Adversarial Radar Inference: Inverse Tracking, Identifying Cognition and Designing Smart Interference

Vikram Krishnamurthy, Fellow, IEEE, Kunal Pattanayak, Student Member, IEEE, Sandeep Gogineni, Member, IEEE, Bosung Kang, Member, IEEE, Muralidhar Rangaswamy, Fellow, IEEE

Abstract—This paper considers three inter-related adversarial inference problems involving cognitive radars. We first discuss inverse tracking of the radar to estimate the adversary’s estimate of the radar’s actions and calibrate the radar’s sensing accuracy. Second, using revealed preference from microeconomics, we formulate a non-parametric test to identify if the cognitive radar is a constrained utility maximizer with signal processing constraints. We consider two radar functionalities, namely, beam allocation and waveform design, with respect to which the cognitive radar is assumed to maximize its utility and construct a set-valued estimator for the radar’s utility function. Finally, we discuss how to engineer interference at the physical layer level to confuse the radar which forces it to change its transmit waveform. The levels of abstraction range from smart interference design based on Wiener filters (at the pulse/waveform level), inverse Kalman filters at the tracking level and revealed preferences for identifying utility maximization at the system level.

Index Terms—Inverse Tracking, Smart Interference, Revealed Preference, Constrained Utility Maximization, Kalman filter, Bayesian Inference, Physical Layer Interference, Adversarial Inference, Radar Signal Processing

Glossary of Symbols.

Inverse Tracking (Sec.II)

- \( x_k \): our kinematic state at time \( k \)
- \( P_{x_{k+1},x_k} \): transition kernel \( p(x_{k+1}|x_k) \)
- \( u_k \): state noise at time \( k \)
- \( Q_k \): covariance of \( u_k \)
- \( y_k \): observation of \( x_k \)
- \( v_k \): observation noise at time \( k \)
- \( R_k \): covariance of \( v_k \)
- \( C \): adversary sensor gain
- \( B_{x_k,y_k} \): conditional pdf of \( y_k \) given state \( x_k \) \( p(y_k|x_k) \)
- \( \pi_k \): adversary’s belief of \( x_k \)
- \( T(\pi,y) \): belief update
- \( \hat{x}_k \): conditional mean of state estimate of \( x_k \)
- \( \Sigma_k \): covariance of state estimate of \( x_k \)
- \( u_k \): adversary’s action at time \( k \)
- \( \phi \): stochastic mapping from \( \pi_k \) to \( u_k \)
- \( a_k \): our measurement of \( u_k \)
- \( G_{\pi_k,a_k} \): conditional pdf of \( a_k \) given belief \( \pi_k \) \( p(a_k|\pi_k) \)
- \( \rho_k \): our belief of \( \pi_k \) given \( x_k \) and \( a_k \)
- \( \hat{x}_k \): conditional mean of \( \hat{x}_k \)
- \( \Sigma_k \): covariance of \( \hat{x}_k \)
- \( \theta \): model parameter for \( C \)
- \( L_N \): log-likelihood
- \( t_k \): innovations of inverse Kalman filter

Identifying Cognition (Sec.III)

- \( n \): slow time scale index
- \( \alpha_n \): probe signal at time \( n \)
- \( \beta_n \): adversary’s response at time \( n \)
- \( U(\beta) \): adversary’s utility function

Smart Interference (Sec.IV)

- \( X_l \): adversary’s received signal at \( l^{th} \) pulse
- \( H_l(\ell) \): transmit channel impulse response at \( l^{th} \) pulse
- \( H_c(\ell) \): clutter channel impulse response at \( l^{th} \) pulse
- \( H_p(\ell) \): probe signal at \( l^{th} \) pulse
- \( W(\ell) \): radar’s transmission waveform at \( l^{th} \) pulse
- \( E_r(\ell) \): measurement noise in \( X(\ell) \)
- \( C_r \): covariance of \( E_r(\ell) \)
- \( Y(\ell) \): our observation of \( W(\ell) \)
- \( E_o(\ell) \): measurement noise in \( Y(\ell) \)
- \( C_o \): covariance of \( E_o(\ell) \)

I. INTRODUCTION

Cognitive sensors are reconfigurable sensors that optimize their sensing mechanism and transmit functionalities. The con-
cept of cognitive radar [11], [26], [27], [20] has evolved over the last two decades and a common aspect is the sense-learn-adapt paradigm. A cognitive fully adaptive radar enables joint optimization of the adaptive transmit and receive functions by sensing (estimating) the radar channel that includes clutter and other interfering signals [5], [13].

