}_k | \boldsymbol{s}_{1:k-1}\}\}\},\end{aligned} \tag{3.45}$$

due to the independence of the jointly Gaussian $\boldsymbol{s}_{1:k-1}$ and $\boldsymbol{s}_k - \mathbb{E}\{\boldsymbol{s}_k | \boldsymbol{s}_{1:k-1}\}$. If we set $L_k = \bar{U}_k \begin{bmatrix} \bar{\Lambda}_k^{-1/2} U_k \Lambda_k^o & O \\ O & O \end{bmatrix}$ and $\Theta_k \geq O$ such that

$$\frac{(\lambda_{k,i}^o)^2}{(\lambda_{k,i}^o)^2 + \theta_{k,i}^2} = \lambda_{k,i} \in [0,1], \text{ for } i = 1, \ldots, t_k, \tag{3.46}$$

then, we would obtain $H_k = S_k$ exactly. Therefore, by induction, we conclude that for any $S_{1:\kappa} \in \Psi$, there exists a certain affine signaling rule such that $H_k = S_k$ for $k = 1, \ldots, \kappa$. □

Remark (Memory vs. Memoryless). When $\mathcal{P}_S$ has perfect measurements, i.e., $\boldsymbol{y}_k = \boldsymbol{x}_k$, then the optimal signaling rules can be memoryless linear-plus-noise policies within the general class of linear-plus-noise policies with complete/bounded memory.

Lemma 3.3 implies the equality at (3.17), which completes the proof of Theorem 3.1. □

Henceforth, we will be working with the right-hand side of (3.16) instead of its left-hand side while analyzing the equilibrium of the game $\mathcal{G}$.

New notation for compact presentation: Let

$$S := \begin{bmatrix} S_\kappa & & \\ & \ddots & \\ & & S_1 \end{bmatrix}, \; V(\omega) := \begin{bmatrix} V_\kappa(\omega) & & \\ & \ddots & \\ & & V_1(\omega) \end{bmatrix},$$

and $\bar{\Psi} \in \mathbb{S}^{m\kappa}$ be the set corresponding to the constraint set Ψ in this new high-dimensional space, i.e., $\mathbb{R}^{m\kappa \times m\kappa}$. Furthermore, let $V_i = V(\omega_i)$ and $p_i := p_{\omega_i}$, where $i \in \mathcal{I}$ and $\mathcal{I}$ is certain index set of the type set Ω.

Based on Theorem 3.1, at the Stackelberg equilibrium, where $\mathcal{P}_S$ is the leader, $\mathcal{P}_S$ faces the following problem:

$$\min_{S \in \bar{\Psi}} \max_{p \in \Delta^{|\Omega|}} \operatorname{Tr}\left\{ S \sum_{i \in \mathcal{I}} p_i V_i \right\} + v_o, \tag{3.47}$$

since $\mathcal{P}_A$ reacts to the committed signaling rule $\eta_{1:\kappa}$ and correspondingly reacts to $S \in \bar{\Psi}$. Thus, (3.47) can also be written as

$$\min_{S \in \bar{\Psi}} \max_{p \in \Delta^{|\Omega|}} \sum_{i \in \mathcal{I}} p_i \operatorname{Tr}\{S V_i\} + v_o. \tag{3.48}$$

The following proposition addresses the existence of an equilibrium for $\mathcal{G}$.

Proposition 3.4 (Existence Result)**.** *There exists at least one tuple of pure actions* $(\eta_{1:\kappa}^*, \{\gamma_{1:\kappa}^{\omega *}(\eta_{1:\kappa})\}_{\omega \in \Omega}, p^*(\eta_{1:\kappa}))$ *attaining the equilibrium of the Stackelberg game* $\mathcal{G}$*, i.e., satisfying* (3.12)*.*

Proof. The proof follows from the equivalence at (3.16), which yields that $\mathcal{P}_S$ faces (3.48). Since the objective function in (3.48) is continuous in the optimization arguments and the constraint sets are decoupled and compact, the extreme value theorem and maximum theorem (showing the continuity of parametric maximization under certain conditions [82]) yields the existence of a solution to (3.48), which completes the proof. □

Remark (Noisy vs. Noiseless Signals)*.* The objective function in (3.48) is linear in the optimization argument $S \in \bar{\Psi}$, and the constraint set $\bar{\Psi}$ is compact and convex. Therefore, given $p \in \Delta^{|\Omega|}$, the solution could be attained at a certain extreme point of $\bar{\Psi}$. However, the following function:

$$\max_{p \in \Delta^{|\Omega|}} \sum_{i \in \mathcal{I}} p_i \operatorname{Tr}\{S V_i\} \tag{3.49}$$

is convex in $S \in \bar{\Psi}$ since the maximum of any family of linear functions is a convex function [81]. Particularly, for $\mu \in [0,1]$, we have

$$\mu \max_{p\in\Delta^{|\Omega|}} \operatorname{Tr}\left\{S\sum_i p_i V_i\right\} + (1-\mu)\max_{p\in\Delta^{|\Omega|}} \operatorname{Tr}\left\{\bar{S}\sum_i p_i V_i\right\}$$
$$\geq \max_{p\in\Delta^{|\Omega|}} \operatorname{Tr}\left\{(\mu S + (1-\mu)\bar{S})\sum_i p_i V_i\right\}.$$

Therefore, the solution can be a non-extreme point of the constraint set $\bar{\Psi}$. Correspondingly, Lemma 3.3 implies that the optimal signals would be affine in the underlying state rather than linear, i.e., there will be additional independent noise term $\boldsymbol{n}_k \sim \mathcal{N}(0,\Theta_k)$, where $\Theta_k \neq O$.

Next, we seek to compute the equilibrium of $\mathcal{G}$. To this end, we examine the equilibrium conditions further. In particular, according to (3.48), given $S \in \bar{\Psi}$, the best action for $\mathcal{P}_A$ is given by

$$p^* \in \left\{p \in \Delta^{|\Omega|} \,|\, p_j = 0 \text{ if } \operatorname{Tr}\{V_j S\} < \max_i \operatorname{Tr}\{V_i S\}\right\} \tag{3.50}$$

since (3.48) is linear in $p \in \Delta^{|\Omega|}$. Then, based on the observation (3.50), the following theorem provides an algorithm to compute the robust sensor outputs.

Theorem 3.5 (Computing the Equilibrium)**.** *The value of the Stackelberg equilibrium* (3.48) *is given by* $\vartheta = \min_{j\in\mathcal{I}}\{\vartheta_j\}$*, where*

$$\begin{aligned}\vartheta_j := \min_{S\in\bar{\Psi}}\ & \operatorname{Tr}\{V_j S\} + v_o \\ \text{s.t. }& \operatorname{Tr}\{(V_j - V_i)S\} \geq 0\ \forall i \in \mathcal{I}.\end{aligned} \tag{3.51}$$

Furthermore, let $\vartheta_{j^*} = \vartheta$ *and*

$$\begin{aligned}S^* \in \operatorname*{argmin}_{S\in\bar{\Psi}}\ & \operatorname{Tr}\{V_{j^*} S\} + v_o \\ \text{s.t. }& \operatorname{Tr}\{(V_{j^*} - V_i)S\} \geq 0\ \forall i \in \mathcal{I}.\end{aligned} \tag{3.52}$$

Then, given $S^* \in \bar{\Psi}$*, the optimal signaling rule* $\eta_{1:\kappa}$ *can be computed according to Lemma 3.3.*

Proof. Based on the existence result in Proposition 3.4, suppose that (S^*, p^*) attains the Stackelberg equilibrium, i.e., solves (3.48). Since $p^* \in \Delta^{|\Omega|}$, there must be at least one type with positive weight. As an example, suppose positive weight for the type $\omega_j \in \Omega$, i.e., $p_j > 0$. This implies that

$$\mathrm{Tr}\{V_j S^*\} \geq \mathrm{Tr}\{V_i S^*\} \ \forall i \tag{3.53}$$

since $\mathrm{Tr}\{V_j S^*\} = \max_{i \in \mathcal{I}} \mathrm{Tr}\{V_i S^*\}$ by (3.50). Furthermore, this also implies that

$$\mathrm{Tr}\{V_j S^*\} = \sum_{i \in \mathcal{I}} p_i^* \,\mathrm{Tr}\{V_i S^*\} \tag{3.54}$$

since if $p_i^* > 0$, then we have

$$\mathrm{Tr}\{V_j S^*\} = \mathrm{Tr}\{V_i S^*\}. \tag{3.55}$$

These necessary conditions yield that

$$\min_{S \in \bar{\Psi}} \max_{p \in \Delta^{|\Omega|}} \sum_{i \in \mathcal{I}} \mathrm{Tr}\{V_i S\} p_i = \min_{S \in \bar{\Psi}} \mathrm{Tr}\{V_j S\} \\ \text{s.t. } \mathrm{Tr}\{(V_j - V_i) S\} \geq 0 \ \forall i \tag{3.56}$$

while the right-hand side is an SDP problem isolated from $\mathcal{P}_A$'s action. Therefore, by searching over the index set $\mathcal{I}$, we can compute the left-hand side, which is the minimum over $\mathcal{I}$. Once the minimum value is computed, S^* can be computed according to the corresponding index, i.e., (3.52). □

Remark. In Theorem 3.5, we search over the index set $\mathcal{I}$ linearly, however, certain pruning operations can be conducted to speed up the computation. As an example, we can search over the extreme points of the convex hull of V_j, $j \in \mathcal{I}$.

Remark. There might be multiple solutions for (3.52). $\mathcal{P}_S$ can be selective among those solutions. In particular, (3.48) implies that $\mathcal{P}_S$ minimizes the cost given that $\mathcal{P}_A$ maximizes it. Therefore, if the true underlying distribution is not the worst possible distribution, then $\mathcal{P}_S$ would not get a cost more than the anticipated one. Any deviation from the worst distribution benefits $\mathcal{P}_S$. Furthermore, in the worst case, $\mathcal{P}_A$ assigns positive probabilities to the types leading to the maximum as in (3.50). Correspondingly, if $\mathcal{P}_S$ selects the solution $S^* \in \bar{\Psi}$ for (3.52) such that the cardinality of $\mathrm{argmax}_j \,\mathrm{Tr}\{V_j S^*\}$ is the smallest, then any positive probability on other types of attacks out of that set would lead to lower cost and would be desirable.

3.3 Noisy or Partial Measurements

In this section, we obtain the optimal signaling rule when there are noisy or partial measurements of the type (3.2) by turning the problem to the same structure with the case of perfect measurements based on a recent result from [37] and then invoking the results from the previous section. There are several challenges in robust sensor design with noisy or partial measurements. As an example, the sufficiency result on the necessary conditions for the covariance of the posterior control-free state, i.e., H_k, does not hold in that case. Therefore, our focus will be on the necessary and sufficient conditions for the covariance of the posterior control-free *measurements*, i.e., $\mathrm{cov}\{\mathbb{E}\{\boldsymbol{y}_k^o|\boldsymbol{s}_{1:k}\}\}$, where $\boldsymbol{y}_k^o := C\boldsymbol{x}_k^o + \boldsymbol{v}_k$. Similar to (3.21), we can show that

$$\mathbb{E}\{\boldsymbol{y}_k^o|\boldsymbol{s}_{1:k}\} = \mathbb{E}\{\boldsymbol{y}_k^o|\boldsymbol{s}_{1:k}^o\}, \tag{3.57}$$

where $\boldsymbol{s}_k^o := L_{k,k}'\boldsymbol{y}_k^o + \ldots + L_{k,1}'\boldsymbol{y}_1^o + \boldsymbol{n}_k$, since $\boldsymbol{u}_{1:k-1}$ is σ-$\boldsymbol{y}_{1:k-1}$ measurable. However, $\{\boldsymbol{y}_k^o\}$ is not necessarily a Markov process. Therefore, we consider

$$\begin{bmatrix} \boldsymbol{y}_k^o \\ \hdashline \boldsymbol{y}_{k-1}^o \\ \vdots \\ \boldsymbol{y}_1^o \end{bmatrix} = \overbrace{\begin{bmatrix} \mathbb{E}\{\boldsymbol{y}_k^o(\boldsymbol{y}_{1:k-1}^o)'\}\mathbb{E}\{\boldsymbol{y}_{1:k-1}^o(\boldsymbol{y}_{1:k-1}^o)'\}^\dagger \\ \hdashline \\ I \end{bmatrix}}^{=:A_k} \begin{bmatrix} \boldsymbol{y}_{k-1}^o \\ \vdots \\ \boldsymbol{y}_1^o \end{bmatrix} + \overbrace{\begin{bmatrix} \boldsymbol{y}_k^o - \mathbb{E}\{\boldsymbol{y}_k^o|\boldsymbol{y}_{1:k-1}^o\} \\ \hdashline \\ O \end{bmatrix}}^{=:\boldsymbol{e}_k}, \tag{3.58}$$

which can also be written in a compact form as

$$\boldsymbol{y}_{1:k}^o = A_k\boldsymbol{y}_{1:k-1}^o + \boldsymbol{e}_k, \tag{3.59}$$

where we denote the vector $\begin{bmatrix}(\boldsymbol{y}_k^o)' & \cdots & (\boldsymbol{y}_1^o)'\end{bmatrix}'$ by $\boldsymbol{y}_{1:k}^o$ with some abuse of notation.

Furthermore, we note that $\boldsymbol{x}_k^o$, $\boldsymbol{y}_{1:k}^o$, and $\boldsymbol{s}_{1:k}^o$ form a Markov chain in the order $\boldsymbol{x}_k^o \to \boldsymbol{y}_{1:k}^o \to \boldsymbol{s}_{1:k}^o$. In that respect, the following lemma from [37] shows that there exists a linear relation between the posterior estimates irrespective of the signal if they are jointly Gaussian and form a Markov chain in a certain order.

Lemma 3.6 ([37]). *Given zero-mean jointly Gaussian random vectors form-*

ing a Markov chain, e.g., $\boldsymbol{x} \to \boldsymbol{y} \to \boldsymbol{s}$ *in this order, the posterior estimates of* $\boldsymbol{x}$ *and* $\boldsymbol{y}$ *given* $\boldsymbol{s}$ *satisfy the following linear relation:*

$$\mathbb{E}\{\boldsymbol{x}|\boldsymbol{s}\} = \mathbb{E}\{\boldsymbol{x}\boldsymbol{y}'\}\mathbb{E}\{\boldsymbol{y}\boldsymbol{y}'\}^{\dagger}\mathbb{E}\{\boldsymbol{y}|\boldsymbol{s}\}, \tag{3.60}$$

which implies $\boldsymbol{s} \to \mathbb{E}\{\boldsymbol{y}|\boldsymbol{s}\} \to \mathbb{E}\{\boldsymbol{x}|\boldsymbol{s}\}$ *in this order.*

Based on Lemma 3.6, we have the following relation between $\mathbb{E}\{\boldsymbol{x}_k^o|\boldsymbol{s}_{1:k}^o\}$ and $\mathbb{E}\{\boldsymbol{y}_{1:k}^o|\boldsymbol{s}_{1:k}^o\}$:

$$\mathbb{E}\{\boldsymbol{x}_k^o|\boldsymbol{s}_{1:k}^o\} = \underbrace{\mathbb{E}\{\boldsymbol{x}_k^o(\boldsymbol{y}_{1:k}^o)'\}\mathbb{E}\{\boldsymbol{y}_{1:k}^o(\boldsymbol{y}_{1:k}^o)'\}^{\dagger}}_{=:D_k}\mathbb{E}\{\boldsymbol{y}_{1:k}^o|\boldsymbol{s}_{1:k}^o\}, \tag{3.61}$$

where $D_k \in \mathbb{R}^{m\times mk}$ does not depend on the signaling rule $\eta_{1:k}(\cdot)$. We define

$$Y_k := \operatorname{cov}\{\mathbb{E}\{\boldsymbol{y}_{1:k}^o|\boldsymbol{s}_{1:k}^o\}\}. \tag{3.62}$$

Then, (3.61) yields that

$$H_k = D_k Y_k D_k'. \tag{3.63}$$

Correspondingly, the problem faced by $\mathcal{P}_S$ can be written as

$$\min_{\substack{\eta_k\in\Upsilon_k\\ k=1,\dots,\kappa}} \sum_{k=1}^{\kappa} \operatorname{Tr}\left\{Y_k\left(\sum_{\omega\in\Omega} p_\omega W_k(\omega)\right)\right\} + v_o, \tag{3.64}$$

where $W_k(\omega) := D_k'V(\omega)D_k$ is also a symmetric matrix. Furthermore, consider the following compact and convex set:

$$\Phi := \{(S_k \in \mathbb{S}^{mk})_{k=1}^{\kappa} | \Sigma_k^y \geq S_k \geq A_k S_{k-1} A_k', k = 1,\dots,\kappa, S_0 = O\}, \tag{3.65}$$

where $\Sigma_k^y := \mathbb{E}\{\boldsymbol{y}_{1:k}^o(\boldsymbol{y}_{1:k}^o)'\}$, $C \in \mathbb{R}^{m\times m}$ and $\Sigma_v \in \mathbb{S}^m$.

Remark. Note that $\Sigma_k^y \in \mathbb{S}^{mk}$, $A_k \in \mathbb{R}^{km\times(k-1)m}$, and $D_k \in \mathbb{R}^{m\times mk}$ can be written as

$$\Sigma_k^y = \begin{bmatrix} O & I_k \otimes C \end{bmatrix} \Sigma^o \begin{bmatrix} O \\ I_k \otimes C' \end{bmatrix} + I_k \otimes \Sigma_v,$$

$$A_k = \begin{bmatrix} \begin{bmatrix} O_{m\times(\kappa-k)m} & C & O_{m\times(k-1)m} \end{bmatrix} \Sigma^o \begin{bmatrix} O \\ I_{k-1} \otimes C' \end{bmatrix} (\Sigma_{k-1}^y)^\dagger \\ I_{(k-1)m} \end{bmatrix},$$

$$D_k = \begin{bmatrix} O_{m\times(\kappa-k)m} & I_m & O_{m\times(k-1)m} \end{bmatrix} \Sigma^o \begin{bmatrix} O \\ I_k \otimes C' \end{bmatrix} (\Sigma_k^y)^\dagger$$

in terms of $\Sigma^o \in \mathbb{S}^{m\kappa}$, defined in Appendix B.2 by (B.9).

Remark (Sufficiency Condition). Without loss of generality, suppose that $\boldsymbol{s}_k \in \mathbb{R}^{mk}$ instead of $\boldsymbol{s}_k \in \mathbb{R}^m$ such that $\mathcal{P}_S$ can *disclose* $\tilde{\eta}_k(\boldsymbol{y}_{1:k}) = \boldsymbol{y}_{1:k}$ with the affine signaling rule $\tilde{\eta}_k(\cdot)$ from $\mathbb{R}^{mk}$ to $\mathbb{R}^{mk}$. Particularly, in practice, we can always set the signaling rule $\eta_k(\cdot)$ from $\mathbb{R}^{mk}$ to $\mathbb{R}^m$ as

$$\eta_k(\boldsymbol{y}_{1:k}) = \mathbb{E}\{\boldsymbol{x}_k^o | \tilde{\eta}_1(\boldsymbol{y}_1), \ldots, \tilde{\eta}_k(\boldsymbol{y}_{1:k})\}. \tag{3.66}$$

For such a signaling rule $\tilde{\eta}_k(\cdot)$, by following similar lines in Step *ii)* in the proof of Theorem 3.1, we can show that a necessary condition on $Y_{1:\kappa}$ is that $Y_{1:\kappa} \in \Phi$. Furthermore, based on Lemma 3.3, a sufficient condition on $Y_{1:\kappa}$ is that for any $S_{1:\kappa} \in \Phi$, there exists a certain signaling rule such that $Y_{1:\kappa} = S_{1:\kappa}$.

The following corollary to Theorem 3.1 provides an equivalent SDP problem (3.16) when there are noisy measurements.