A. Objectives

This paper addresses the next step and achieves the following objectives schematically shown in Figure 1. The framework in this paper involves an adversarial signal processing problem comprising “us” and an “adversary”. “Us” refers to an asset such as a drone/UA V or electromagnetic signal that probes an “adversary” cognitive radar. Figure 2 shows the schematic setup. A cognitive sensor observes our kinematic state \( x_k \) in noise as the observation \( y_k \). It then uses a Bayesian tracker to update its posterior distribution \( \pi_k \) of our state \( x_k \) and chooses an action \( u_k \) based on this posterior. We observe the sensor’s action in noise as \( a_k \). Given knowledge of “our” state sequence \( \{x_k\} \) and the observed actions \( \{a_k\} \) taken by the adversary’s sensor, we focus on the following inter-related aspects:

1. **Inverse tracking and estimating the Adversary’s Sensor Gain.** Suppose the adversary radar observes our state in noise; updates its posterior distribution \( \pi_k \) of our state \( x_k \) using a Bayesian tracker, and then chooses an action \( u_k \) based on this posterior. Given knowledge of “our” state and sequence of noisy measurements \( \{a_k\} \) of the adversary’s actions \( \{u_k\} \), how can the adversary radar’s posterior distribution (random measure) be estimated? We will develop an inverse Bayesian filter for tracking the radar’s posterior belief of our state and present an example involving the Kalman filter where the inverse filtering problem admits a finite dimensional characterization.

A related question is: How to remotely estimate the adversary radar sensor’s conditional pdf of observation given the state when it is estimating us? This is important because it tells us how accurate the adversary’s sensor is; in the context of Figure 2 it tells us, how accurately the adversary tracks our drone. The data we have access to is our state (probe signal) sequence \( \{x_k\} \) and measurements of the adversary’s radar actions \( \{a_k\} \). Estimating the adversary’s sensor accuracy is non-trivial with several challenges. First, even though we know our state and state dynamics model (transition law), the adversary does not. The adversary needs to estimate our state and state transition law based on our trajectory; and we need to estimate the adversary’s estimate of our state transition law. Second, computing the MLE of the adversary’s sensor gain also requires inverse filtering.

2. **Revealed Preferences and Identifying Cognitive Radars.** Suppose the cognitive radar is a constrained utility maximizer that optimizes its actions \( u_k \) subject to physical level (Bayesian filter) constraints. How can we detect this utility maximization behavior? The actions \( u_k \) can be viewed as resources the radar adaptively allocates to maximize its utility. We consider two such resource allocation problems, namely:

   - **Beam Allocation:** The radar adaptively switches its beam while tracking multiple targets.
   - **Waveform Design:** The radar adaptively designs its waveform while ensuring the signal-to-interference-plus-noise ratio (SINR) exceeds a pre-defined threshold.

Nonparametric detection of utility maximization behavior is the central theme of revealed preference in microeconomics. A remarkable result is Afriat’s theorem: it provides a necessary and sufficient condition for a finite dataset to have originated from a utility maximizer. We will develop constrained set-valued utility estimation methods that account for signal processing constraints introduced by the Bayesian tracker for performing adaptive beam allocation and waveform design respectively.

B. Perspective

The adversarial dynamics considered in this paper fit naturally within the so called Dynamic Data and Information Processing (DDIP) paradigm. The adversary’s radar senses, adapts and learns from us. In turn we adapt, sense and learn from the adversary. So in simple terms we are modeling and analyzing the interaction of two DDIP systems. In this context, this paper has three major themes schematically shown in Figure 1: inverse filtering which is a Bayesian framework for interacting DDIP systems, inverse cognitive sensing which is a non-parametric approach for utility estimation for interacting DDIP systems, and interference design to confuse the adversary radar.

C. Organization

We conclude this section with a brief outline of the key results of the following sections, and their relevant to the sense, 1The terms SCNR and SINR are used interchangeably in the paper.
learn and adapt elements of the SLA paradigm of Figure 1.

**Sense:** In Sec. II we discuss inverse tracking techniques to estimate the sensor accuracy of an adversary radar. We focus mainly on the inverse Kalman filter and illustrate in carefully chosen examples how the adversary sensor’s accuracy can be estimated. This constitutes the ‘sensing’ aspect of the SLA paradigm.

**Learn:** In Sec. III we abstractly view the adversary radar as a cognitive decision maker that maximizes a utility function subject to physical resource constraints. Specifically, we show that if the cognitive radar optimizes its waveform to maintain its SINR above a threshold, then we can identify (and hence, ‘learn’) the utility function of the radar. The utility function provides deeper knowledge of the radar’s behavior and constitutes the ‘learn’ element of the SLA paradigm.