Corollary 3.7 (Equivalence Result with Noisy or Partial Measurements)**.** *Given $p \in \Delta^{|\Omega|}$, for any signaling rule $\eta_{1:\kappa}$, there exists $S_{1:\kappa} \in \Phi$ such that*

$$U_S(\eta_{1:\kappa}, \{\gamma_{1:\kappa}^{\omega*}(\eta_{1:\kappa})\}_{\omega\in\Omega}, p) = \sum_{k=1}^{\kappa} \mathrm{Tr}\left\{S_k\left(\sum_{\omega\in\Omega} W_k(\omega)\right)\right\} + v_o. \tag{3.67}$$

Furthermore, for any $S_{1:\kappa} \in \Phi$, there exists a signaling rule $\eta_{1:\kappa}$ such that

$$\sum_{k=1}^{\kappa} \mathrm{Tr}\left\{S_k\left(\sum_{\omega\in\Omega} W_k(\omega)\right)\right\} + v_o = U_S(\eta_{1:\kappa}, \{\gamma_{1:\kappa}^{\omega*}(\eta_{1:\kappa})\}_{\omega\in\Omega}, p). \tag{3.68}$$

Based on Corollary 3.7, the following corollary to Theorem 3.5 provides an algorithm to compute the robust sensor outputs for the cases with noisy or partial measurements.

Corollary 3.8 (Computing the Equilibrium with Noisy or Partial Measurements)**.** *The value of the Stackelberg equilibrium*

$$\min_{S\in\bar{\Phi}} \max_{p\in\Delta^{|\Omega|}} \sum_{i\in\mathcal{I}} p_i \mathrm{Tr}\{W_i S\} + v_o, \tag{3.69}$$

where W_i and $\bar{\Phi}$ are defined accordingly, is given by $\vartheta = \min_{j\in\mathcal{I}}\{\vartheta_j\}$, where

$$\begin{aligned}\vartheta_j := \min_{S\in\bar{\Phi}}\ & \mathrm{Tr}\left\{W_j S\right\} + v_o\\ \text{s.t. } & \mathrm{Tr}\left\{(W_j - W_i)S\right\} \geq 0 \ \forall i \in \mathcal{I}.\end{aligned}$$

Furthermore, let $\vartheta_{j^*} = \vartheta$ and

$$\begin{aligned}S^* \in \operatorname*{argmin}_{S\in\bar{\Phi}}\ & \mathrm{Tr}\left\{W_{j^*} S\right\} + v_o\\ \text{s.t. } & \mathrm{Tr}\left\{(W_{j^*} - W_i)S\right\} \geq 0 \ \forall i \in \mathcal{I}.\end{aligned}$$

Given $S^* \in \bar{\Phi}$, the optimal signaling rule $\tilde{\eta}_{1:\kappa}$ can be computed according to Theorem 3.1 with corresponding Σ_k^y and A_k instead of Σ_k^o and A, for $k = 1, \ldots, \kappa$. Then, we can compute the actual signaling rules $\eta_{1:\kappa}$ via (3.66)*.*

3.4 Illustrative Examples

As numerical illustrations, we compare the performance of the proposed secure sensor design framework with classical sensors that disclose the measurement to the controller directly. The controller can have three different types: type-ω_o corresponding to benign controller, and type-α and type-β corresponding to malicious controllers. As an illustrative example, we set the time horizon $\kappa = 10$, the state's dimension $m = 4$, and the control input's dimension $r = 2$. We consider that the state can be partitioned into the separate processes $\{\boldsymbol{t}_k \in \mathbb{R}^2\}$ and $\{\boldsymbol{z}_k \in \mathbb{R}^2\}$, i.e., $\boldsymbol{x}_k' = \begin{bmatrix}\boldsymbol{t}_k' & \boldsymbol{z}_k'\end{bmatrix}$, and the state recursion is given by

$$\begin{bmatrix}\boldsymbol{t}_{k+1}\\ \boldsymbol{z}_{k+1}\end{bmatrix} = \begin{bmatrix}A_t & O\\ O & A_z\end{bmatrix}\begin{bmatrix}\boldsymbol{t}_k\\ \boldsymbol{z}_k\end{bmatrix} + \begin{bmatrix}B_t\\ O\end{bmatrix}\boldsymbol{u}_k + \begin{bmatrix}\boldsymbol{w}_k^t\\ \boldsymbol{w}_k^z\end{bmatrix}, \tag{3.70}$$

where

$$A_t := \begin{bmatrix} 1/\sqrt{2} & 0 \\ 0 & 1/2 \end{bmatrix}, \; A_z := \begin{bmatrix} 1/3 & 1/10 \\ 1/10 & 1/\sqrt{2} \end{bmatrix}, \; B_t := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Furthermore, we let the initial state $\boldsymbol{x}_1 \sim \mathcal{N}(0, \Sigma_1)$ and the state noise $\boldsymbol{w}_k \sim \mathcal{N}(0, \Sigma_w)$ have the covariance matrices:

$$\Sigma_1 := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1.5 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}, \; \Sigma_w := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0.98 & -0.228 \\ 0 & 0 & -0.228 & 0.985 \end{bmatrix},$$

which implies $\{\boldsymbol{z}_k\}$ is a stationary exogenous process. The benign controller objective is given by

$$\sum_{k=1}^{\kappa} \left\| \begin{bmatrix} \boldsymbol{t}_{k+1} - \boldsymbol{z}_{k+1} \\ \boldsymbol{t}_{k+1} \end{bmatrix} \right\|^2 + \|\boldsymbol{u}_k\|^2, \tag{3.71}$$

which implies that type-ω_o controller and $\mathcal{P}_S$ seek to regularize the controlled process $\{\boldsymbol{t}_k\}$ around the zero vector and the exogenous process $\{\boldsymbol{z}_k\}$. On the other hand, the other malicious type controllers' objectives are misaligned with (3.71) rather than being its complete opposite. Let $\boldsymbol{t}_k = \begin{bmatrix} \boldsymbol{t}_k^{(1)} & \boldsymbol{t}_k^{(2)} \end{bmatrix}'$. Then, type-$\alpha$ $\mathcal{P}_C$ seeks to regularize $\{\boldsymbol{t}_k^{(1)} \in \mathbb{R}\}$ around zero and thus the control objective is given by

$$\sum_{k=1}^{\kappa} \left\| \boldsymbol{t}_{k+1}^{(1)} \right\|^2 + \|\boldsymbol{u}_k\|^2. \tag{3.72}$$

Type-β $\mathcal{P}_C$ seeks to regularize the other component of $\boldsymbol{t}_k$, $\{\boldsymbol{t}_k^{(2)} \in \mathbb{R}\}$, again around zero and thus his control objective is given by

$$\sum_{k=1}^{\kappa} \left\| \boldsymbol{t}_{k+1}^{(2)} \right\|^2 + \|\boldsymbol{u}_k\|^2. \tag{3.73}$$

We consider four different scenarios in terms of the measurements:

- Scenario-1: Perfect Measurements, i.e., $\boldsymbol{y}_k = \boldsymbol{x}_k$.
- Scenario-2: Noisy Measurements, i.e., $\boldsymbol{y}_k = \boldsymbol{x}_k + \boldsymbol{v}_k$.
- Scenario-3: Partial Measurements, i.e., $\boldsymbol{y}_k = C\boldsymbol{x}_k$.

- Scenario-4: Partial Noisy Measurements, i.e.,

$$\boldsymbol{y}_k = C\boldsymbol{x}_k + \boldsymbol{v}_k.$$

We let $\boldsymbol{v}_k \sim \mathcal{N}(0, I_4)$ and

$$C := \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \tag{3.74}$$

which is a singular matrix. In Tables 3.1-3.4, we compare the performance of the secure sensor design framework with the classical sensors in terms of the following performance metric:

$$\max_{p \in \Delta^{|\Omega|}} \sum_{k=1}^{\kappa} \operatorname{Tr}\left\{ H_k \sum_{\omega \in \Omega} p_\omega V_k(\omega) \right\}, \tag{3.75}$$

i.e., in terms of the impact of the sensor feedback and for the worst possible distribution over the controllers' types, based on Theorem 3.1 and Corollary 3.7 while $V_{1:\kappa}(\omega)$, for $\omega \in \Omega$, is derived in Appendix B.2.

Remark (Performance Metric). Note that the performance metric (3.75) excludes $v_o \in \mathbb{R}$ from the original cost function (3.17) in perfect measurements case or (3.68) in partial or noisy measurements case since $v_o \in \mathbb{R}$ does not depend on how the measurements have been shared with the controller, and therefore is fixed for all the scenarios. Correspondingly, the performance metric could be *negative* while the original cost function is always non-negative by definition. △

Across Tables 3.1-3.4, i.e., across all Scenarios 1-4, we have the following observations in common: *i*) the proposed framework outperforms the classical sensors that disclose the (perfect or noisy) measurements directly without any crafting; *ii*) the cost for the proposed framework and the classical full disclosure strategy is the same when there is only benign type almost surely; *iii*) the benign type $\mathcal{P}_C$ is dominated by both type-α $\mathcal{P}_C$ and type-β $\mathcal{P}_C$ in the worst distribution, i.e., benign type has zero probability almost surely in the worst distribution; *iv*) type-β $\mathcal{P}_C$ is stronger attacker than type-α $\mathcal{P}_C$ by leading to higher cost.

Table 3.1: Scenario-1: Perfect Measurements. Comparison of the costs between secure sensor design and full information disclosure for the cases with different sets of types. Note that *lower* cost is *desirable*.

	Almost-surely One Type		One Malicious with Benign Type		All Together	
	Secure	Full	Secure	Full	Secure	Full
type-α	−18.19	−14.63	−18.19	−14.63	−12.23	−3.95
type-ω_o	−28.66	−28.66				
type-β	−12.37	−3.95	−12.37	−3.95		

As seen in Table 3.1, in Scenario-1, the cost of the proposed framework for all the cases, i.e., for different sets of types, is the smallest compared to the other scenarios, where there can be partial or noisy measurements. Particularly, the perfect measurements give the utmost *freedom* to $\mathcal{P}_S$ to select the signaling rule. Therefore, if there were any other case with partial or noisy measurements, where $\mathcal{P}_S$ achieves lower cost, then $\mathcal{P}_S$ could have selected that corresponding composed signaling rule in the case with perfect measurement. Partial or noisy measurements limit $\mathcal{P}_S$'s ability to deceive the attackers. Furthermore, we observe that when all the types can exist with a positive probability, the cost is higher than the cases when only one attacker exists. This yields that the worst distribution to defend against is not dominated by the strongest attacker, who is type-β $\mathcal{P}_C$ in this scenario. In other words, the possibility of a mixture over the stronger and weaker attackers can be more powerful.

In Scenarios 2 and 3, as seen in Tables 3.2 and 3.3, the performance degrades compared to Scenario 1 in the proposed framework. However, such a performance degradation is not the case for the full information disclosure in general. As an example, when there is only type-β $\mathcal{P}_C$ almost surely, the

Table 3.2: Scenario-2: Noisy Measurements. Comparison of the costs between secure sensor design and full information disclosure for the cases with different sets of types.

	Almost-surely One Type		One Malicious with Benign Type		All Together	
	Secure	Full	Secure	Full	Secure	Full
type-α	−12.59	−10.13	−12.59	−10.13	−8.71	−2.86
type-ω_o	−20.16	−20.16				
type-β	−8.85	−2.86	−8.85	−2.86		

Table 3.3: Scenario-3: Partial Measurements. Comparison of the costs between secure sensor design and full information disclosure for the cases with different sets of types.

	Almost-surely One Type		One Malicious with Benign Type		All Together	
	Secure	Full	Secure	Full	Secure	Full
type-α	−12.15	−10.42	−12.15	−10.42	−12.09	−10.40
type-ω_o	−18.91	−18.91				
type-β	−12.11	−10.40	−12.11	−10.40		

Table 3.4: Scenario-4: Partial Noisy Measurements. Comparison of the costs between secure sensor design and full information disclosure for the cases with different sets of types.

<table>
<tr><th></th><th colspan="2">Almost-surely
One Type</th><th colspan="2">One Malicious
with Benign Type</th><th colspan="2">All Together</th></tr>
<tr><th></th><th>Secure</th><th>Full</th><th>Secure</th><th>Full</th><th>Secure</th><th>Full</th></tr>
<tr><td rowspan="2">type-α</td><td rowspan="2">−9.94</td><td rowspan="2">−8.73</td><td rowspan="3">−9.94</td><td rowspan="3">−8.73</td><td rowspan="6">−9.75</td><td rowspan="6">−8.55</td></tr>
<tr></tr>
<tr><td rowspan="2">type-ω_o</td><td rowspan="2">−14.89</td><td rowspan="2">−14.89</td></tr>
<tr><td rowspan="3">−9.75</td><td rowspan="3">−8.55</td></tr>
<tr><td rowspan="2">type-β</td><td rowspan="2">−9.75</td><td rowspan="2">−8.55</td></tr>
<tr></tr>
</table>

cost is higher in Scenario 3 than the one in Scenario 1 for full disclosure of the measurement. This is mainly because the objectives of the malicious type controller is not the complete opposite of the benign type controller. Therefore, even though in all the cases illustrated in this section, we have observed that there can even be examples, where the full disclosure of the measurement can lead to a *positive* cost, which would imply that disclosing even no information with the controller would lead to lower cost, i.e., 0, since no information disclosure yields that the covariance of the posterior control-free state is $H_k = O$. Furthermore, we observe that the possibility of a mixture over the stronger and weaker attackers can also be more powerful in Scenarios 2 and 3.

In Scenario-4, as seen in Table 3.4, the cost for the case when there is only the benign type is the highest. However, while the costs for the cases when there is only type-α attacker is higher than the corresponding cases in Scenario-2, the costs for the cases when there is only type-β attacker is *lower* than the corresponding cases in Scenario-2. Note that type-β attacker is still stronger than type-α attacker by leading to higher cost. Furthermore, the costs for the case when all the types can exist with a positive probability also leads to a similar twist, where we observe a higher cost in Scenario-2. We also note that type-β attacker dominates the worst distribution over all the types since the costs for the case where there is only type-β is the same with the cost for the case when there are all types. Therefore, we can conclude that depending on the type of controllers and how informative the measurements are, the costs can vary in a complicated way while the proposed framework provides the optimal way to compute the robust sensor outputs and a performance assessment tool for, e.g., various sensor placement techniques.

3.5 Concluding Remarks

In this chapter, we have proposed and addressed the robust sensor design problem for cyber-physical systems with linear Gaussian dynamics against multiple advanced and evasive attackers with quadratic control objectives. By designing sensor outputs cautiously in advance, we have sought to deceive the attackers about the underlying state of the system so that they would act/attack to the system in-line with the normal operation. Our goal has been to exploit the aligned part between the attackers' and the system's objectives so that the attackers would only have fulfilled the aligned part by crafting the information available to them. To this end, we have modeled the problem formally in a game-theoretical hierarchical setting, where the advanced attackers can be aware of the designed signaling rules.

We have formulated an equivalent problem to the problem faced by the sensor against any attacker with a known objective. This new problem was an SDP problem. We have introduced additional linear constraints on that equivalent problem and provided an SDP algorithm to compute the optimal robust sensor design strategies against multiple types of attackers. We have also extended the results to scenarios where the sensor could have access to partial or noisy measurements of the underlying state. Finally, we have examined the performance of the proposed framework across various scenarios and compared with the classical sensor outputs that disclose the measurements directly without any crafting.

Some future directions of research on this topic include formulation of secure sensor design strategies for robust control of systems, and considering scenarios where the attackers can have side information about the underlying state, which would limit the sensor's ability to deceive the attackers. Another interesting research direction would be the application of the framework to sensor placement or sensor selection. Furthermore, even though we have motivated the framework by relating it to security, the framework could also address strategic information disclosure over multi-agent control networks with misaligned control objectives.

4

SIGNALING FOR GENERAL DISTRIBUTIONS

> *There are two ways to induce a person to do something. One is to provide incentives, by which we mean anything which changes marginal utility–explicit payments, coercion, or supply of complementary goods. The other is to persuade, by which we mean anything which changes beliefs.*
>
> – Emir Kamenica and Matthew Gentzkow [15]

To induce intelligent decision makers to take certain actions, we can create incentives via external means, e.g., explicit payments, but we can also persuade them to take the actions by their own will without the need for any external means if we can craft the information available to them [15]. In informed (rational) decisions, understanding of *how* the information is generated plays an essential role. Without such an understanding, rationality necessitates the consideration of *who* generates the information. For example, if the objectives of the information provider and the decision maker are known to be misaligned, then the rational decision maker should take into account that the (selfish) information provider must have generated the information in a way that manipulates the decision. Such a problem of interest was originally introduced and analyzed by Crawford and Sobel in their inaugural paper [4]. They have considered the scenarios where the information of interest is drawn from a compact state space according to a commonly known distribution. When the (quite general) cost measures of the players are misaligned by a commonly known bias term, the authors have drawn the conclusion that in any incentive compatible, i.e., Nash, equilibrium, the information provider partitions the state space in a certain way and then signals the partition of the information realized.

On the other hand, if how the information/signal is generated is transparent to the decision maker, the decision maker would just follow the (non-strategic) machinery of the Bayesian reaction. Correspondingly, transparency of the signals sent gives more power to the information provider seeking to control the rational reaction of the decision maker. This brings in the possibility of persuading intelligent decision makers to take certain actions through transparent information transmissions. One way to ensure transparency is the commitment power of the information provider. Relatively recently, such a problem of interest has been examined by Kamenica and Gentzkow in their seminal paper [15]. They have considered the scenarios where the decision maker is aware of the content of the messages received due to the committed transparency/honesty even though the information provider may not reveal the underlying information completely. They have provided a geometrical interpretation of the optimal persuasive signaling strategy and examined the persuasion capability of the information provider. A detailed justification of the information provider's commitment power can be found in [15] and a recent survey of literature on Bayesian persuasion could be found in [21].

In this chapter, we are also interested in the signaling models with policy commitment. As a special subclass[1] of the Bayesian persuasion framework, here the information provider is interested in the perception of the decision maker about the underlying information of interest with respect to some quadratic cost measure rather than any decision made (possibly) based on that perception. Without loss of generality, we incorporate the commitment power of the information provider via a hierarchical structure where the information provider leads the interaction from a hierarchically higher position by announcing his/her signaling strategies publicly. This hierarchical viewpoint enables us to examine the interaction between the information provider and the decision maker under the solution concept of Stackelberg equilibrium [3], where the information provider is the leader.

We note that hierarchical signaling could have important applications in multi-agent noncooperative environments since asymmetry of information that agents have access to is prevalent due to the diversity of the agents' perspectives. For example, distributed signal processing over sensor networks seeks to exploit this diversity through information exchanges among cooperative sensors in order to broaden their horizons (e.g., see [83]). However, in a noncooperative environment, selfish agents could have incentive to share

[1] We name this sub-class "hierarchical signaling" to distinguish it from general Bayesian persuasion.

the information private to them strategically with the other agents in order to gain advantage with respect to their own distinct objective. Correspondingly, as argued in [84], commitment/transparency could play an important role for the credibility of the agents on the long run. Furthermore, in adversarial environments, commitment of the defender could be viewed as the defender avoiding the vulnerability of obscurity based defense against the possibility that the attacker could have learned the defense strategy, e.g., via regression analysis, once it is deployed widely.

Prior Literature Originating in the fields of economics, recently, strategic signaling has also attracted significant attention in the fields of communication and control due to its compelling applications in noncooperative multi-agent environments. Due to the versatility of Gaussian distribution in engineering applications, these studies have mainly focused on Gaussian information models, different from the literature in the economics.

Within the framework of [4], in [29], the authors have identified the condition under which a non-partition equilibrium can exist in the scenarios where the underlying information is Gaussian, there exists an additive Gaussian noise channel, the players have quadratic cost measures, and the information provider has a soft power constraint on the signal sent. Under the solution concept of Stackelberg equilibrium, in [31], the authors have studied the problem setting of [4] when the misalignment factor between the objectives of the information provider and the decision maker, i.e., the bias term, is private to the information provider. They have shown that the optimal signaling strategy is linear in the scenarios where the underlying information is (multivariate) Gaussian, the players have quadratic cost measures, and the decision maker has bounded rationality by using linear estimates only. Indeed, for the same settings of [31], in [22], the author had shown that the optimal signaling strategy is linear even when the decision maker is completely rational by selecting any measurable decision policy and provided an analytical formulation of the optimal signaling strategy. Under the same settings with [31] yet for a completely rational receiver and scalar Gaussian information, [30] has shown the optimality of linear signaling strategies when there is an additive Gaussian noise channel and the information provider has a hard power constraint.

In the earlier chapters, we have addressed hierarchical Gaussian signaling in non-cooperative dynamic communication and control systems over a finite horizon. For discrete-time (multivariate) Gauss-Markov processes, in Chapter 2, we have shown the optimality of linear signaling strategies within the general class of measurable policies and formulated an equivalent (in optimality) semi-definite program (SDP), which enables computation of the optimal signaling strategies numerically through existing SDP solvers efficiently. In [42], we have shown that the equivalence to an SDP is not limited to equivalence in optimality and would still hold when we include certain additional constraints in the optimization. In that way, for non-cooperative linear quadratic Gaussian control problems, we have addressed in Chapter 3 optimal linear signaling strategies of a sensor who seeks to deceive a private-type controller in settings where the distribution over the types of the controller is not known.

For Gaussian information, we can obtain well structured results, e.g., linear signaling strategies, also in dynamic and noisy environments, as shown in the studies reviewed above. However, for distributions other than Gaussian, we still have significant but yet not completely explored problems. Notably, for general distributions with compact support, [15] brings in a geometrical interpretation into the problem, which requires the computation of a convex envelope of a function, which can be prominently challenging even for finite yet relatively large state spaces [85]. We also note that, as studied in [86–88], a relatively simpler characterization of the solution is possible for a special class of Bayesian persuasion problems, which is different from our problem settings. There have also been computational approaches for the Bayesian persuasion problem, e.g., [89, 90]. Particularly, the non-strategic nature of the decision maker makes it possible to formulate the problem as a single optimization problem faced by the information provider. Based on the revelation principle, the authors formulate a linear program to compute the optimal signaling strategy, which, however, turns out to be impractical to solve numerically unless the finite state space is fairly small [89, 90]. Therefore the authors consider the scenarios where the players' cost measures are independently (and identically) drawn from a known distribution for each state, and examine connections with auction theory. We also note that for such an LP formulation, the action space of the receiver is considered to be finite, however, in our setting, the receiver's decision is his/her belief and correspondingly his/her action space is a continuum even when the underlying information is discrete.

Contributions of This Chapter In this chapter, our goal is to address hierarchical signaling for a general class of square integrable multivariate distributions. We again consider the scenario where there are two decision makers: a sender and a receiver. The sender has access to the realizations of two random vectors (with commonly known statistical profiles): information of interest and some private information. The receiver seeks to estimate the information of interest in the mean-square-error sense based on the signal he/she receives. To this end, the receiver seeks to compute the optimal Bayesian (possibly nonlinear) estimate of the information of interest using the signal he/she receives. However, the sender constructs the signal strategically in a stochastic way in order to deceive the receiver to perceive the information of interest as that private information with respect to another quadratic cost measure. The sender selects the signaling strategy from the general class of stochastic kernels. Furthermore, by turning the problem around, the proposed setting could also be applicable to preserve privacy. While sharing the information of interest, the sender could seek to minimize the informational leakage of the private information when the information of interest and the private information are not independent of each other. Although we mainly focus on the former, i.e., deceptive signaling, problem, we will also show how the results would be extended to the latter, i.e., persuasive privacy, problem.

Under the solution concept of Stackelberg equilibrium, where the sender is the leader, we seek to compute the least possible cost for the sender at an equilibrium. Note that a Stackelberg game admits a unique value for the leader at all the equilibria if they exist. Particularly, the follower reacts in a non-strategic way given the leader's strategy. Correspondingly, we can formulate the problem faced by the leader as a "single" optimization problem by characterizing the follower's non-strategic reaction. In other words, the commitment power of the sender brings the signaling problem into the domain of optimization instead of fixed-point analysis as in the incentive compatible models, e.g., [4].

For any signaling strategy, the optimal reaction of the receiver is given by the conditional expectation of the information of interest, where the conditioning is on the signal sent by the sender. We note that in general, it is challenging to obtain the conditional expectation in an analytical form for arbitrary joint statistical profiles of the signal and the information of interest.

Therefore, we seek to examine the problem faced by the sender further in order to transform it into a structured, exploitable, form. As shown in [22], the problem faced by the sender turns out to be a linear function of the correlation matrix of the posterior estimate. We note that the relationship between the correlation matrix of the posterior estimate and the signaling strategies is highly nonlinear. However, by characterizing tractable necessary and sufficient conditions on the correlation matrix of the posterior estimate enables us to compute the minimum cost for the sender. In [42], we have shown that for Gaussian distributions, the necessary and sufficient condition on the correlation matrix of the posterior can be expressed via certain linear matrix inequalities while these linear matrix inequalities are not sufficient for the general class of distributions. This is another intriguing feature of Gaussian distribution which provides the sender with utmost flexibility to deceive the receiver within the general class of square integrable distributions with fixed mean and covariance.

As an initial step toward addressing the problem for arbitrary distributions, we first consider discrete distributions. Although, now, the problem is a finite-dimensional optimization problem, obtaining its solution is still challenging due to its highly nonlinear and non-convex nature. One of our contributions in this chapter is to transform this challenging problem into a structured, exploitable, form. To this end, we formulate an equivalent linear optimization problem over the convex cone of completely positive matrices. We say that a matrix $\Xi \in \mathbb{R}^{n\times n}$ is completely positive if there exists an (entry-wise) non-negative matrix $B \in \mathbb{R}_+^{n\times k}$ such that $\Xi = BB'$ [91]. Even though it is a linear optimization problem, the cone of completely positive matrices is still not tractable [91]. Furthermore, the proof of equivalence is constructive yet requires the factorization of a completely positive matrix (see [92, 93]). Notably this cone turns out to be tractable for sizes up to 4 [91, 94].

On the other hand, the dual of the equivalent problem is a linear optimization problem over the cone of copositive matrices. We say that a symmetric matrix $A \in \mathbb{S}^n$ is copositive provided that $\underline{b}'A\underline{b} \geq 0$ for all $\underline{b} \in \mathbb{R}_+^n$ [91]. We can show that the strong duality is attained for our problem setting. We note that some classes of NP-hard problems could be transformed into copositive programs [95]. It is an active research area to exploit the compact structure of the cone of copositive matrices to approximate the underlying constraint space with sequential polyhedral or semi-definite cones for any accuracy level at the expense of computational complexity, e.g., [95–100]. Therefore, by transforming the hierarchical signaling problem into this class of problems, we can benefit from these powerful computational tools developed (or to be developed) in the optimization community over the course of time. We examine the approximation power of the proposed solution concept given a discretization of a continuous distribution via, e.g., a quantization scheme [101]. We also formulate an upper bound on the approximation error in terms of the quantization error. Finally, we examine the performance of the proposed solution concept over various numerical examples.

We can list the main contributions of this chapter as follows:

- We address the problem of optimal hierarchical signaling to deceive a receiver to perceive the underlying information of interest as some private information for a general class of distributions.

- We show that the proposed solution concept also works for privacy applications where a sender seeks to minimize the informational leakage on his/her private information while sharing the information of interest with the receiver.

- For discrete distributions, we formulate an equivalent linear optimization problem over the convex cone of completely positive matrices and show its strong duality with a linear optimization problem over the convex cone of copositive matrices. This equivalence enables us to use the existing computational tools [95–97] to solve this class of problems at any level of accuracy.

- We formulate an upper bound on the error of approximation if we use the proposed solution concept for a discretized version of the underlying continuous distribution, e.g., via a quantization scheme.

The chapter is organized as follows: In Section 4.1, we formulate the deceptive signaling game for the general class of continuous distributions. In Section 4.2, we compute the optimal signaling strategy for finite state spaces by formulating an equivalent linear optimization problem over the cone of completely positive matrices, and examine the loss induced if we use the proposed solution concept for a discretized version of a continuous state space. In Section 4.3, we discuss the computational approaches to solve the equivalent optimization problem. In Section 4.4, we provide illustrative numerical

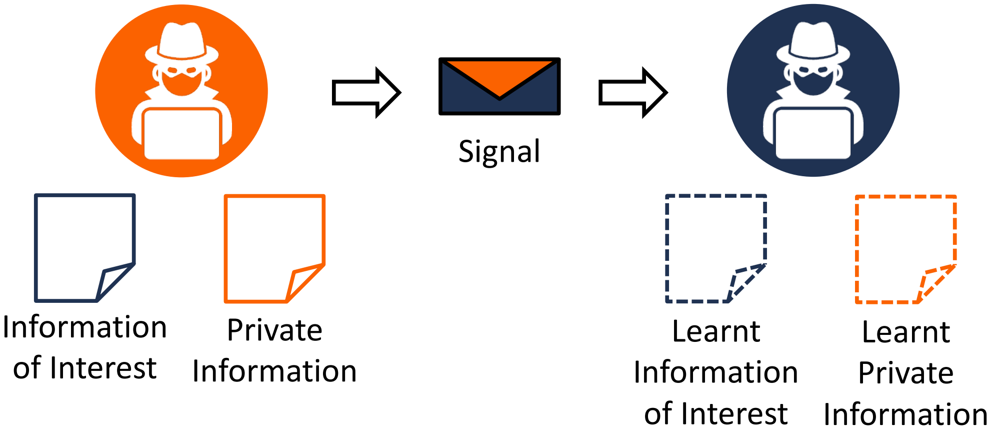


Figure 4.1: Hierarchical signaling model, where a sender has access to some information of interest as well as private information, and sends a signal composed of them to a receiver while the receiver seeks to learn the information of interest. The receiver will be learning both of them while the sender seeks to induce the receiver to perceive the information of interest as the private information.

examples. Section 4.5 concludes the chapter with several remarks and possible research directions.

4.1 Problem Formulation

Consider two non-cooperating decision makers: a sender ($\mathcal{P}_S$) and a receiver ($\mathcal{P}_R$), as seen in Fig. 4.1. $\mathcal{P}_S$ has access to an underlying information of interest and also to some private information, which are realizations of m-dimensional random vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ with supports $\mathcal{X} \subset \mathbb{R}^m$ and $\mathcal{Y} \subset \mathbb{R}^m$, respectively. The supports are not necessarily compact and can be as large as the entire $\mathbb{R}^m$, e.g., the support of a multivariate Gaussian distribution. The random variables 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.,

$$(\Omega, \mathcal{F}, \mathbf{P}) \xrightarrow{\boldsymbol{x}} (\mathcal{X}, \mathcal{B}^m, \mathbf{P}_x), \tag{4.1}$$

$$(\Omega, \mathcal{F}, \mathbf{P}) \xrightarrow{\boldsymbol{y}} (\mathcal{Y}, \mathcal{B}^m, \mathbf{P}_y), \tag{4.2}$$

where $\mathcal{B}^m$ denotes the Borel σ-algebra on $\mathbb{R}^m$. We note that explicit definition of the probability space does not play a role in the analysis. We consider the scenarios where $\boldsymbol{x}$ and $\boldsymbol{y}$ belong to the normed space of all square integrable m-dimensional random vectors with the norm: $\|\boldsymbol{x}\| = \mathbb{E}\{\boldsymbol{x}'\boldsymbol{x}\}^{1/2}$.

$\mathcal{P}_S$ selects his[2] strategy $\pi(\cdot)$ as a "stochastic kernel" from $\mathcal{X}\times\mathcal{Y}$ to $\mathcal{S}\subset\mathbb{R}^{2m}$ such that the signal sent is given by

$$\boldsymbol{s} = \pi(\boldsymbol{x},\boldsymbol{y}), \text{ a.e. over } \mathcal{S}. \tag{4.3}$$

Let us denote the set of all such signaling rules by Π, i.e., $\pi\in\Pi$. On the other side, after a realization of the signal sent is received, $\mathcal{P}_R$ selects her strategy $\gamma(\cdot)$ that is a Borel measurable function from $\mathcal{S}$ to $\mathcal{X}$ such that her estimate of the underlying information is given by

$$\hat{\boldsymbol{x}} = \gamma(\boldsymbol{s}), \text{ a.e. over } \mathcal{X}. \tag{4.4}$$

The strategy space of $\mathcal{P}_R$ is denoted by Γ, which is the set of all measurable functions from $\mathcal{S}$ to $\mathcal{X}$.

The decision makers select their strategies according to distinct cost measures. $\mathcal{P}_R$ has the cost measure

$$c_R(\pi,\gamma) = \|\boldsymbol{x}-\hat{\boldsymbol{x}}\|^2 \tag{4.5}$$

to be minimized via $\gamma\in\Gamma$, i.e., seeks to estimate the underlying information of interest. On the other side, $\mathcal{P}_S$ has the cost measure

$$c_S(\pi,\gamma) = \|\boldsymbol{y}-\hat{\boldsymbol{x}}\|^2 \tag{4.6}$$

to be minimized via $\pi\in\Pi$, i.e., seeks to induce $\mathcal{P}_R$ to perceive the information of interest as the private information instead of true itself.

We consider a hierarchical setting where $\mathcal{P}_R$ makes a Bayes estimate of the information of interest based on the signal received by knowing the content of the signal, i.e., the signaling rule $\pi\in\Pi$. Correspondingly, we model the interaction between the decision makers under the solution concept of Stackelberg equilibrium [3], where $\mathcal{P}_S$ is the leader, who commits and announces

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

to play his strategy beforehand, while $\mathcal{P}_R$ is the follower, who selects her strategy knowing $\mathcal{P}_S$'s strategy. In particular, we can view the sequence of moves as follows:

1. $\mathcal{P}_S$ selects $\pi \in \Pi$ according to (4.6) and by anticipating the optimal response of $\mathcal{P}_R$.

2. $\mathcal{P}_R$ observes the signaling rule chosen by $\mathcal{P}_S$ and selects $\gamma \in \Gamma$ according to (4.5).

3. Nature chooses the outcome $\omega \in \Omega$, and correspondingly $x = \boldsymbol{x}(\omega)$, $y = \boldsymbol{y}(\omega)$, and $s = \boldsymbol{s}(\omega)$, which is $\boldsymbol{s}(\omega) = \pi(\boldsymbol{x}(\omega), \boldsymbol{y}(\omega))$.

4. $\mathcal{P}_R$ observes the realization $s \in \mathcal{S}$.

5. $\mathcal{P}_R$ estimates $x \in \mathcal{X}$ given $s \in \mathcal{S}$ via $\gamma \in \Gamma$.

Note that we can view the estimate of $x \in \mathcal{X}$ as a realization of the random vector $\hat{\boldsymbol{x}}$, as described in (4.4). In the following, we provide a formal description of this game.

Definition (Deceptive Signaling Game). The deceptive signaling game

$$\mathcal{G} := (\Pi, \Gamma, \boldsymbol{x}, \boldsymbol{y}, c_S(\cdot), c_R(\cdot)) \tag{4.7}$$

is a Stackelberg game between the leader $\mathcal{P}_S$ and the follower $\mathcal{P}_R$. We let $B(\pi) \subset \Gamma$ be the optimum reaction set of the follower $\mathcal{P}_R$ for a given strategy $\pi \in \Pi$ of $\mathcal{P}_S$. Then, the pair of the strategy and the optimum reaction set $(\pi^*, B(\pi^*))$ attains the Stackelberg equilibrium provided that

$$\pi^* \in \operatorname*{argmin}_{\pi \in \Pi} \max_{\gamma \in B(\pi)} c_S(\pi, \gamma) \tag{4.8a}$$

$$B(\pi) = \operatorname*{argmin}_{\gamma \in \Gamma} c_R(\pi, \gamma). \tag{4.8b}$$

Note that different from the previous literature on Bayesian persuasion, here $\mathcal{P}_S$ considers the scenarios where $\mathcal{P}_R$ breaks the tie in the reverse direction of $\mathcal{P}_S$'s favor, which would be more justifiable given the deceptive intention of $\mathcal{P}_S$. However, in our case, due to the strictly convex cost measure of $\mathcal{P}_R$, the best reaction set of $\mathcal{P}_R$ for any given signaling strategy $\pi \in \Pi$ will already turn out to be a singleton with probability 1.

We also note that we can turn the problem around by considering different quadratic cost measures so that the proposed solution concept could also have applications for, e.g., privacy, as long as the cost measures are quadratic and $\mathcal{P}_R$'s optimum reaction turns out to be the mean of the posterior estimate. In that respect, we introduce the "persuasive privacy" problem, where $\mathcal{P}_S$ and $\mathcal{P}_R$ have a contract dictating $\mathcal{P}_S$ to disclose the information of interest $\boldsymbol{x}$, but following the contract, $\mathcal{P}_S$ also seeks to control the perception of $\mathcal{P}_R$ about the private information $\boldsymbol{y}$ since $\mathcal{P}_R$ could infer the private information based on the signal sent. Correspondingly, if $\boldsymbol{x}$ and $\boldsymbol{y}$ are not completely independent of each other, direct disclosure of $\boldsymbol{x}$ could reveal $\boldsymbol{y}$ to a certain extent. Therefore, $\mathcal{P}_S$ might seek to preserve such leakage of private information by signaling to $\mathcal{P}_R$ strategically. For example, we might view $\mathcal{P}_R$ seeking to estimate both $\boldsymbol{x}$ and $\boldsymbol{y}$ based on the signal $\boldsymbol{s} = \pi^p(\boldsymbol{x},\boldsymbol{y})$. To this end, $\mathcal{P}_R$ selects decision rules $\gamma_x^p : \mathcal{X} \to \mathcal{X}$ and $\gamma_y^p : \mathcal{Y} \to \mathcal{Y}$ that minimize

$$c_R^p(\pi^p,\gamma^p) = \|\boldsymbol{x} - \gamma_x^p(\pi^p(\boldsymbol{x},\boldsymbol{y}))\|^2 + \|\boldsymbol{y} - \gamma_y^p(\pi^p(\boldsymbol{x},\boldsymbol{y}))\|^2,$$

where $\gamma^p := (\gamma_x^p, \gamma_y^p) \in \Gamma^p$ and Γ^p denotes the space of such decision rule pairs. On the other side, $\mathcal{P}_S$ constructs the signal $\boldsymbol{s}$ via a signaling rule $\pi^p \in \Pi$ to minimize

$$c_S^p(\pi^p,\gamma^p) = \|\boldsymbol{x} - \gamma_x^p(\pi^p(\boldsymbol{x},\boldsymbol{y}))\|^2 - \|\boldsymbol{y} - \gamma_y^p(\pi^p(\boldsymbol{x},\boldsymbol{y}))\|^2.$$

We note that the sign of the second term in the cost measure of $\mathcal{P}_R$ is positive since $\mathcal{P}_R$ seeks to estimate the private information $\boldsymbol{y}$, whereas the sign of the second term in the cost measure of $\mathcal{P}_S$ is negative since $\mathcal{P}_S$ seeks to maximize the estimation error of $\mathcal{P}_R$ for the private information.

Similar to the description of the deceptive signaling game $\mathcal{G}$, in the following, we provide a formal description of this "persuasive privacy" game.