**Adapt:** In Sec. IV we consider a slightly modified setup where the radar chooses its waveform to maximize its SCNR. We show that by intelligently probing the radar with interference signals and observing the changes in the radar’s waveform, we can confuse the adversary’s radar by decreasing its SCNR. This adaptive signal processing algorithm is justified only if the ‘sense’ and ‘learn’ aspect of the SLA paradigm function properly, that is, the counter-adversarial system knows how the radar will react to changes in its environment.

Finally, we emphasize that the three main aspects of inverse tracking (sensing the estimate of the adversary), identifying utility maximization (learning the adversary’s utility function) and adaptive interference (adapting our response) are instances of the general paradigm of sense-learn-adapt in counter-adversarial systems. As mentioned above, our formulation deals with the interaction of two such sense-learn-adapt systems.

II. **Inverse Tracking and Estimating Adversary’s Sensor**

This section discusses inverse tracking in an adversarial system schematically illustrated in Figure 2. Our main ideas involve estimating the adversary’s estimate of us and estimating the adversary’s sensor conditional pdf of observation given the state.

A. **Background and Preliminary Work**

We start by formulating the problem which involves two entities; “us” and “adversary”. With \( k = 1, 2, \ldots \) denoting discrete time, the model has the following dynamics:

\[
\begin{align*}
    x_k & \sim P_{x_{k-1},x} = p(x|x_{k-1}), \quad x_0 \sim \pi_0 \\
    y_k & \sim B_{x_k,y} = p(y|x_k) \\
    \pi_k & = T(\pi_{k-1}, y_k) = p(x_k|y_{1:k}) \\
    a_k & \sim G_{\pi_{k-1},a} = p(a|\pi_k)
\end{align*}
\]

Let us explain the notation in (1):

- \( x_k \in \mathcal{X} \) is our Markovican state with transition kernel \( P_{x_{k-1},x} \), prior \( \pi_0 \) and state space \( \mathcal{X} \).
- \( y_k \) is the adversary’s noisy observation of our state \( x_k \) with conditional pdf of observation given the state \( B_{x_k,y} \).
- \( \pi_k \) is the adversary’s belief (posterior) of our state \( x_k \) where \( y_{1:k} \) denotes the observation sequence \( y_1, \ldots, y_k \). The operator \( T \) in (1) is the classical Bayesian optimal filter that computes the posterior belief of the state given observation \( y \) and current belief \( \pi \).

\[
T(\pi, y) = \text{vec} \left( \frac{B_{x,y} \int_{\mathcal{X}} P_{\zeta,x} \pi(\zeta) d\zeta}{\int_{\mathcal{X}} B_{x,y} \int_{\mathcal{X}} P_{\zeta,x} \pi(\zeta) d\zeta} \right), \quad x \in \mathcal{X}
\]

Let \( \Pi \) denote the space of all such beliefs. When the state space \( \mathcal{X} \) is finite, then \( \Pi \) is the unit \( X - 1 \) dimensional simplex of \( X \)-dimensional probability mass functions.

- \( a_k \) denotes our measurement of the adversary’s action based on its current belief \( \pi_k \). The adversary chooses an action \( u_k \) as a (possibly) stochastic function of \( \pi_k \) and we obtain a noisy measurement of \( u_k \) as \( a_k \). We encode this as \( G_{\pi_k,a_k} \), the conditional probability of observing action \( a_k \) given the adversary’s belief \( \pi_k \). Although not explicitly shown, \( G \) abstracts two stochastic maps: 1) the map from the adversary’s belief \( \pi_k \) to its action \( u_k \), and 2) the map from the adversary’s action \( u_k \) to our noisy measurement \( a_k \) of this action.

**Aim:** Referring to model (1) and Figure 2 we address the following questions in this section:
Fig. 2: Schematic of Adversarial Inference Problem. Our side is a drone/UA V or electromagnetic signal that probes the adversary’s cognitive radar system. Based on the action $a_k$ of the adversary, our side computes the estimate of the adversary’s estimate of our state $x_k$ using the inverse Kalman filter outlined in Sec. II-B.

1) How to estimate the adversary’s belief given measurements of its actions (which are based on its filtered estimate of our state)? In other words, assuming probability distributions $P, B, G$ are known, we aim to estimate the adversary’s belief $π_k$ at each time $k$, by computing posterior $p(π_k | π_0, x_{0:k}, a_{1:k})$.

2) How to estimate the adversary’s observation kernel $B$, i.e. its sensor gain? This tells us how accurate the adversary’s sensor is.

From a practical point of view, estimating the adversary’s belief and sensor parameters allows us to calibrate its accuracy and predict (in a Bayesian sense) future actions of the adversary.