Definition (Persuasive Privacy Game). The persuasive privacy game

$$\mathcal{G}^p := (\Pi, \Gamma^p, \boldsymbol{x}, \boldsymbol{y}, c_S^p(\cdot), c_R^p(\cdot)) \tag{4.9}$$

is a Stackelberg game between the leader $\mathcal{P}_S$ and the follower $\mathcal{P}_R$. The pair of the strategy and the optimum reaction set $(\pi^p, B^p(\pi^p))$ attains the

Stackelberg equilibrium provided that

$$\pi^p \in \operatorname*{argmin}_{\pi \in \Pi} \max_{\gamma \in B^p(\pi)} c_S^p(\pi, \gamma) \tag{4.10a}$$

$$B^p(\pi) = \operatorname*{argmin}_{\gamma \in \Gamma^p} c_R^p(\pi, \gamma). \tag{4.10b}$$

In the following, we mainly address the deceptive signaling game $\mathcal{G}$ while remarking how the results would also be applicable for the persuasive privacy game $\mathcal{G}^p$.

4.2 Main Result

Before delving into the technical details, in the following we first provide an overview of the main result of this chapter and the steps we follow toward its solution. We first focus on identifying the underlying optimization problem faced by $\mathcal{P}_S$. Note that $\mathcal{P}_R$ follows the machinery of Bayesian estimation for any signaling rule selected/committed by $\mathcal{P}_S$. By incorporating this (non-strategic) machinery into $\mathcal{P}_S$'s cost measure (4.6), we can write the optimal hierarchical signaling problem as a single optimization problem faced by $\mathcal{P}_S$.

Before addressing the problem for the general class of distributions, we seek to address the problem for finite state spaces. This will also enable us to formulate the best achievable performance for $\mathcal{P}_S$ approximately for continuous distributions if we discretize them via, e.g., a quantization scheme. Although the problem faced by $\mathcal{P}_S$ is no longer an infinite-dimensional optimization problem when the underlying state space is finite, the problem turns out to be a highly nonlinear and non-convex optimization problem. To mitigate this issue, we formulate an equivalent linear optimization problem over the cone of completely positive matrices. Although this problem is a linear optimization problem, which has compact structure, because of the underlying constraint space, i.e., the cone of completely positive matrices, it is not tractable and indeed some classes of NP-hard problems could be transformed into this form [91]. The difficulty of this equivalent problem is also a formal indication of the difficulty level for the original optimization problem. In other words, a polynomial-time solution for the hierarchical signaling problem would have implied a polynomial-time solution for a large class of completely positive programs.

Furthermore, the dual of the equivalent problem is a linear optimization problem over the cone of copositive matrices, and we can show that the strong duality is attained for our problem setting. However, this cone is also not tractable, but its compact structure enables us to approximate the underlying constraint space with sequential polyhedral or semi-definite cones for any level of accuracy at the expense of computational complexity [95–97]. Therefore, by transforming the hierarchical signaling problem into this form, we can use these existing computational tools. In order to extend the results to continuous distributions, we examine the approximation error on the cost metric of $\mathcal{P}_S$ when the underlying distribution is discretized via a given quantization scheme. In the following, we provide the technical details.

4.2.1 Optimization Problem Faced by $\mathcal{P}_S$

Since $\mathcal{P}_R$'s objective is a mean-square-error minimization problem, as described in (4.5), it is well known that the best reaction of $\mathcal{P}_R$, for any given signaling rule $\pi \in \Pi$, is uniquely given by $\hat{\boldsymbol{x}} = \mathbb{E}\{\boldsymbol{x}|\boldsymbol{s}\}$ almost everywhere over $\mathcal{X}$. Consider the augmented vector $\boldsymbol{z} := \begin{bmatrix}\boldsymbol{x}' & \boldsymbol{y}'\end{bmatrix}'$ composed of the information of interest $\boldsymbol{x}$ and the private information $\boldsymbol{y}$. We denote the support of $\boldsymbol{z}$ by $\mathcal{Z} := \mathcal{X} \times \mathcal{Y}$ and define $\hat{\boldsymbol{z}} := \mathbb{E}\{\boldsymbol{z}|\boldsymbol{s}\}$ almost everywhere over $\mathcal{Z}$. Henceforth we will call $\hat{\boldsymbol{z}}$ "posterior" instead of posterior estimate of the augmented vector.

Through this new auxiliary parameter, we can write the problem faced by $\mathcal{P}_S$ in a compact form. To this end, let the optimum reaction of $\mathcal{P}_R$ for a committed signaling strategy $\pi \in \Pi$ be denoted by $\gamma^*(\pi)$ so that we can show its dependence on π explicitly. Then the problem faced by $\mathcal{P}_S$, as defined in (4.6), can be written as

$$c_S(\pi, \gamma^*(\pi)) = \operatorname{Tr}\{\mathbb{E}\{\boldsymbol{y}\boldsymbol{y}'\}\} + \operatorname{Tr}\{V\mathbb{E}\{\hat{\boldsymbol{z}}\hat{\boldsymbol{z}}'\}\}, \tag{4.11}$$

where

$$V := \begin{bmatrix} I & -I \\ -I & O \end{bmatrix} \tag{4.12}$$

since we have $\mathbb{E}\{\boldsymbol{z}\hat{\boldsymbol{z}}'\} = \mathbb{E}\{\mathbb{E}\{\boldsymbol{z}\hat{\boldsymbol{z}}'|\boldsymbol{s}\}\} = \mathbb{E}\{\hat{\boldsymbol{z}}\hat{\boldsymbol{z}}'\}$.

Remark. In the persuasive privacy game $\mathcal{G}^p$, the optimum reaction of $\mathcal{P}_R$ would be $\gamma_x^p(\boldsymbol{s}) = \mathbb{E}\{\boldsymbol{x}|\boldsymbol{s}\}$, almost everywhere over $\mathcal{X}$, and $\gamma_y^p(\boldsymbol{s}) = \mathbb{E}\{\boldsymbol{y}|\boldsymbol{s}\}$, almost everywhere over $\mathcal{Y}$. Correspondingly, the problem faced by $\mathcal{P}_S$ could be written in that case as

$$c_S^p(\pi^p, \gamma^p(\pi^p)) = \mathrm{Tr}\left\{V^p \mathbb{E}\left\{\hat{\boldsymbol{z}}\hat{\boldsymbol{z}}'\right\}\right\} - \mathrm{Tr}\left\{V^p \mathbb{E}\left\{\boldsymbol{z}\boldsymbol{z}'\right\}\right\}, \tag{4.13}$$

where

$$V^p := \begin{bmatrix} -I & O \\ O & I \end{bmatrix}. \tag{4.14}$$

The following results are also applicable to $\mathcal{G}^p$ if we simply replace $V \in \mathbb{S}^{2m}$ by $V^p \in \mathbb{S}^{2m}$.

Therefore, the infinite-dimensional optimization problem faced by $\mathcal{P}_S$ can be written as

$$\mathrm{Tr}\left\{\mathbb{E}\left\{\boldsymbol{y}\boldsymbol{y}'\right\}\right\} + \min_{\pi\in\Pi} \mathrm{Tr}\left\{V \mathbb{E}\left\{\hat{\boldsymbol{z}}\hat{\boldsymbol{z}}'\right\}\right\}, \tag{4.15}$$

where we have taken the first term at the right-hand side of (4.11) out of the optimization objective since $\mathrm{Tr}\left\{\mathbb{E}\left\{\boldsymbol{y}\boldsymbol{y}'\right\}\right\}$ has a fixed value, i.e., does not depend on the optimization argument $\pi \in \Pi$. Furthermore, the problem faced by $\mathcal{P}_S$ depends on the optimization argument $\pi \in \Pi$ only via[3] $\mathbb{E}\left\{\hat{\boldsymbol{z}}\hat{\boldsymbol{z}}'\right\}$ while the optimization objective is linear in $\mathbb{E}\left\{\hat{\boldsymbol{z}}\hat{\boldsymbol{z}}'\right\}$. This motivates us to examine the relation between the correlation matrix of the posterior $\mathbb{E}\left\{\hat{\boldsymbol{z}}\hat{\boldsymbol{z}}'\right\}$ and the signaling rule $\pi \in \Pi$ further.

Instead of attempting the problem as direct optimization on the strategy space of $\mathcal{P}_S$, we seek to formulate the necessary and sufficient conditions on the correlation matrix of the posterior estimate. Note that the optimization objective (4.15) depends on the (infinite-dimensional) optimization argument $\pi \in \Pi$ only through a (finite-dimensional) matrix corresponding to the correlation matrix of the posterior estimate of the underlying information. By exploiting the relation between the signaling strategies and the correlation matrix of the posterior estimate, we seek to obtain a tractable finite-dimensional problem equivalent to the original infinite-dimensional optimization problem. This has already been shown to be possible via a linear optimization problem with tractable constraints, e.g., linear matrix inequalities, for the special class of Gaussian distributions [22,42]. In [42], however, we have also shown that this finite-dimensional problem can only be viewed as a lower bound (indeed not a tight one) for the general class of distributions.

[3] Information drawn from square integrable distributions ensures that $\mathbb{E}\left\{\hat{\boldsymbol{z}}\hat{\boldsymbol{z}}'\right\}$ is well defined.

4.2.2 An Equivalent Problem over the Cone of Completely Positive Matrices

In order to address (4.8) in the most general form, let us first focus on the special case where $n := |\mathcal{Z}| < \infty$. Recall that the geometrical approach developed in [15] can be used effectively for finite state spaces with fairly small sizes, while the geometrical approach developed in [86] can be effectively used for relatively larger size problems if the problem faced by $\mathcal{P}_S$ only depends on the mean of the posterior. Therefore the solution for (4.8) has remained open even for finite state spaces since here the problem faced by $\mathcal{P}_S$ depends on the correlation matrix of the posterior. Further, by addressing (4.8) for finite state spaces at large scales brings in the possibility of addressing (4.8) approximately for continuum state spaces.

Taking the state space to be finite, we can restrict ourselves to the scenarios where $n \leq k := |\mathcal{S}| < \infty$ without loss of generality. In the web appendix of [15], the authors have shown that the size of the signal space can be set the same with the size of the state space, i.e., $k = n$, without loss of generality. However, we do not impose such an upper bound on k. We can view the signaling strategy selected by $\mathcal{P}_S$ as if $\mathcal{P}_S$ selects a mixed strategy over $\mathcal{S}$ for each $z \in \mathcal{Z}$, i.e., determines the probabilities of sending the signals in $\mathcal{S}$. With a slight abuse of notation, we denote the probability that $\mathcal{P}_S$ sends $s \in \mathcal{S}$ for $z \in \mathcal{Z}$ by $\pi(s|z) \in [0,1]$. Note that for each $z \in \mathcal{Z}$, $\mathcal{P}_S$ will be sending a signal with probability 1, which yields that

$$\sum_{s \in \mathcal{S}} \pi(s|z) = 1. \tag{4.16}$$

Note that null signaling, i.e., sending no signal, does not lead to a contradiction since it can practically be viewed as sending the same signal for all the states. Suppose that the prior distribution has complete support on $\mathcal{Z}$ and let $p_o(z) \in (0,1]$ denote the probability that the state $z \in \mathcal{Z}$ is realized. Then Bayes rule yields that the probability of state $z \in \mathcal{Z}$ being realized given that signal $s \in \mathcal{S}$ is received is given by[4]

$$p_s(z) := \frac{\pi(s|z)p_o(z)}{p(s)}, \tag{4.17}$$

[4] A signal $s \in \mathcal{S}$ would be received if the associated probability is positive, i.e., $p(s) > 0$.

where $p(s)$, denoting the probability that the signal $s \in \mathcal{S}$ is sent, is given by

$$p(s) = \sum_{z \in \mathcal{Z}} \pi(s|z) p_o(z). \tag{4.18}$$

Therefore, for given $s \in \mathcal{S}$, we have

$$\hat{z} := \mathbb{E}\{\boldsymbol{z}|\boldsymbol{s} = s\} = \sum_{z \in \mathcal{Z}} p_s(z) z, \tag{4.19}$$

which yields that

$$\mathbb{E}\{\hat{\boldsymbol{z}}\hat{\boldsymbol{z}}'\} = \sum_{s \in \mathcal{S}} p(s) \left(\sum_{z \in \mathcal{Z}} p_s(z) z \right) \left(\sum_{z \in \mathcal{Z}} p_s(z) z' \right). \tag{4.20}$$

We can write the correlation matrix of the posterior (4.20) in a compact form as

$$\mathbb{E}\{\hat{\boldsymbol{z}}\hat{\boldsymbol{z}}'\} = Z \Xi_\pi Z', \tag{4.21}$$

where $Z := \begin{bmatrix} z_1 \dots z_n \end{bmatrix} \in \mathbb{R}^{2m \times n}$ and we introduce $\Xi_\pi \in \mathbb{S}^n$ whose ith row and jth column entry is given by

$$\Xi_\pi[i,j] = \sum_{s \in \mathcal{S}} p(s) p_s(z_i) p_s(z_j). \tag{4.22}$$

Then, the problem faced by $\mathcal{P}_S$ can be written as

$$\min_{\pi \in \Pi} \operatorname{Tr}\{\mathbb{E}\{\hat{\boldsymbol{z}}\hat{\boldsymbol{z}}'\} V\} = \min_{\pi \in \Pi} \operatorname{Tr}\left\{\Xi_\pi \bar{V}\right\}, \tag{4.23}$$

where $\bar{V} := Z' V Z$.

Remark. We can address the problem according to the solution concept developed in [15] as follows. The cost for $\mathcal{P}_S$ if $\mathcal{P}_R$ has the posterior belief $\underline{p} \in \Delta(\mathcal{Z})$ is given by

$$\hat{c}(\underline{p}) = \operatorname{Tr}\left\{\bar{V}\underline{p}\underline{p}'\right\} \tag{4.24}$$

since $\hat{z} = Z\underline{p}$ for the posterior belief $\underline{p} \in \Delta(\mathcal{Z})$ and correspondingly we have $\mathbb{E}\{\hat{\boldsymbol{z}}\hat{\boldsymbol{z}}'\} = Z\underline{p}\underline{p}'Z'$. Then, the solution concept says that the minimum cost for $\mathcal{P}_S$ is attained at $C(\underline{p}_o)$, where $C(\underline{p})$ is the convex envelope of $\hat{c}(\underline{p})$, i.e.,

$$C(\underline{p}) \equiv \inf\{c | (\underline{p}, c) \in \operatorname{co}\{\hat{c}\}\}, \tag{4.25}$$

where $\operatorname{co}\{\hat{c}\}$ denotes the convex hull of the graph of $\hat{c}$. However, $V \in \mathbb{S}^{2m}$

(or $V^p \in \mathbb{S}^{2m}$), as described in (4.12) (or in (4.14)), has both positive and negative eigenvalues, which yields that the function $\hat{c}$ is neither convex nor concave. This makes the computation of the convex envelope prominently challenging. Therefore, we develop a new solution concept.

The following proposition provides a compact characterization of a necessary and sufficient condition on Ξ_π.

Proposition 4.1. *For any signaling rule $\pi \in \Pi$, $\Xi_\pi \in \mathbb{S}^n$, as described in (4.22), satisfies $\Xi_\pi \in \mathcal{CP}^n$ and $\Xi_\pi \underline{1} = \underline{p}_o$, where $\underline{p}_o := \begin{bmatrix} p_o(z_1) & \dots & p_o(z_n) \end{bmatrix}'$.*

Furthermore for any completely positive matrix $\Xi \in \mathcal{CP}^n$ that satisfies $\Xi \underline{1} = \underline{p}_o$, there exists a signaling rule $\pi \in \Pi$ such that $\Xi_\pi = \Xi$. Consider a factorization[5] of $\Xi \in \mathcal{CP}^n$, as $\Xi^* = \sum_{i=1}^k \underline{b}_i \underline{b}_i'$, where $\underline{b}_i \in \mathbb{R}_+^n$. Then, the corresponding signaling strategy is given by[6]

$$\pi^*(s_i|z_j) = \underline{b}_i' \underline{1} \frac{b_{i,j}}{p_o(z_j)}, \ \forall\ i = 1, \dots, k, j = 1, \dots, n, \tag{4.26}$$

where $b_{i,j} \geq 0$ denotes the jth entry of $\underline{b}_i$.

Proof. The proof is provided in Appendix C.1. □

Remark. We note that a necessary condition on $\mathbb{E}\{\hat{\boldsymbol{z}}\hat{\boldsymbol{z}}'\}$ is given by [42]

$$\mathbb{E}\{\boldsymbol{z}\boldsymbol{z}'\} \geq \mathbb{E}\{\hat{\boldsymbol{z}}\hat{\boldsymbol{z}}'\} \geq \mathbb{E}\{\boldsymbol{z}\}\mathbb{E}\{\boldsymbol{z}\}', \tag{4.27}$$

which corresponds to

$$\mathbb{E}\{\boldsymbol{z}\boldsymbol{z}'\} \geq Z\Xi_\pi Z' \geq \mathbb{E}\{\boldsymbol{z}\}\mathbb{E}\{\boldsymbol{z}\}'. \tag{4.28}$$

However, given the necessary and sufficient condition that $\Xi_\pi \in \mathcal{CP}^n$ and $\Xi_\pi \underline{1} = \underline{p}_o$, this condition (4.28) turns out to be redundant.

Based on Proposition 4.1, the following corollary shows that the highly nonlinear non-convex optimization problem faced by $\mathcal{P}_S$ could be written, "equivalently", as a linear optimization problem over the convex cone of completely positive matrices. We emphasize that there is no relaxation on the optimization problem and the equivalence is not limited to optimality.

[5] A completely positive matrix could have multiple different factorization even for the same $k \in \mathbb{N}$ [92]. This also yields that the corresponding signaling strategy is not unique in general.

[6] Note that the prior distribution has complete support over $\mathcal{Z}$ by definition.

Corollary 4.2. *The problem faced by $\mathcal{P}_S$ can be written in an equivalent form as*

$$\min_{\pi \in \Pi} \operatorname{Tr}\{\mathbb{E}\{\hat{z}\hat{z}'\} V\} = \begin{array}{l} \min\limits_{\Xi \in \mathcal{CP}^n} \operatorname{Tr}\left\{\Xi \bar{V}\right\}, \\ \text{s.t. } \Xi \underline{1} = \underline{p}_o \end{array} \tag{4.29}$$

where $\bar{V} = Z'VZ$.

Interestingly, the following proposition shows that the equivalent problem, as described by the right-hand side of (4.29) turns out to be a semi-definite program (SDP), which can be solved with the existing numerical tools/solvers efficiently if $n \leq 4$.

Proposition 4.3. *Let $n \leq 4$. Then, we have*

$$\begin{array}{lcl} \min_{\Xi \in \mathcal{CP}^n} \operatorname{Tr}\left\{\Xi \bar{V}\right\} & = & \min_{\Xi \in \mathbb{S}_+^n} \operatorname{Tr}\left\{\Xi \bar{V}\right\}. \\ \text{s.t. } \Xi \underline{1} = \underline{p}_o & & \text{s.t. } \Xi \underline{1} = \underline{p}_o, \Xi \in \mathbb{R}_+^{n \times n} \end{array} \tag{4.30}$$

Furthermore, an SDP relaxation of the problem for $n > 4$ is given by

$$\begin{array}{lcl} \min_{\Xi \in \mathcal{CP}^n} \operatorname{Tr}\left\{\Xi \bar{V}\right\} & \geq & \min_{\Xi \in \mathbb{S}_+^n} \operatorname{Tr}\left\{\Xi \bar{V}\right\}. \\ \text{s.t. } \Xi \underline{1} = \underline{p}_o & & \text{s.t. } \Xi \underline{1} = \underline{p}_o, \Xi \in \mathbb{R}_+^{n \times n} \end{array} \tag{4.31}$$

Proof. This follows since $\mathcal{CP}^n \subseteq \mathbb{S}_+^n \cap \mathbb{R}_+^{n \times n}$ for all n, while $\mathcal{CP}^n = \mathbb{S}_+^n \cap \mathbb{R}_+^{n \times n}$ if, and only if, $n \leq 4$ [91, 94]. □

With respect to the trace inner product, given the primal problem:

$$\min_{\Xi \in \mathcal{CP}^n} \operatorname{Tr}\left\{\Xi \bar{V}\right\}, \text{ s.t. } \Xi \underline{1} = \underline{p}_o, \tag{4.32}$$

the dual problem is given by

$$\max_{\underline{y} \in \mathbb{R}^n, S \in \mathcal{COP}^n} \underline{p}_o' \underline{y}, \text{ s.t. } \underline{1}\underline{y}' - S = \bar{V}. \tag{4.33}$$

Furthermore, the following proposition shows the strong duality between (4.32) and (4.33), which enables us to solve only one of them while obtaining the value of both of them.

Proposition 4.4. *The primal problem* (4.32) *is feasible, has finite value, and has an interior point. Therefore, there exists a strong duality between* *the primal problem* (4.32) *and its dual* (4.33)*, i.e., we have*

$$\begin{array}{lcl} \min_{\Xi\in\mathcal{CP}^n} \operatorname{Tr}\left\{\Xi\bar{V}\right\} & = & \max_{\underline{y}\in\mathbb{R}^n, S\in\mathcal{COP}^n} \underline{p}_o'\underline{y}. \\ \text{s.t. } \Xi\underline{1} = \underline{p}_o & & \text{s.t. } \underline{1}\underline{y}' - S = \bar{V} \end{array} \tag{4.34}$$

Proof. We can show that there exists an interior point in the feasible set of the optimization problem based on the characterization of the interior of $\mathcal{CP}^n$ provided in [102]. Particularly, a mixture of full and null signaling leads to $\Xi_\pi \in \operatorname{int}\{\mathcal{CP}^n\}$ and $\Xi_\pi\underline{1} = \underline{p}_o$. The technical details of the proof is provided in Appendix C.2. □

4.2.3 Theoretical Approximation Guarantees

We have formulated the minimum cost of $\mathcal{P}_S$ for the scenarios where the state space is finite. We can, however, adopt the solution concept to the general class of distributions by discretizing a continuous state space through a quantization scheme. However, such discretization would lead to loss of information and correspondingly the computed minimum cost could deviate from the true one. Therefore, in this subsection, we seek to restrain this deviation. To this end, by turning the problem around, we can view the problem setting as $\mathcal{P}_S$ selecting a random vector within the general class of square integrable distributions and sending a realization of that signal rather than selecting a signaling strategy within the general class of stochastic kernels. Note that $\mathcal{P}_S$ should take into account the joint distribution of the underlying distribution and the signal sent, which would normally have been determined by the signaling strategy.

Based on this observation, the following corollary provides theoretical guarantees on the approximation capability of the solution concept for a given quantization scheme.

Corollary 4.5. *Consider a quantization of the continuous random variable* $\boldsymbol{z} \in \mathcal{Z}$*, denoted by* $\boldsymbol{z}_q \in \mathcal{Z}$*, i.e.,* $\boldsymbol{z}_q$ *attains the same value within any bin of the quantization. Let* $\boldsymbol{e} = \boldsymbol{z} - \boldsymbol{z}_q$*, almost everywhere over* $\mathcal{Z}$*, denote the quantization error. Then, we have*

$$\left|\min_{\boldsymbol{s}} \operatorname{Tr}\left\{\mathbb{E}\left\{\hat{\boldsymbol{z}}\hat{\boldsymbol{z}}'\right\}V\right\} - \min_{\boldsymbol{s}} \operatorname{Tr}\left\{\mathbb{E}\left\{\hat{\boldsymbol{z}}_q\hat{\boldsymbol{z}}_q'\right\}V\right\}\right| \leq \epsilon, \tag{4.35}$$

where $\hat{\boldsymbol{z}} = \mathbb{E}\{\boldsymbol{z}|\boldsymbol{s}\}$, $\hat{\boldsymbol{z}}_q = \mathbb{E}\{\boldsymbol{z}_q|\boldsymbol{s}\}$, *and*

$$\epsilon = (2\|\boldsymbol{z}_q\| + \|\boldsymbol{e}\|)\|V\|_2\|\boldsymbol{e}\|, \tag{4.36}$$

which yields that $\epsilon \to 0$ *when* $\|\boldsymbol{e}\| \to 0$.

Proof. The proof is provided in Appendix C.3. □

4.3 Computational Approaches

Although the equivalent problems (4.32) and (4.33) are linear optimization problems over convex constraint sets, they are difficult to solve numerically since the cones of completely positive and copositive matrices are not tractable if $n > 4$. However, for $n > 4$, we can approximate the solution with any desired error rate at the expense of computational complexity by using existing computational tools developed in the optimization community over the course of time, e.g., [95–100]. Furthermore, each new development in this active research area (due to its broad applications) will bring in new computational tools and insights to address the problem. Indeed, as remarked below, the signaling framework could also bring in new insights to copositive programs.

Remark. In general, optimization over completely positive matrices is a reformulation of some nonconvex quadratic program and correspondingly factorization of its solution is of main interest in order to identify the corresponding optimal minimizer for the original problem. However factorization of a given completely positive matrix is also challenging. However, the knowledge of its CP-rank can play an important role in the computational approaches for factorization, e.g., as in [93]. However, in [103], the authors have posted the computation of the CP-rank of a given matrix as one of the open problems in the theory of completely positive matrices. There exists known upper bounds on CP-rank of a matrix, e.g., see [104, Theorem 4.1], and in [93], the authors have exploited these bounds to factorize a given completely positive matrix.

On the other hand, given a solution of the primal problem $\Xi_* = B_* B_*'$, where $B_* \in \mathbb{R}_+^{n\times k}$, we can set the size of the signaling space for the corresponding optimal signaling strategy as k. The revelation principle, however, yields that we can set the size of the signal space as $k = n$ without loss of generality, as shown in Proposition 4 of the web appendix of [15]. This yields that in the primal problem (4.32), there always exists a solution whose CP-rank is less than or equal to n. Its generalization to the general class of copositive programs could be an interesting future research direction since this could lead to new computational tools that search for a solution over a substantially smaller space. Note that the known bounds on CP-rank are polynomial in n.

We can approximate $\mathcal{CP}^n$ through polyhedral cones [95, 98, 99] from inside and outside of $\mathcal{CP}^n$ such that their (nested) sequence converges to $\mathcal{CP}^n$ asymptotically. For each polyhedral approximation, the corresponding optimization problem becomes an LP, which can be solved in polynomial time. A comparison between inner and outer approximations quantifies the accuracy of the approximation. Furthermore, we can be strategic while approximating the underlying cone since the main objective is to solve the optimization problem rather than approximating the cone everywhere. For example, in [95], the authors have proposed a fast algorithm to approximate the cone of copositive matrices "adaptively" via inner and outer polyhedral constraints. A distinctive feature of this algorithm is to adapt the quality of approximation according to the optimization objective. In other words, the adaptive algorithm seeks to attain fine approximation around some neighborhood of the solution of the optimization problem while letting the approximation be coarse anywhere else.

4.3.1 Polyhedral Inner and Outer Approximations

Note that the extreme rays of $\mathcal{CP}^n$ have rank 1, i.e., they can be written as $\underline{b}\underline{b}'$, where $\underline{b} \in \mathbb{R}_+^n$ [91]. Correspondingly, $\mathcal{CP}^n$ can be viewed as the conic hull of vectors from the unit simplex Δ_{n-1} in $\mathbb{R}^n$ [99]. Consider a family of simplices $\mathcal{P} = \{\Delta^1, \ldots, \Delta^t\}$ satisfying

$$\Delta_{n-1} = \bigcup_{i=1}^{t} \Delta^i \text{ and } \operatorname{int}\left\{\Delta^i\right\} \cap \operatorname{int}\left\{\Delta^j\right\} = \varnothing \text{ if } i \neq j.$$

Given the family of simplices $\mathcal{P}$, we define the polyhedral cones:[7]

$$\mathcal{I}_{\mathcal{P}} := \left\{ \sum_{\underline{b} \in V_{\mathcal{P}}} \lambda_b \underline{b} \underline{b}' : \lambda_b \geq 0 \right\}, \tag{4.37}$$

$$\mathcal{O}_{\mathcal{P}} := \left\{ \sum_{\underline{b}, \underline{c} \in V_{\mathcal{P}}} \lambda_{b,c} (\underline{b} \underline{c}' + \underline{c} \underline{b}') : \lambda_{b,c} \geq 0 \right\}, \tag{4.38}$$

where $V_{\mathcal{P}}$ denotes the set of vertices in $\mathcal{P}$. In [95], the authors have shown that $\mathcal{I}_{\mathcal{P}} \subseteq \mathcal{CP}^n \subseteq \mathcal{O}_{\mathcal{P}}$ for any $\mathcal{P}$. Let $\mathrm{CP}(\mathcal{K})$ denote the solution of the following $\mathcal{K}$-cone program:

$$\begin{aligned} \mathrm{CP}(\mathcal{K}) = \min \ & \mathrm{Tr}\left\{ \Xi \bar{V} \right\} \\ \text{s.t. } & \Xi \underline{1} = \underline{p}_o \\ & \Xi \in \mathcal{K}. \end{aligned} \tag{4.39}$$

Since $\mathcal{I}_{\mathcal{P}} \subseteq \mathcal{CP}^n \subseteq \mathcal{O}_{\mathcal{P}}$, we have

$$\mathrm{CP}(\mathcal{I}_{\mathcal{P}}) \geq \mathrm{CP}(\mathcal{CP}^n) \geq \mathrm{CP}(\mathcal{O}_{\mathcal{P}}). \tag{4.40}$$

Correspondingly, through a sequence of simplical partitions, we can construct a sequence of nested polyhedral cones $\mathcal{I}_1 \subseteq \mathcal{I}_2 \subseteq \ldots$ and $\mathcal{O}_1 \supseteq \mathcal{O}_2 \supseteq \ldots$ that converge to $\mathcal{CP}^n$, i.e.,

$$\mathcal{CP}^n = \overline{\bigcup_{i \in \mathbb{N}} \mathcal{I}_i} \text{ and } \mathcal{CP}^n = \bigcap_{i \in \mathbb{N}} \mathcal{O}_i, \tag{4.41}$$

from below and above, respectively [95].

4.3.2 Resemblance to the Equivalent Problem Formulated in [15]

We can view a polyhedral inner approximation of $\mathcal{CP}^n$, e.g., via the conic hull of the vertices of the simplical partition of the unit simplex, as a discretization of the feasible set of the optimization problem through a discretization of the unit simplex [99]. Correspondingly, based on (4.37), the upper bound in

[7] The subscripts b and c denote the index of the associated vectors.

(4.40) can be written as

$$\min_{\underline{\lambda}\in\mathbb{R}_+^{|V_{\mathcal{P}}|}} \mathrm{Tr}\left\{\sum_{\underline{b}\in V_{\mathcal{P}}} \lambda_b \underline{b}\underline{b}'\bar{V}\right\} \text{ s.t. } \sum_{\underline{b}\in V_{\mathcal{P}}} \lambda_b \underline{b}\cancel{(\underline{b}'\underline{1})} = \underline{p}_o, \tag{4.42}$$

which is equivalent to

$$\min_{\lambda\in\mathbb{R}_+^{|V_{\mathcal{P}}|}} \sum_{\underline{b}\in V_{\mathcal{P}}} c_b\lambda_b \text{ s.t. } \sum_{\underline{b}\in V_{\mathcal{P}}} \underline{b}\lambda_b = \underline{p}_o, \tag{4.43}$$

where $c_b := \mathrm{Tr}\left\{\underline{b}\underline{b}'\bar{V}\right\}$.

Note that, in [15, Corollary 1], the authors have shown that the problem faced by $\mathcal{P}_S$ is equivalent to the following optimization problem:

$$\min_{\tau\in\Delta(\Delta(\mathcal{Z}))} \int_{\Delta(\mathcal{Z})} \hat{c}_S(p)\tau(dp) \text{ s.t. } \int_{\Delta(\mathcal{Z})} p\tau(dp) = p_o, \tag{4.44}$$

where, with a slight abuse of notation, $\hat{c}_S(p)$ denotes $\mathcal{P}_S$'s cost for a given common belief $p\in\Delta(\mathcal{Z})$, the constraint $\int_{\Delta(\mathcal{Z})} p\tau(dp) = p_o$ is called the Bayes plausibility, and τ could be viewed as a probability measure over the posterior distributions. The resemblance between (4.44) and (4.43) is notable. Particularly, a discretization of the simplex $\Delta(\mathcal{Z})$ in (4.44) would have lead to (4.43).

4.3.3 Relaxed Specifications and Sender-Favorite Discrete Distributions

Recall that the Gaussian distribution leads to the least possible cost for the sender when the correlation matrix of the underlying random vector is fixed. Similarly, within the proposed framework, we can relax certain specifications on the prior distribution to find out the corresponding most favorable distribution for the sender. For example, an interesting relaxation would be to consider the scenarios where only the mean of the underlying prior distribution is fixed, i.e., $Z\Xi\underline{1} = \underline{\mu}_o \in \mathbb{R}^{2m}$. Corresponding equivalent linear optimization problem is given by

$$\min_{\Xi\in\mathcal{CP}^n} \mathrm{Tr}\left\{\Xi\bar{V}\right\} \text{ s.t. } \begin{bmatrix} Z \\ \underline{1}' \end{bmatrix}\Xi\underline{1} = \begin{bmatrix} \underline{\mu}_o \\ 1 \end{bmatrix}, \tag{4.45}$$

Table 4.1: Joint distributions in Scenario I.

Scenario I.		Evidence Suggests	
		(G) $\boldsymbol{x} = -1$	(NG) $\boldsymbol{x} = 1$
Prosecutor Thinks	(G) $\boldsymbol{y} = -1$	0.3	0.7

Table 4.2: Joint distributions in Scenario II.

Scenario II.		Evidence Suggests	
		(G) $\boldsymbol{x} = -1$	(NG) $\boldsymbol{x} = 1$
Prosecutor Thinks	(NG) $\boldsymbol{y} = 1$	0.1	0.4
	(G) $\boldsymbol{y} = -1$	0.2	0.3

Table 4.3: Joint distributions in Scenario III.

Scenario III.		Evidence Suggests		
		(G) $\boldsymbol{x} = -1$	(I) $\boldsymbol{x} = 0$	(NG) $\boldsymbol{x} = 1$
Prosecutor Thinks	(NG) $\boldsymbol{y} = 1$	0.05	0.05	0.1
	(I) $\boldsymbol{y} = 0$	0.05	0.15	0.1
	(G) $\boldsymbol{y} = -1$	0.2	0.2	0.1

where we have $2m + 1$ linear constraints different from the primal problem, where there are n linear constraints. We can enrich the class of problems that can be formulated within the proposed framework by considering partial specifications of the underlying distribution or its mean.

4.4 Illustrative Examples

Similar to the example introduced in [15], let us consider the interaction between a prosecutor ($\mathcal{P}_S$) and a judge ($\mathcal{P}_R$) during the trial of a defendant.

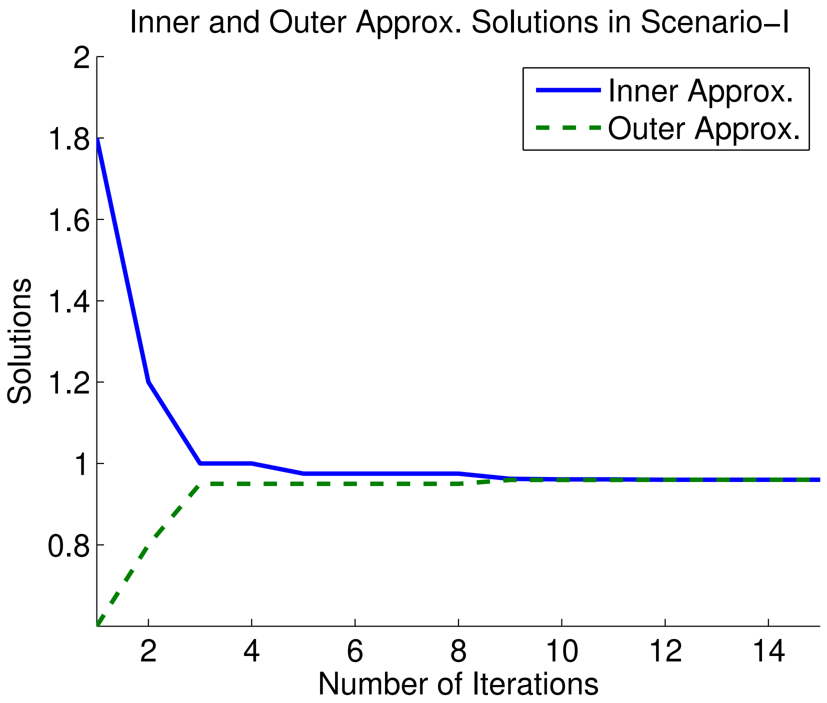


Figure 4.2: Computation of the minimum cost for $\mathcal{P}_S$ in deceptive signaling game via sequential inner and outer polyhedral approximations in Scenario I.

Particularly, now the prosecutor has access to

- the information of interest $x \in \mathcal{X}$ corresponding to the status of a defendant based on some evidence
- the private information $y \in \mathcal{Y}$ corresponding to the prosecutor's intuition about the status of the defendant

Irrespective of the evidence, our self-confident and righteous prosecutor seeks to induce the judge to perceive the status of the defendant in line with his intuition. On the other side, the judge is only interested in what the evidence says about the status of the defendant. We consider three scenarios where the underlying joint distributions over the prosecutor's intuition and what the evidence suggests about the defendant's status are as tabulated in Tables 4.1, 4.2, and 4.3, where (NG), (I), and (G) correspond to the status of 'not guilty', 'innocent', and 'guilty', respectively.

Note that in Scenario I, the prosecutor's intuition always says that the defendant is guilty, which can also be viewed as the prosecutor always seeks for conviction similar to the example studied in [15]. However, this differs

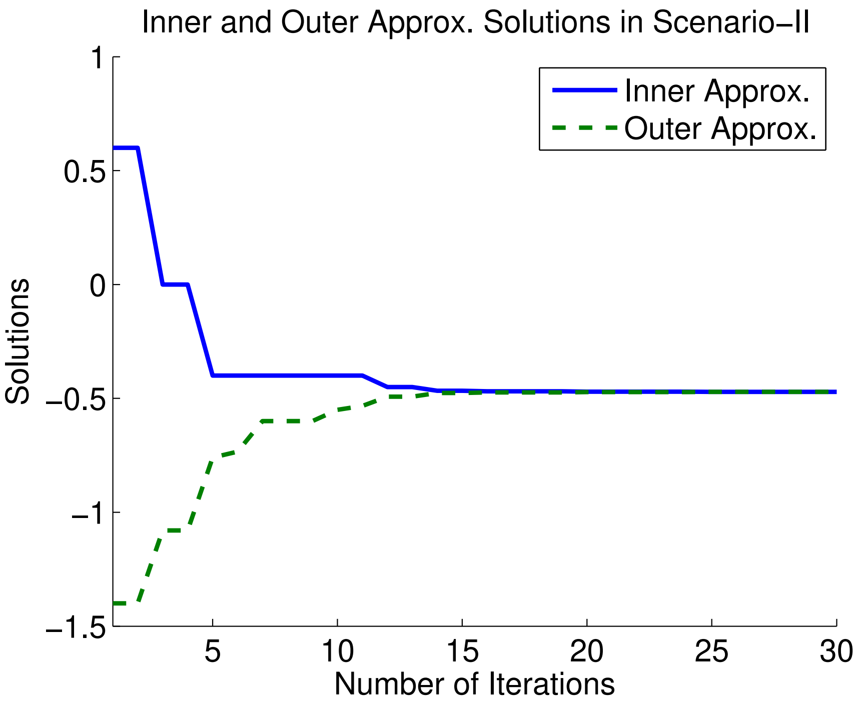


Figure 4.3: Computation of the minimum cost for $\mathcal{P}_S$ in deceptive signaling game via sequential inner and outer polyhedral approximations in Scenario II.

from the example in [15] in terms of the cost measures, and therefore also the result is different. The cost of $\mathcal{P}_S$ when $\mathcal{P}_R$ has the belief $\begin{bmatrix}1-\mu & \mu\end{bmatrix}'$, where $\mu := \mathbb{P}\boldsymbol{z} = \begin{bmatrix}-1 & -1\end{bmatrix}'$, is given by

$$\hat{c}(\mu) = 4\mu^2 - 8\mu + 3, \tag{4.46}$$

which is a convex function. Note that even though $\operatorname{Tr}\left\{\bar{V}\underline{pp}'\right\}$ is a non-convex function of $\underline{p}$, it turns out to be a convex function over the unit simplex under the specific settings of this example. However, as observed in the following examples, this is not always the case. Furthermore, as characterized in [15], since $\hat{c}(\cdot)$ is a convex function, null signaling is the optimal one in Scenario I. Alternatively, we have its convex envelope $C(\mu) = \hat{c}(\mu)$ and the minimum cost for $\mathcal{P}_S$ is given by $C(\mu) = \hat{c}(\mu_o) = 0.96$, where μ_o is the prior probability of $\begin{bmatrix}-1 & -1\end{bmatrix}'$, i.e., 0.3.

On the other hand, in Scenarios II and III, the associated cost of $\mathcal{P}_S$ for a given posterior belief of $\mathcal{P}_R$ does not end up to be a convex function. The dimensions of freedom to select the posterior are 3 and 8, respectively, in Sce-

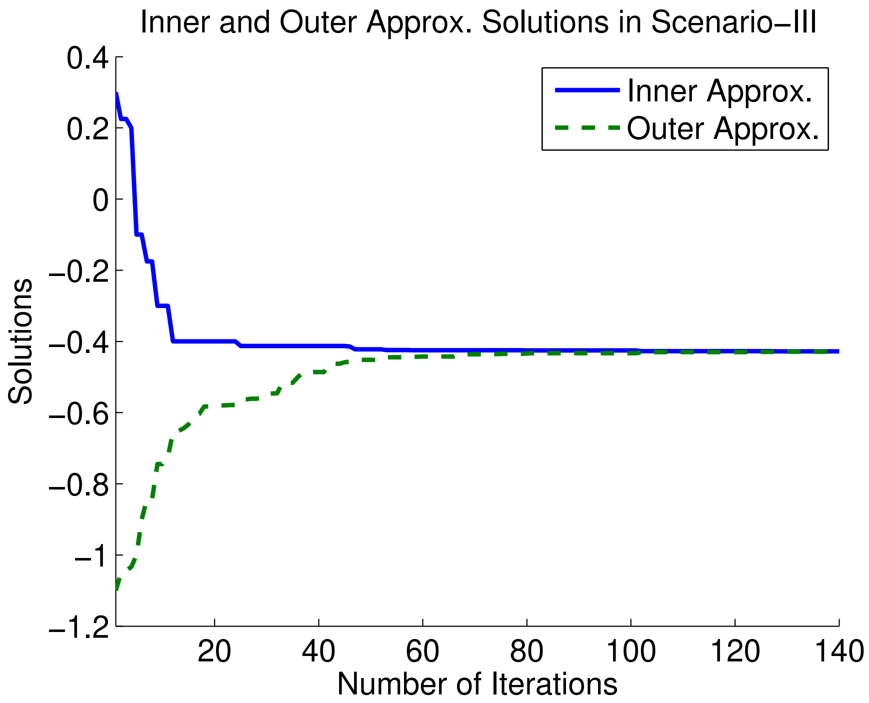


Figure 4.4: Computation of the minimum cost for $\mathcal{P}_S$ in deceptive signaling game via sequential inner and outer polyhedral approximations in Scenario III.

Table 4.4: Cost of $\mathcal{P}_S$ in deceptive signaling game for Scenarios I-III.

Scenarios	I	II	III
Size of State Space	2	4	9
Null Signaling $\text{Tr}\left\{\bar{V}\underline{p}_o\underline{p}_o'\right\}$	**0.96**	0.16	0
Full Signaling $\text{Tr}\left\{\bar{V}\text{diag}\{\underline{p}_o\}\right\}$	1.8	0.6	0.3
Optimal Signaling $\text{Tr}\left\{\bar{V}\Xi^*\right\}$	**0.96**	**-0.4715**	**-0.4283**
SDP-Relaxation	**0.96**	**-0.4715**	**-0.4283**

narios II and III. Therefore, in order to apply the same solution concept, we need to compute the convex envelope of some non-convex functions defined over $\mathbb{R}^3$ and $\mathbb{R}^8$, instead of $\mathbb{R}$ as we do in Scenario I. However, through the proposed framework, we can efficiently compute the minimum cost for $\mathcal{P}_S$ and the associated optimal signaling strategies in those scenarios. In Table 4.4, we tabulate the results. Proposition 4.3 says that the SDP-relaxation

Table 4.5: Cost of $\mathcal{P}_S$ in persuasive privacy game for Scenarios I-III. Note that $\bar{V}^p = Z'V^pZ$.

Scenarios	I	II	III
Size of State Space	2	4	9
Null Signaling $\text{Tr}\left\{\bar{V}^p \underline{p}_o \underline{p}_o'\right\}$	0.84	-0.16	0.09
Full Signaling $\text{Tr}\left\{\bar{V}^p \text{diag}\{\underline{p}_o\}\right\}$	**0**	0	0.1
Optimal Signaling $\text{Tr}\left\{\bar{V}^p \Xi^*\right\}$	**0**	**-0.9583**	**-0.4707**
SDP-Relaxation	**0**	**-0.9583**	**-0.4707**

and the primal problem are equivalent for $n \leq 4$, as also seen in Table 4.4. We also note that the SDP-relaxation has turned out to be a tight lower bound in Scenario III, where $n = 9$. In Figs. 4.2-4.4, we illustrate the convergence behavior of the solutions of the inner and outer polyhedral approximations across the iterations. Note that with the increase of the size of the state space, the corresponding number of iterations necessary for convergence increase significantly while the computational complexity of each iteration increases further with an increase in the size of the state space.

We have also analyzed the cost of $\mathcal{P}_S$ in the persuasive privacy game over Scenarios I-III. We have tabulated the results in Table 4.5. Similar to the case in the deceptive signaling game, we can apply the solution process introduced in [15] to this problem for Scenario I. Correspondingly, the cost of $\mathcal{P}_S$ when $\mathcal{P}_R$ has the belief $\begin{bmatrix}1-\mu & \mu\end{bmatrix}'$, where $\mu := \mathbb{P}\boldsymbol{z} = \begin{bmatrix}-1 & -1\end{bmatrix}'$, is now given by

$$\hat{c}(\mu) = -4\mu^2 + 4\mu, \tag{4.47}$$

which is a concave function. As characterized in [15], since $\hat{c}(\cdot)$ is a concave function, we can conclude that full signaling is the optimal one in Scenario I. Alternatively, a geometrical inspection yields that the convex envelope of $\hat{c}(\mu)$ is given by $C(\mu) = 0$, which coincides with the cost for the full signaling case as expected. We also note that the number of iterations for the convergence of inner and outer approximations are observed to be similar with the cases in the deceptive signaling game.

4.5 Concluding Remarks

We have addressed the problem of optimal hierarchical signaling between a sender and a receiver for a general class of square integrable multivariate distributions, which has applications to deception and privacy. We have considered a noncooperative communication setting where the sender and the receiver have different cost measures. This leads to the possibility of strategic crafting of the messages sent by the sender. The sender has had access to the information of interest and some private information, both of them being realizations of random vectors with arbitrary distributions. We have shown that the proposed solution concept can compute the minimum cost for the sender in the deception and privacy applications. For the former one, the sender seeks to induce the receiver to perceive the information of interest as the private information. In the latter one, the sender seeks to minimize the informational leakage of the private information while sharing the information of interest with the receiver.

For discrete distributions, we have formulated an equivalent linear optimization problem over the cone of completely positive matrices. This has brought the hierarchical signaling problem into the framework of copositive programs so that we could use the existing computational tools that can solve it to any level of accuracy. For continuous distributions, we have also addressed the approximation error of the minimum cost for the sender if we have employed the solution concept for its discretized version obtained via a quantization scheme. Finally we have analyzed the performance of the proposed solution concept over various numerical examples.

In addition to developing efficient computational tools to address the equivalent cone program, some other future directions of research include: formulation of optimal hierarchical signaling in dynamic and/or noisy environments with multiple senders and/or multiple receivers, and applications of the setting in other noncooperative communication and control scenarios.

5

CONCLUDING REMARKS

Nothing is more common on earth than to deceive and be deceived.
– Johann G. Seume

We have sought to introduce strategic information transmission to cyber-physical systems as a deception-as-defense mode of operation. We have selected the deception models where the informed agent commits to his/her strategies beforehand in order to avoid obscurity based strategies that can become vulnerable once the uninformed agent becomes aware of the strategy. With a specific focus on Gaussian distributions due to their versatility in engineering applications, we have sought to formulate the optimal signaling strategies in dynamic environments. For Gauss-Markov information, we have analyzed how a deceptive information provider can shape the shared information in order to control a decision maker's decisions in dynamic communication settings. We note that the problem involved two nested infinite-dimensional optimization problems. For quadratic objective functions over a finite horizon, we have formulated an equivalent SDP problem enabling tractable analysis compared to direct optimization over those infinite dimensional strategy spaces. We have shown that linear sender and receiver strategies can yield the equilibrium within the general class of Borel-measurable policies in strategic communication.

The formulation of optimal signaling strategies for Gauss-Markov information in dynamic environments has brought in the possibility of adopting strategic signaling also in dynamic control systems as deception-as-defense mode of operation. We have introduced robust sensor design framework as a security measure in stochastic control systems to provide resiliency against multiple attackers with misaligned control objectives. We have specifically considered LQG control systems, where the controller could have been compromised by various types of attackers with certain adversarial control objectives. We have designed the *linear* sensor outputs cautiously by taking the possibility of undetected attacks into consideration. We have provided an SDP-based algorithm to compute the robust sensor outputs that lead to minimum damage in terms of system's quadratic control objective.

Although we could have obtained well structured, e.g., linear, signaling strategies for Gaussian information, formulation of optimal signaling strategies for a general class of distributions is more involved and less likely to yield such elegant structures in general. The earlier literature has only addressed it for a special class of problems and for discrete distributions with fairly small state spaces. Therefore, we have sought to formulate the persuasion capacity of a sender for a general class of multivariate square integrable distributions. Again, instead of a direct approach based on the strategy spaces, we have formulated an equivalent linear optimization problem over the cone of completely positive matrices for finite state spaces. In that way, we could apply the existing computational tools developed in the optimization community to solve such a class of problems. The ability to compute the persuasion capacity of discrete distributions with large state spaces has brought in the possibility of computing the persuasion capacity approximately for continuous distributions. We have also provided guarantees on the level of approximation of such approaches.

Based on these results, there are various directions for future research including their generalizations to signaling problems over networks of multiple senders and/or receivers, and with uncertainties such as noisy measurements, noisy channels, unknown cost measures, and unknown state dynamics. More detailed lists of future research directions have also been provided at the end of each chapter.

APPENDIX A

TECHNICAL RESULTS IN CHAPTER 2

A.1 Proof of Lemma 2.1

The minimization problem in (2.13) can be written as

$$\min_{\substack{\eta_k \in \Omega_k, \\ k=1,\dots,n}} \sum_{k=1}^{n} \mathrm{Tr}\{V_k \mathbb{E}\{\hat{\boldsymbol{x}}_k \hat{\boldsymbol{x}}_k'\}\} = \min_{\substack{\eta_k \in \Omega_k, \\ k=1,\dots,n}} \sum_{k=1}^{n} \mathrm{Tr}\{V_k H_k\}. \tag{A.1}$$

Note that the posterior covariances $H_1, \dots, H_n$ depend on the signaling rules $\eta_1, \dots, \eta_n$, and they are real and symmetric matrices by definition. Next, we aim to find necessary conditions on H_k's to derive a tight lower bound on (2.13). To this end, consider the following positive semi-definite matrix:

$$\mathbb{E}\{(\boldsymbol{x}_k - \hat{\boldsymbol{x}}_k)(\boldsymbol{x}_k - \hat{\boldsymbol{x}}_k)'\} = \Sigma_k - H_k \succeq O,$$

which implies $\Sigma_k \succeq H_k$, for $k = 1, \dots, n$. Furthermore, after some algebra, it can be shown that

$$\mathbb{E}\{(\hat{\boldsymbol{x}}_k - \mathbb{E}\{\boldsymbol{x}_k | \boldsymbol{y}_{1:k-1}\})(\hat{\boldsymbol{x}}_k - \mathbb{E}\{\boldsymbol{x}_k | \boldsymbol{y}_{1:k-1}\})'\} = H_k - AH_{k-1}A', \tag{A.2}$$

and therefore $H_k - AH_{k-1}A' \succeq O$ and correspondingly $H_k \succeq AH_{k-1}A'$.

The posterior covariances $H_1, \dots, H_k$ are real, symmetric matrices and should at least satisfy the constraints: $\Sigma_1 \succeq H_1 \succeq O$, and $\Sigma_k \succeq H_k \succeq AH_{k-1}A'$, for $k = 2, \dots, n$. Based on this, we can formulate another optimization problem (2.16) in which the optimization arguments $S_1, \dots, S_n \in \mathbb{S}^p$ are subject to the constraints in (2.16). Since we have shown that those constraints are necessary (not necessarily sufficient yet), the minimization problem (2.16) is a lower bound on (2.13). By the linear objective function $\sum_k \mathrm{Tr}\{V_k S_k\}$ and the semi-definiteness constraints on S_k, (2.16) is an SDP problem.

A.2 Proof of Lemma 2.3

Suppose that $E = (E_1, \dots, E_n) \in \Psi$ is an extreme point of Ψ and there exists an element E_k such that E_k is not an extreme point of $\Phi_k(E_{-k})$. Then, there exist two distinct $M, N \in \Phi_k(E_{-k})$ such that $E_k = tM + (1-t)N$, for some $t \in (0,1)$. Note that since $M, N \in \Phi_k(E_{-k})$, the matrices M and N satisfy

$$A^{-1}E_{k+1}(A')^{-1} \geq M \geq AE_{k-1}A',$$
$$A^{-1}E_{k+1}(A')^{-1} \geq N \geq AE_{k-1}A'$$

by (2.19). Therefore,

$$E_M := (E_1, \dots, E_{k-1}, M, E_{k+1}, \dots, E_n) \in \Psi,$$
$$E_N := (E_1, \dots, E_{k-1}, N, E_{k+1}, \dots, E_n) \in \Psi,$$

and $E_M \neq E_N$ since $M \neq N$. However, we can write the extreme point E as $E = tE_M + (1-t)E_N$, for some $t \in (0,1)$ even though $E_M, E_N \in \Psi$, and this leads to a contradiction. Hence, if $(E_1, \dots, E_n) \in \Psi$ is an extreme point, the elements E_k are the extreme points of the corresponding sub-constraint sets $\Phi_k(E_{-k})$.

A.3 Proof of Lemma 2.4

Note that eigenvalues of a symmetric idempotent matrix are either 0 or 1, and suppose that for a symmetric idempotent matrix $P \in \Phi$, there exist two distinct symmetric matrices $M \in \Phi$ and $N \in \Phi$ such that $P = tM + (1-t)N$ for some $t \in (0,1)$. Let $p_1, p_0 \in \mathbb{R}^p$ be eigenvectors of P corresponding to eigenvalues 1 and 0, respectively. Note that since the eigenvalues of M and N are bounded, for any vector $p \in \mathbb{R}^p$, $0 \leq p'Mp \leq 1$ and $0 \leq p'Np \leq 1$. Then, through convex combination, we have

$$tp_1'Mp_1 + (1-t)p_1'Np_1 = p_1'Pp_1 = 1,$$
$$tp_0'Mp_0 + (1-t)p_0'Np_0 = p_0'Pp_0 = 0,$$

which leads to $p_1'Mp_1 = p_1'Np_1 = 1$ and $p_0'Mp_0 = p_0'Np_0 = 0$. Therefore, p_1 and p_0 are eigenvectors of M and N. Furthermore, the eigenvalues of M and N

corresponding to the eigenvectors p_1 and p_0 are 1 and 0, respectively. Since p_1 and p_0 are arbitrary eigenvectors of P, the matrices M and N have the same eigenvalues and eigenvectors with P, and correspondingly $P = M = N$, which, however, yields a contradiction. In view of these contradictions, we can say that a symmetric idempotent matrix is an extreme point of Φ.

Lastly, we aim to show that any other matrix which is not an idempotent matrix, say Z, cannot be an extreme point of Φ. Let Z have an eigen decomposition $Z = Q\mathrm{diag}(\lambda_1, \ldots, \lambda_p)Q'$. Since Z is not an idempotent matrix, there exists an eigenvalue, say λ_i, which is neither 1 nor 0. Then, for any $t \in (0,1)$, there exist two distinct $\lambda_{i,1}, \lambda_{i,2} \in [0,1]$ such that $\lambda_i = t\lambda_{i,1} + (1-t)\lambda_{i,2}$, e.g., set $\lambda_{i,1} = \lambda_i/t$ and $\lambda_{i,2} = 0$. Correspondingly, for the matrices

$$M \coloneqq Q\,\mathrm{diag}(\ldots, \lambda_{i,1}, \ldots)\,Q' \text{ and } N \coloneqq Q\,\mathrm{diag}(\ldots, \lambda_{i,2}, \ldots)\,Q',$$

we have $Z = tM + (1-t)N$, yet $M \neq N$, i.e., Z is not an extreme point of Φ.

APPENDIX B

TECHNICAL RESULTS IN CHAPTER 3

B.1 Computation of $K^{\omega}_{1:\kappa}, \Delta^{\omega}_{1:\kappa}$, and Δ^{ω}_{0}

A routine completion of squares leads to [56, 63]

$$\mathbb{E}\left\{\sum_{k=1}^{\kappa} \|\boldsymbol{x}_{k+1}\|^2_{Q_\omega} + \|\boldsymbol{u}_k\|^2_{R_\omega}\right\} = \sum_{k=1}^{\kappa} \mathbb{E}\left\{\|\boldsymbol{u}_k + K^{\omega}_k \boldsymbol{x}_k\|^2_{\Delta^{\omega}_k}\right\} + \Delta^{\omega}_0, \tag{B.1}$$

where

$$K^{\omega}_k = (\Delta^{\omega}_k)^{-1} B' \tilde{Q}^{\omega}_{k+1} A \tag{B.2}$$

$$\Delta^{\omega}_k = B' \tilde{Q}^{\omega}_{k+1} B + R_\omega \tag{B.3}$$

$$\Delta^{\omega}_0 = \mathrm{Tr}\{Q_\omega \Sigma_1\} + \sum_{k=1}^{\kappa} \mathrm{Tr}\{\tilde{Q}^{\omega}_{k+1} \Sigma_w\} \tag{B.4}$$

and $\{\tilde{Q}^{\omega}_k\}$ is given by the discrete-time dynamic Riccati equation

$$\tilde{Q}^{\omega}_k = Q_\omega + A'(\tilde{Q}^{\omega}_{k+1} - \tilde{Q}^{\omega}_{k+1} B (\Delta^{\omega}_k)^{-1} B' \tilde{Q}^{\omega}_{k+1}) A$$

and $\tilde{Q}^{\omega}_{\kappa+1} = Q_\omega$.

B.2 Computation of $V_{1:\kappa}(\omega)$ and v_o

Let $\omega_o \in \Omega$ denote the type of the benign controller, who has the same objective with $\mathcal{P}_S$. We define

$$\Phi(\omega) := \begin{bmatrix} I & K_\kappa^\omega B & K_\kappa^\omega AB & \cdots & K_\kappa^\omega A^{\kappa-2}B \\ & I & K_{\kappa-1}^\omega B & \cdots & K_{\kappa-1}^\omega A^{\kappa-3}B \\ & & I & \cdots & K_{\kappa-2}^\omega A^{\kappa-4}B \\ & & & \ddots & \vdots \\ & & & & I \end{bmatrix}$$

$$K(\omega) := \begin{bmatrix} K_\kappa^\omega & & \\ & \ddots & \\ & & K_1^\omega \end{bmatrix}, \ \Delta(\omega) := \begin{bmatrix} \Delta_\kappa^\omega & & \\ & \ddots & \\ & & \Delta_1^\omega \end{bmatrix}.$$

Then, (B.1) can be written as

$$\|\Phi(\omega)\boldsymbol{u} + K(\omega)\boldsymbol{x}^o\|^2_{\Delta(\omega)} + \Delta_0^\omega \tag{B.5}$$

in terms of the augmented vectors $\boldsymbol{u}, \boldsymbol{x}^o \in \mathbb{R}^{m\kappa}$. Correspondingly, the optimal attack is $\boldsymbol{u}^* = -\Phi(\omega)^{-1}K(\omega)\hat{\boldsymbol{x}}^o$, where $\hat{\boldsymbol{x}}^o := \begin{bmatrix}\mathbb{E}\{\boldsymbol{x}_\kappa^o|\boldsymbol{s}_{1:\kappa}\}' & \cdots & \mathbb{E}\{\boldsymbol{x}_1^o|\boldsymbol{s}_1\}'\end{bmatrix}'$, for type-$\omega$ controller. Therefore, $\mathcal{P}_S$, i.e., type-ω_o, faces the following problem:

$$\sum_{\omega\in\Omega} p_\omega \|K(\omega_o)\boldsymbol{x}^o - T(\omega)\hat{\boldsymbol{x}}^o\|_{\Delta(\omega_o)} + \Delta_0^{\omega_o}, \tag{B.6}$$

where $T(\omega) := \Phi(\omega_o)\Phi(\omega)^{-1}K(\omega)$. We introduce

$$\Xi(\omega) := T(\omega)'\Delta(\omega_o)T(\omega) - T(\omega)'\Delta(\omega_o)K(\omega_o) - K(\omega_o)'\Delta(\omega_o)T(\omega), \tag{B.7}$$

$$v_o := \mathrm{Tr}\{\Sigma^o K(\omega_o)'\Delta(\omega_o)K(\omega_o)\} + \Delta_0^{\omega_o}, \tag{B.8}$$

where $\Sigma^o := \mathbb{E}\{\boldsymbol{x}^o(\boldsymbol{x}^o)'\}$ is given by

$$\Sigma^o := \begin{bmatrix} \Sigma_\kappa^o & A\Sigma_{\kappa-1}^o & \cdots & A^{\kappa-1}\Sigma_1^o \\ \Sigma_{\kappa-1}^o A' & \Sigma_{\kappa-1}^o & & A^{\kappa-2}\Sigma_1^o \\ \vdots & & \ddots & \vdots \\ \Sigma_1^o(A^{\kappa-1})' & \Sigma_1^o(A^{\kappa-2})' & \cdots & \Sigma_1^o \end{bmatrix}. \tag{B.9}$$

Note that $v_o \in \mathbb{R}$ does not depend on the types of the controllers. Then, (B.6) can be written as

$$\sum_{\omega \in \Omega} p_\omega \mathrm{Tr}\{\mathbb{E}\{\hat{\boldsymbol{x}}^o(\hat{\boldsymbol{x}}^o)'\}\Xi(\omega)\} + v_o, \tag{B.10}$$

where we have

$$\mathbb{E}\{\hat{\boldsymbol{x}}^o(\hat{\boldsymbol{x}}^o)'\} := \begin{bmatrix} H_\kappa & AH_{\kappa-1} & \cdots & A^{\kappa-1}H_1 \\ H_{\kappa-1}A' & H_{\kappa-1} & & A^{\kappa-2}H_1 \\ \vdots & & \ddots & \vdots \\ H_1(A^{\kappa-1})' & H_1(A^{\kappa-2})' & \cdots & H_1 \end{bmatrix}.$$

Therefore, the corresponding $V_k(\omega) \in \mathbb{S}^m$ in (3.23) is given by

$$V_k(\omega) = \Xi_{k,k}(\omega) + \sum_{l=k+1}^{\kappa} \Xi_{k,l}(\omega)A^{l-k} + (A^{l-k})'\Xi_{l,k}(\omega), \tag{B.11}$$

where $\Xi_{k,l}(\omega) \in \mathbb{R}^{m \times m}$ is an $m \times m$ block of $\Xi(\omega)$, with indexing from the right-bottom to the left-top.

APPENDIX C

TECHNICAL RESULTS IN CHAPTER 4

C.1 Proof of Proposition 4.1

Claim C.1. *For any signaling rule $\pi \in \Pi$, $\Xi_\pi \in \mathbb{S}^n$ satisfies $\Xi_\pi \in \mathcal{CP}^n$ and $\Xi_\pi \underline{1} = \underline{p}_o$, where $\underline{p}_o := \begin{bmatrix} p_o(z_1) & \dots & p_o(z_n) \end{bmatrix}'$.*

Proof. We can decompose $\Xi_\pi \in \mathbb{S}^n$, as described in (4.22), as $\Xi_\pi = AA'$, where

$$A := \begin{bmatrix} p_{s_1}(z_1)p(s_1)^{1/2} & \cdots & p_{s_k}(z_1)p(s_k)^{1/2} \\ \vdots & & \vdots \\ p_{s_1}(z_n)p(s_1)^{1/2} & \cdots & p_{s_k}(z_n)p(s_k)^{1/2} \end{bmatrix}, \tag{C.1}$$

which is clearly a non-negative matrix since all the entries are products of (non-negative) probability measures. This yields that $\Xi_\pi \in \mathcal{CP}^n$.

For a given signaling rule $\pi \in \Pi$, let $\mathcal{S}_o \subseteq \mathcal{S}$ denote the set of signals that $\mathcal{P}_S$ sends with positive probability, i.e., $p(s) > 0$ for all $s \in \mathcal{S}_o$. Then, the sum of entries of Ξ_π at the ith row is given by

$$\sum_{j=1}^{n} \Xi_\pi[i,j] \overset{(a)}{=} \sum_{s \in \mathcal{S}_o} p(s) p_s(z_i) \overbrace{\sum_{j=1}^{n} p_s(z_j)}^{=1}, \tag{C.2}$$

$$\overset{(b)}{=} \sum_{s \in \mathcal{S}_o} \cancel{p(s)} \frac{\pi(s|z_i)p_o(z_i)}{\cancel{p(s)}}, \tag{C.3}$$

$$= p_o(z_i) \sum_{s \in \mathcal{S}_o} \pi(s|z_i), \tag{C.4}$$

$$\overset{(c)}{=} p_o(z_i), \tag{C.5}$$

where (a) follows from (4.17) and (4.18), (b) follows from (4.17), and (c) follows from (4.16). By (C.5), we have $\Xi_\pi \underline{1} = \underline{p}_o$, which completes the proof of the claim. □

Claim C.2. *For any completely positive matrix $\Xi \in \mathcal{CP}^n$ that satisfies $\Xi\underline{1} = \underline{p}_o$, there exists a signaling rule $\pi \in \Pi$ such that $\Xi_\pi = \Xi$, where $\Xi_\pi \in \mathcal{CP}^n$ is as described in* (4.22).

Proof. Consider any completely positive matrix $\Xi \in \mathcal{CP}^n$ that satisfies $\Xi\underline{1} = \underline{p}_o$. By the definition of completely positive matrices, we can decompose $\Xi \in \mathcal{CP}^n$ into $\Xi = BB'$, where

$$B = \begin{bmatrix} \underline{b}_1 & \dots & \underline{b}_k \end{bmatrix} \in \mathbb{R}_+^{n\times k} \tag{C.6}$$

is some non-negative matrix. We note that the decomposition is not necessarily a unique one [91]. For example, by padding zero columns into B, we can generate infinitely many decompositions. Correspondingly, we assume, without loss of generality, that in the decomposition of $\Xi \in \mathcal{CP}^n$, the non-negative matrix $B \in \mathbb{R}_+^{n\times k}$ does not have an all zero column, i.e., $\underline{b}_i \neq \underline{0}$ for all $i = 1, \dots, k$.

Recall that for any given signaling rule $\pi \in \Pi$, we can decompose $\Xi_\pi = AA'$, where the matrix $A \in \mathbb{R}_+^{n\times|\mathcal{S}|}$ is as described in (C.1). Correspondingly, if we can show that there exists a signaling rule $\pi \in \Pi$ such that $A = B$, then this would imply that $\Xi = \Xi_\pi$ for that signaling rule. To this end, we let $|\mathcal{S}| = k$, and introduce auxiliary vectors

$$\underline{\pi}_i := \begin{bmatrix} \pi(s_i|z_1) & \dots & \pi(s_i|z_n) \end{bmatrix}', \tag{C.7}$$

which, by (4.18), yields that $p(s_i) = \underline{\pi}_i'\underline{p}_o$. Therefore, by substituting (4.17) in (C.1), we can write the matrix A as

$$A = P_o \begin{bmatrix} \frac{\underline{\pi}_1}{\sqrt{\underline{\pi}_1'\underline{p}_o}} & \cdots & \frac{\underline{\pi}_k}{\sqrt{\underline{\pi}_k'\underline{p}_o}} \end{bmatrix}, \tag{C.8}$$

where $P_o := \operatorname{diag}\{\underline{p}_o\}$, which is nonsingular since the prior distribution p_o has complete support on $\mathcal{Z}$. Correspondingly, A would be equal to B provided that

$$\frac{P_o\underline{\pi}_i}{\sqrt{\underline{\pi}_i'\underline{p}_o}} = b_i,\ \forall i = 1, \dots, k, \tag{C.9}$$

and it can be verified that we have (C.9) if

$$\underline{\pi}_i = \underline{b}_i'\underline{1}P_o^{-1}\underline{b}_i. \tag{C.10}$$

However, we also need to inspect the validity of (C.10) as a signaling rule. Particularly, we have the constraints on the signaling strategies that $\pi(s|z) \geq 0$ for all $s \in \mathcal{S}$ and $z \in \mathcal{Z}$, and (4.16).[1] The former constraint is satisfied by the definition, since $\underline{b}_i$ is a column of the non-negative matrix $B \in \mathbb{R}_+^{n\times k}$. Verification of the latter constraint (4.16) is relatively more involved. To this end, let us introduce

$$\underline{\Pi} := \begin{bmatrix} \underline{\pi}_1 & \dots & \underline{\pi}_k \end{bmatrix}. \tag{C.11}$$

Then, the latter constraint is equivalent to $\underline{\Pi 1} = \underline{1}$, i.e., the sum of columns of $\underline{\Pi}$ is an all 1s vector. If we set $\underline{\pi}_i$ as in (C.10), then we would obtain

$$\underline{\Pi} = \begin{bmatrix} (\underline{b}_1'\underline{1})P_o^{-1}\underline{b}_1 & \dots & (\underline{b}_k'\underline{1})P_o^{-1}\underline{b}_n \end{bmatrix}, \tag{C.12}$$

and correspondingly the sum of columns of $\underline{\Pi}$ is given by

$$\underline{\Pi 1} = P_o^{-1}\sum_{i=1}^{k}\underline{b}_i(\underline{b}_i'\underline{1}). \tag{C.13}$$

Note that $(\underline{b}_i'\underline{1})P_o^{-1}\underline{b}_i = P_o^{-1}\underline{b}_i(\underline{b}_i'\underline{1})$ since $\underline{b}_i'\underline{1}$ is just a scalar.

Recall that the completely positive matrix $\Xi \in \mathcal{CP}^n$ satisfies $\Xi\underline{1} = \underline{p}_o$, which can also be written as

$$BB'\underline{1} = \underline{p}_o \Leftrightarrow \sum_{i=1}^{k}\underline{b}_i\underline{b}_i'\underline{1} = \underline{p}_o. \tag{C.14}$$

Therefore, by (C.13) and (C.14), we obtain $\underline{\Pi 1} = P_o^{-1}\underline{p}_o = \underline{1}$, and correspondingly (C.10) is a valid signaling strategy, which completes the proof of the claim. □

Based on (4.23), Claims C.1 and C.2 yield (4.29), and (4.26) follows from (C.10), which completes the proof.

C.2 Proof of Proposition 4.4

The primal problem is feasible since the constraint set is not empty based on Claims C.1 and C.2.

[1] Note that if both of these constraints hold, this would also imply that $\pi(s|z) \in [0,1]$ for all $s \in \mathcal{S}$ and $z \in \mathcal{Z}$.

The fact that the primal problem has finite value follows by the extreme value theorem since the optimization objective is linear in the optimization argument and the constraint set

$$\{\Xi \in \mathcal{CP}^n | \Xi \underline{1} = \underline{p}_o\} \tag{C.15}$$

is a closed and bounded subset of $\mathcal{CP}^n$.

It is relatively more involved to show that the primal problem entails an interior point. Particularly, a characterization of the interior of $\mathcal{CP}^n$ is given by [102, Theorem 3.3]

$$\begin{aligned} \operatorname{int}\{\mathcal{CP}^n\} = \{AA' \,|\, \operatorname{rank} A = n, A = \begin{bmatrix} \underline{a} & \tilde{A} \end{bmatrix} \\ \ni \underline{a} > 0, \tilde{A} \geq 0\}. \end{aligned} \tag{C.16}$$

Therefore, the question is whether there exists a $\Xi \in \operatorname{int}\{\mathcal{CP}^n\}$ such that $\Xi \underline{1} = \underline{p}_o$.

Based on Claims C.1 and C.2, let us consider the associated signaling problem where we set the signal space as $\mathcal{S} = \{s_o = \varnothing, s_1 = z_1, \ldots, s_n = z_n\}$, and the prior distribution over $\mathcal{Z}$ to have full support, without loss of generality. Consider the two extreme cases: full disclosure and null disclosure, respectively, given and denoted by $\overline{\pi}(z_i) = z_i$, and $\underline{\pi}(z_i) = \varnothing$ for all $i = 1, \ldots, n$. Note that for a given signaling strategy $\pi \in \Pi$, an entry of the associated completely positive matrix Ξ_π is described in (4.22). Furthermore, a component of a decomposition of Ξ_π is described in (C.1). Correspondingly, we obtain

$$\Xi_{\overline{\pi}} = \overline{AA'} \ni \overline{A} := \begin{bmatrix} \underline{0} & P_o \end{bmatrix}, \tag{C.17}$$

$$\Xi_{\underline{\pi}} = \underline{AA'} \ni \underline{A} := \begin{bmatrix} \underline{p}_o & O \end{bmatrix}. \tag{C.18}$$

This yields that if $\mathcal{P}_S$ selects a signaling strategy $\pi \in \Pi$ that discloses $z \in \mathcal{Z}$ truthfully, i.e., $s_i = z_i$, with probability $\lambda \in (0,1)$ and discloses s_o otherwise, then we obtain

$$\Xi_\pi = AA' \ni A := \begin{bmatrix} (1-\lambda)\underline{p}_o & \lambda P_o \end{bmatrix}, \tag{C.19}$$

in which the first column is a positive vector and $\operatorname{rank} A = n$ since p_o is an all-positive vector, i.e., the prior distribution has full support over $\mathcal{Z}$ by the formulation. This yields that $\Xi_\pi \in \operatorname{int}\{\mathcal{CP}^n\}$ and $\Xi_\pi \underline{1} = \underline{p}_o$.

Since the conditions for the strong duality theorem [105, Theorem 4.7.1] hold, we have strong duality between the primal and dual problems, which concludes the proof.

C.3 Proof of Corollary 4.5

We first note that the following inequality always holds

$$\min_{\boldsymbol{s}} \operatorname{Tr}\left\{\mathbb{E}\left\{\hat{\boldsymbol{z}}\hat{\boldsymbol{z}}'\right\} V\right\} \leq \min_{\boldsymbol{s}} \operatorname{Tr}\left\{\mathbb{E}\left\{\hat{\boldsymbol{z}}_q\hat{\boldsymbol{z}}_q'\right\} V\right\} \tag{C.20}$$

since any quantization would restrict $\mathcal{P}_S$'s strategy space for continuous distributions.

Let $\hat{\boldsymbol{e}} = \hat{\boldsymbol{z}} - \hat{\boldsymbol{z}}_q$ for a given signal $\boldsymbol{s}$, i.e., $\hat{\boldsymbol{e}} = \mathbb{E}\left\{\boldsymbol{e}|\boldsymbol{s}\right\}$. Then, for any signal $\boldsymbol{s} \sim \mathcal{Z}$, we have

$$\mathbb{E}\left\{\hat{\boldsymbol{z}}\hat{\boldsymbol{z}}'\right\} = \mathbb{E}\left\{\hat{\boldsymbol{z}}_q\hat{\boldsymbol{z}}_q'\right\} + \mathbb{E}\left\{\hat{\boldsymbol{z}}_q\hat{\boldsymbol{e}}'\right\} + \mathbb{E}\left\{\hat{\boldsymbol{e}}\hat{\boldsymbol{z}}_q'\right\} + \mathbb{E}\left\{\hat{\boldsymbol{e}}\hat{\boldsymbol{e}}'\right\}.$$

Correspondingly, we obtain

$$\begin{aligned}\min_{\boldsymbol{s}} \operatorname{Tr}\left\{\mathbb{E}\left\{\hat{\boldsymbol{z}}\hat{\boldsymbol{z}}'\right\} V\right\} \geq{}& \min_{\boldsymbol{s}} \operatorname{Tr}\left\{\mathbb{E}\left\{\hat{\boldsymbol{z}}_q\hat{\boldsymbol{z}}_q'\right\} V\right\} \\ &+ \min_{\boldsymbol{s}} \operatorname{Tr}\left\{(\mathbb{E}\left\{\hat{\boldsymbol{z}}_q\hat{\boldsymbol{e}}'\right\} + \mathbb{E}\left\{\hat{\boldsymbol{e}}\hat{\boldsymbol{z}}_q'\right\} + \mathbb{E}\left\{\hat{\boldsymbol{e}}\hat{\boldsymbol{e}}'\right\})V\right\}.\end{aligned} \tag{C.21}$$

Let us take a closer look at the second term on the right-hand side, which can also be written as

$$-\max_{\boldsymbol{s}} -\operatorname{Tr}\left\{(\mathbb{E}\left\{\hat{\boldsymbol{z}}_q\hat{\boldsymbol{e}}'\right\} + \mathbb{E}\left\{\hat{\boldsymbol{e}}\hat{\boldsymbol{z}}_q'\right\} + \mathbb{E}\left\{\hat{\boldsymbol{e}}\hat{\boldsymbol{e}}'\right\})V\right\}. \tag{C.22}$$

Then, the Cauchy-Schwarz inequality for random vectors yields that (C.22) is bounded from above by

$$-2\mathbb{E}\left\{\hat{\boldsymbol{z}}_q' V\hat{\boldsymbol{e}}\right\} - \mathbb{E}\left\{\hat{\boldsymbol{e}}' V\hat{\boldsymbol{e}}\right\} \leq (2\|\hat{\boldsymbol{z}}_q\| + \|\hat{\boldsymbol{e}}\|)\|V\|_2\|\hat{\boldsymbol{e}}\|,$$

since $\|-V\|_2 = \|V\|_2$. Note that the right-hand side depends on the signal $\boldsymbol{s}$.

However, we also have

$$\|\boldsymbol{z}_q - \hat{\boldsymbol{z}}_q\|^2 = \|\boldsymbol{z}_q\|^2 - \|\hat{\boldsymbol{z}}_q\|^2 \geq 0, \tag{C.23}$$

$$\|\boldsymbol{e} - \hat{\boldsymbol{e}}\|^2 = \|\boldsymbol{e}\|^2 - \|\hat{\boldsymbol{e}}\|^2 \geq 0. \tag{C.24}$$

Therefore, by (C.23) and (C.24), we obtain

$$-2\mathbb{E}\left\{\hat{\boldsymbol{z}}_q' V \hat{\boldsymbol{e}}\right\} - \mathbb{E}\left\{\hat{\boldsymbol{e}}' V \hat{\boldsymbol{e}}\right\} \leq (2\|\boldsymbol{z}_q\| + \|\boldsymbol{e}\|)\|V\|_2\|\boldsymbol{e}\|, \tag{C.25}$$

where, now, the right-hand side does not depend on the signal. Therefore, we obtain

$$\epsilon \geq \min_{\boldsymbol{s}} \operatorname{Tr}\left\{\mathbb{E}\left\{\hat{\boldsymbol{z}}_q \hat{\boldsymbol{z}}_q'\right\} V\right\} - \min_{\boldsymbol{s}} \operatorname{Tr}\left\{\mathbb{E}\left\{\hat{\boldsymbol{z}} \hat{\boldsymbol{z}}'\right\} V\right\} \geq 0,$$

where ϵ is as described in (4.36), which completes the proof.

REFERENCES

[1] Y. N. Harari, *Homo Sapiens: A Brief History of Humankind.* Harper Collins Publishers, 2015.

[2] B. Brown, M. Chun, and J. Manyika, "Are your ready for the era of 'big data'," *McKinsey Quarterly*, vol. 4, no. 1, pp. 24–35, 2011.

[3] T. Başar and G. J. Olsder, *Dynamic Noncooperative Game Theory.* Society for Industrial Mathematics (SIAM) Series in Classics in Applied Mathematics, 1999.

[4] V. Crawford and J. Sobel, "Strategic information transmission," *Econometrica*, vol. 50, no. 6, pp. 1431–1451, 1982.

[5] J. Sobel, *Signaling Games.* New York, NY: Springer New York, 2009, pp. 8125–8139.

[6] J. Farrell and R. Gibbons, "Cheap talk with two audiences," *American Economic Review*, vol. 79, pp. 1214–1223, 1986.

[7] J. Farrell and M. Rabin, "Cheap talk," *J. Econ. Pers.*, vol. 10, no. 3, pp. 103–118, 1996.

[8] T. W. Gilligan and K. Krehbiel, "Collective decision-making and standing committees: An informational rational for restrictive amendments procedures," *Journal of Law, Economics & Organizations*, vol. 3, pp. 287–335, 1989.

[9] V. Krishna and J. Morgan, "A model of expertise," *The Quarterly Journal of Economics*, vol. 116, pp. 747–775, 2000.

[10] M. Battaglini, "Multiple referrals and multidimensional cheap talk," *Econometrica*, vol. 70, no. 4, pp. 1379–1401, 2002.

[11] S. Morris, "Political correctness," *Journal of Political Economy*, vol. 109, pp. 231–265, 2001.

[12] N. Kartik, M. Ottaviani, and F. Squintani, "Credulity, lies, and costly talk," *J. Econ. Theory*, vol. 134, no. 1, pp. 93–116, 2007.

[13] J. Mathis, “Full revelation of information in sender - receiver games of persuasion,” *J. Econ. Theory*, vol. 143, no. 1, pp. 571–584, 2008.

[14] M. Golosov, V. Skreta, A. Tsyvinski, and A. Wilson, “Dynamic strategic information transmission,” *J. Economic Theory*, vol. 151, pp. 304–341, 2014.

[15] E. Kamenica and M. Gentzkow, “Bayesian persuasion,” *American Economic Review*, vol. 101, pp. 25 090–2615, 2011.

[16] D. Bergemann and S. Morris, “Information design, Bayesian persuasion, and Bayes correlated equilibrium,” *American Economic Review Papers & Proceedings*, vol. 106, no. 5, pp. 586–591, 2016.

[17] D. Bergemann and S. Morris, “Information design: A unified perspective,” *Journal of Economic Literature*, vol. forthcoming, 2018.

[18] M. Gentzkow and E. Kamenica, “Bayesian persuasion with multiple senders and rich signal spaces,” *Games and Economic Behavior*, vol. 104, pp. 411–429, 2017.

[19] J. C. Ely, “Beeps,” *American Economic Review*, vol. 107, pp. 31–53, 2017.

[20] M. Gentzkow and E. Kamenica, “Costly persuasion,” *American Economic Review*, vol. 104, no. 5, pp. 457–462, 2014.

[21] E. Kamenica, “Bayesian persuasion and information design,” *Annual Review of Economics*, vol. 11, 2019.

[22] W. Tamura, “A theory of multidimensional information disclosure,” *Working paper, available at SSRN 1987877*, 2014.

[23] J. Pawlick, E. Colbert, and Q. Zhu, “A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy,” *ArXiv:1712.05441*, 2017.

[24] D. G. Howe and H. Nissenbaum, “TrackMeNot: Resisting surveillance in web search,” in *On the Identity Trail: Privacy, Anonymity and Identity in a Networked Society*, I. Kerr, C. Lucock, and V. Steeves, Eds. Oxford University Press, 2009.

[25] A. Clark, Q. Zhu, R. Poovendran, and T. Başar, “Deceptive routing in relay networks,” in *Proceedings of International Conference on Decision and Game Theory for Security on Lecture Notes in Computer Science*, J. Grossklags and J. Warland, Eds. Berlin, Heidelberg: Springer, 2012.

[26] Q. Zhu, A. Clark, R. Poovendran, and T. Başar, "Deceptive routing games," in *Proceedings of IEEE Conf. on Decision and Control*, 2012, pp. 2704–2711.

[27] L. Spitzner, *Honeypots: Tracking Hackers.* Addison-Wesley Professional, 2002.

[28] T. E. Carroll and D. Grosu, "A game theoretic investigation of deception in network security," *Security and Commun. Nets*, vol. 4, no. 10, 2011.

[29] S. Sarıtaş, S. Yüksel, and S. Gezici, "Quadratic multi-dimensional signaling games and affine equilibria," *IEEE Trans. Autom. Control*, vol. 62, no. 2, pp. 605–619, 2017.

[30] E. Akyol, C. Langbort, and T. Başar, "Information-theoretic approach to strategic communication as a hierarchical game," *Proceedings of the IEEE*, vol. 105, no. 2, pp. 205–218, 2017.

[31] F. Farokhi, A. Teixeira, and C. Langbort, "Estimation with strategic sensors," *IEEE Trans. Autom. Control*, vol. 62, no. 2, pp. 724–739, 2017.

[32] M. O. Sayin, E. Akyol, and T. Başar, "On the structure of equilibrium strategies in dynamic Gaussian signaling games," in *Proceedings of the IEEE Multi–Conference on Systems and Control*, 2016, pp. 749–754.

[33] M. O. Sayin, E. Akyol, and T. Başar, "Strategic control of a tracking system," in *Proceedings of the 55th IEEE Conference on Decision and Control*, 2016, pp. 6147–6153.

[34] M. O. Sayin, E. Akyol, and T. Başar, "Hierarchical multistage Gaussian signaling games in noncooperative communication and control systems," *Automatica*, vol. 107, pp. 9–20, 2019.

[35] M. O. Sayin and T. Başar, "Dynamic information disclosure for deception," in *Proceedings of the 57th IEEE Conference on Decision and Control (CDC)*, 2018.

[36] M. O. Sayin and T. Başar, "On the optimality of linear signaling to deceive Kalman filters over finite/infinite horizons," in *Proceedings of International Conference on Decision and Game Theory for Security on Lecture Notes in Computer Science*, T. Alpcan, J. S. Baras, T. Başar, A. Ephremides, and M. Tambe, Eds. Stockholm, Sweden: Springer, 2019.

[37] M. O. Sayin and T. Başar, "Deceptive multi-dimensional information disclosure over a Gaussian channel," in *Proceedings of the American Control Conference (ACC)*, 2018, pp. 6545–6552.

[38] M. O. Sayin and T. Başar, “Robust sensor design against multiple attackers with misaligned control objectives,” *arXiv:1901.10618*, 2019.

[39] M. O. Sayin and T. Başar, “Secure sensor design for cyber-physical systems against advanced persistent threats,” in *Proceedings of International Conference on Decision and Game Theory for Security on Lecture Notes in Computer Science*, S. Rass, B. An, C. Kiekintveld, F. Fang, and S. Schauder, Eds., vol. 10575. Vienna, Austria: Springer, Oct. 2017, pp. 91–111.

[40] M. O. Sayin and T. Başar, “Secure sensor design against undetected infiltration: Minimum impact-minimum damage,” *arXiv:1801.01630*, 2018.

[41] M. O. Sayin and T. Başar, “Secure sensor design for resiliency of control systems prior to attack detection,” in *Proceedings of the IEEE Conference on Control Technology and Applications (CCTA)*, 2018.

[42] M. O. Sayin and T. Başar, “Deception-as-defense framework for cyber-physical systems,” *arXiv:1902.01364*, 2019.

[43] M. O. Sayin and T. Başar, “Optimal hierarchical signaling for quadratic cost measures and general distributions: A copositive program characterization,” *ArXiv:1907.09070*, 2019.

[44] E. Akyol, C. Langbort, and T. Başar, “Privacy constrained information processing,” in *Proceedings of the 54th IEEE Conference on Decision and Control*, 2015, pp. 4511–4516.

[45] S. Sarıtaş, S. Yüksel, and S. Gezici, “Dynamic signaling games under Nash and Stackelberg equilibria,” in *Proceedings of the IEEE International Symposium on Information Theory*, 2016, pp. 1631–1635.

[46] E. Akyol, C. Langbort, and T. Başar, “Strategic compression and transmission of information,” in *Proceedings of the IEEE Inf. Theory Workshop*, 2015.

[47] I. Greenberg, “The role of deception in decision theory,” *J. Conflict Resolution*, vol. 26, pp. 139–156, 1982.

[48] I. Greenberg, “The effect of deception on optimal decisions,” *Operations Research Letters*, vol. 4, 1982.

[49] D. Li and J. B. Cruz-Jr., “Information, decision-making and deception in games,” *Decision Support Systems*, vol. 47, pp. 518–527, 2009.

[50] Q. Zhu and T. Başar, "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 Systems*, vol. 35, no. 1, pp. 46–65, 2015.

[51] Y. Han, J. Chan, T. Alpcan, C. Leckie, and B. I. P. Rubinstein, "A game theoretical approach to defend against co-resident attacks in cloud computing: Preventing co-residence using semi-supervised learning," *IEEE Trans. on Information Forensics Security*, vol. 11, no. 3, pp. 556–570, 2015.

[52] Y. Han, J. Chan, T. Alpcan, and C. Leckie, "Using virtual machine allocation policies to defend against co-resident attacks in cloud computing," *IEEE Trans. on Dependable and Secure Computing*, vol. 14, no. 1, pp. 95–108, 2017.

[53] "Verizon's 2016 data breach investigation report," http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/, 2016, accessed: 2016-11-2.

[54] S. Jajodia, V. S. Subrahmanian, and V. Swarup, *Cyber Deception: Building the Scientific Foundation.* Springer International Publishing, Switzerland, 2016.

[55] K. E. Heckman, M. J. Walsh, F. J. Stech, T. A. O'Boyle, S. R. Dicato, and A. F. Herber, "Active cyber network defense with denial and deception," *J. Computers and Security*, vol. 37, pp. 72–77, 2013.

[56] P. R. Kumar and P. Varaiya, *Stochastic Systems.* Prentice-Hall, 1986.

[57] P. Billingsley, *Probability and Measure.* John Wiley & Sons Inc., 2008.

[58] G. Blekherman, P. A. Parrilo, and R. R. Thomas, *Semidefinite Optimization and Convex Algebraic Geometry.* Society for Industrial Mathematics (SIAM) Series on Optimization, 2012.

[59] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.1," http://cvxr.com/cvx, mar 2014.

[60] M. Grant and S. Boyd, "Graph implementations for nonsmooth convex programs," in *Recent Advances in Learning and Control.* Springer-Verlag Limited, 2008, pp. 95–110.

[61] G. Sierksma, V. Soltan, and T. Zamfirescu, "Invariane of convex sets under linear transformations," *Linear and Multilinear Algebra*, vol. 35, pp. 37–47, 1993.

[62] R. A. Horn and C. R. Johnson, *Matrix Analysis.* Cambridge University Press, 1985.

[63] R. Bansal and T. Başar, "Simultaneous design of measurement and control strategies for stochastic systems with feedback," *Automatica*, vol. 25, no. 5, pp. 679–694, 1989.

[64] T. Tanaka and H. Sandberg, "SDP-based joint sensor and controller design for information regularized optimal LQG control," in *Proc. 54th IEEE Conf. Decision and Control (CDC)*, 2012.

[65] R. B. Myerson, *Game Theory: Analysis of Conflict.* Harvard University Press, 1997.

[66] J. Giraldo, E. Sarkar, A. A. Cardenas, M. Maniatakos, and M. Kantarcioglu, "Security and privacy in cyber-physical systems: A survey of surveys," *IEEE Design & Test*, vol. 34, pp. 7–17, 2017.

[67] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security – A survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, 2017.

[68] N. Nelson, "The impact of Dragonfly malware on industrial control systems," *The SANS Institute*, 2016.

[69] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Information and System Security*, vol. 14, no. 1, 2009.

[70] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc. 47th Allerton Conf. Communication, Control, and Computing*, 2009.

[71] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on SCADA systems," *IEEE Trans. Control Syst. Tech.*, vol. 22, no. 4, 2014.

[72] Y. Mo and B. Sinopoli, "Integrity attacks on cyber-physical systems," in *Proc. 1st ACM Int. Conf. High Confidence Networked Systems*, 2012, pp. 47–54.

[73] Y. Mo and B. Sinopoli, "On the performance degradation of cyber-physical systems under stealthy integrity attacks," *IEEE Trans. Autom. Control*, vol. 61, no. 9, pp. 2618–2624, 2016.

[74] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "Revealing stealthy attacks in control systems," in *Proc. 50th Allerton Conf. Communication, Control, and Computing*, 2012.

[75] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, 2013.

[76] H. Fawzi, P. Tabuada, and S. Diggavi, “Secure estimation and control for cyber physical systems under adversarial attacks,” *IEEE Trans. Autom. Control*, vol. 59, no. 6, pp. 1454–1467, 2014.

[77] Y. Chen, S. Kar, and J. M. F. Moura, “Cyber physical attacks with control objectives and detection constraints,” in *Proc. 55th IEEE Conf. on Decision and Control (CDC)*, 2016, pp. 1125–1130.

[78] Y. Chen, S. Kar, and J. M. F. Moura, “Cyber physical attacks constrained by control objectives,” in *Proc. Americal Control Conference (ACC)*, 2016, pp. 1185–1190.

[79] R. Zhang and P. Venkitasubramaniam, “Stealthy control signal attacks in linear quadratic Gaussian control systems: Detectability reward tradeoff,” *IEEE Trans. Inf. Forensics and Security*, vol. 12, no. 7, pp. 1555–1570, 2017.

[80] F. Miao, Q. Zhu, M. Pajic, and G. J. Pappas, “Coding schemes for securing cyber-physical systems against stealthy data injection attacks,” *IEEE Trans. Autom. Control*, vol. 4, no. 1, pp. 106–117, 2017.

[81] S. Boyd and L. Vandenberghe, *Convex Optimization.* Cambridge University Press, 2004.

[82] E. Ok, *Real Analysis with Economics Applications.* Princeton University Press, 2007.

[83] A. G. Dimakis, S. Kar, J. M. F. Moura, M. G. Rabbat, and A. Scaglione, “Gossip algorithms for distributed signal processing,” *Proceedings of the IEEE*, vol. 98, no. 11, pp. 1847–1864, 2010.

[84] L. Rayo and I. Segal, “Optimal information disclosure,” *J. Political Economy*, vol. 118, no. 5, pp. 949–987, 2010.

[85] F. Tardella, “On the existence of polyhedral convex envelopes,” in *Frontiers in Global Optimization. Nonconvex Optimization and Its Applications*, C. A. Floudas and P. Pardalos, Eds. Boston, MA: Springer, 2004, vol. 74.

[86] M. Gentzkow and E. Kamenica, “A Rothschild-Stiglitz approach to Bayesian persuasion,” *American Economic Review*, vol. 106, no. 5, pp. 597–601, 2016.

[87] A. Kolotilin, “Optimal information disclosure: A linear programming approach,” *Theoretical Economics*, vol. 13, pp. 607–635, 2018.

[88] P. Dworczak and G. Martini, “The simple economics of optimal persuasion,” *Journal of Political Economy*, vol. forthcoming, 2019.

[89] S. Dughmi and H. Xu, "Algorithmic Bayesian persuasion," in *Proceedings of the 47th ACM Symposium on Theory of Computing (STOC)*, 2016.

[90] S. Dughmi, "Algorithmic information structure design: A survey," *ACM SIGecom Exchanges*, vol. 15, no. 2, pp. 2–24, 2017.

[91] A. Berman and N. Shaked-Monderer, *Completely Positive Matricees.* World Scientific Publishing, 2003.

[92] P. J. C. Dickinson and M. Dür, "Linear time complete positivity and detection and decomposition of sparse matrices," *SIAM Journal on Matrix Analysis and Applications*, vol. 33, pp. 701–720, 2012.

[93] P. Groetzner and M. Dür, "A factorization method for completely positive matrices," *preprint*, 2019.

[94] J. E. Maxfield and H. Minc, "On the matrix equation X'X = A," *Proceedings of the Edinburgh Mathematical Society*, vol. 13, no. II, pp. 125–129, 1962.

[95] S. Bundfuss and M. Dür, "An adaptive linear approximation algorithm for copositive programs," *SIAM J. Optim.*, vol. 20, no. 1, pp. 30–53, 2009.

[96] P. Parillo, "Structured semidefinite programs and semi-algebraic geometry methods in robustness and optimization," Ph.D. dissertation, California Institute of Technology, 2000.

[97] E. de Klerk and R. Sotirov, "Approximation of the stability in semidefinite programming relaxations of the quadratic assignment problem," *SIAM J. Optim.*, vol. 12, no. 4, 2002.

[98] E. A. Yildirim, "On the accuracy of uniform polyhedral approximations of the copositive cone," *Optimization Methods and Software*, vol. 27, no. 1, pp. 155–173, 2012.

[99] E. A. Yildirim, "Inner approximations of completely positive reformulations of mixed binary quadratic programs: A unified analysis," *Optimization Methods and Software*, vol. 32, no. 6, pp. 1163–1186, 2017.

[100] M. S. Bostanabad, J. Gouveia, and T. K. Pong, "Inner approximating the completely positive cone via the cone of scaled diagonally dominant matrices," *ArXiv:1807.00379*, 2018.

[101] R. M. Gray and D. L. Neuhoff, "Quantization," *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2325–2383, 1998.

[102] P. J. Dickinson, "An improved characterisation of the interior of the completely positive cone," *Electronic J. Linear Algebra*, vol. 20, pp. 723–729, 2011.

[103] A. Berman, M. Dür, and N. Shaked-Monderer, "Open problems in the theory of completely positive and copositive matrices," *Electronic Journal of Linear Algebra*, vol. 29, pp. 46–58, 2015.

[104] I. M. Bomze, P. J. C. Dickinson, and G. Still, "The structure of completely positive matrices according to their cp-rank and cp-plus-rank," *Linear Algebra and its Applications*, vol. 482, pp. 191–206, 2015.

[105] B. Gärtner and J. Matoušek, *Approximation algorithms and semidefinite programming.* Springer-Verlag Berlin Heidelberg, 2012.