Related Works. In recent works [34], [35], [33], the mapping from belief $π$ to adversary’s action $a$ was assumed deterministic. In comparison, our proposed research here assumes a probabilistic map between $π$ and $a$ and we develop Bayesian filtering algorithms for estimating the posterior along with MLE (Maximum Likelihood Estimation) algorithms for estimating the underlying model. Estimating/reconstructing the posterior given decisions based on the posterior is studied in [31] and game-theoretic generalizations [4]. There are strong parallels between inverse filtering and Bayesian social learning [10], [24], [23], [22]; the key difference is that social learning aims to estimate the underlying state given noisy posteriors, whereas our aim is to estimate the posterior given noisy measurements of the posterior and the underlying state. Recently, [21] used cascaded Kalman filters for LQG control over communication channels. This work motivates the design of the function $ φ $ in [3] below that maps the adversary’s belief to its action; see also footnote 5. Finally, in [11], the authors investigate the inverse problem of trajectory identification based on target measurements, where the target is assumed to follow a constant velocity model.

**B. Inverse Tracking Algorithms**

How to estimate the adversary’s posterior distribution of us?

---

As mentioned in footnote 6, this assumption simplifies the setup; otherwise we need to estimate the adversary’s estimate of us, which makes our task substantially complex.

Here we discuss inverse tracking for the model [11]. Define the posterior distribution $ρ_k(π_k) = p(π_k | a_{1:k}, x_{0:k})$ of the adversary’s posterior distribution given our state sequence $x_{0:k}$ and actions $a_{1:k}$. Note that the posterior $ρ_k(·)$ is a random measure since it is a posterior distribution of the adversary’s posterior distribution (belief) $π_k$. By using a discrete time version of Girsanov’s theorem and appropriate change of measure [15] (or a careful application of Bayes rule) we can derive the following functional recursion for $ρ_k$ (see [29])

$$
ρ_{k+1}(π) = \frac{G_{π,a_{k+1}} \int_{π} B_{π_{k+1},y_{k+1}} ρ_k(π_k) dπ_k}{\int_{π} G_{π,a_{k+1}} \int_{π} B_{π_{k+1},y_{k+1}} ρ_k(π_k) dπ_k} \quad (3)
$$

Here $y_{π_{k+1}}$ is the observation such that $π = T(π_k, y)$ where $T$ is the adversary’s filter [2]. We call $3$ the optimal inverse filter since it yields the Bayesian posterior of the adversary’s belief given our state and noisy measurements of the adversary’s actions.

**Example: Inverse Kalman Filter**

We consider a special case of (3) where the inverse filtering problem admits a finite dimensional characterization in terms of the Kalman filter. Consider a linear Gaussian state space model

$$
\begin{align*}
x_{k+1} &= Ax_k + w_k, \quad x_0 \sim π_0 \\
y_k &= Cx_k + v_k
\end{align*}
$$

where $x_k \in \mathcal{X}$ is “our” state with initial density $π_0 \sim \mathcal{N}(\hat{x}_0, \Sigma_0)$, $y_k \in \mathcal{Y} = \mathbb{R}^Y$ denotes the adversary’s observations, $w_k \sim \mathcal{N}(0, Q_k)$, $v_k \sim \mathcal{N}(0, R_k)$ and $\{w_k\}$, $\{v_k\}$ are mutually independent i.i.d. processes. Here, $\mathcal{N}(\mu, C)$ denotes the normal distribution with mean $\mu$ and covariance matrix $C$.

Based on observations $y_{1:k}$, the adversary computes the belief $π_k = \mathcal{N}(\hat{x}_k, Σ_k)$ where $\hat{x}_k$ is the conditional mean state
estimate and $\Sigma_k$ is the covariance; these are computed via the classical Kalman filter equations:

$$
\Sigma_{k+1|k} = A\Sigma_k A^T + Q_k
$$

$$
S_{k+1} = C\Sigma_{k+1|k} C^T + R_k
$$

$$
\hat{x}_{k+1} = A\hat{x}_k + \Sigma_{k+1|k} C^T (y_{k+1} - CA\hat{x}_k)
$$

$$
\Sigma_{k+1} = \Sigma_{k+1|k} - \Sigma_{k+1|k} C^T S_{k+1}^{-1} C\Sigma_{k+1|k}
$$

(7)

The adversary then chooses its action as $a_k = \phi(\Sigma_k) \hat{x}_k$ for some pre-specified function $\phi$. We measure the adversary’s action as

$$
a_k = \phi(\Sigma_k) \hat{x}_k + \epsilon_k, \quad \epsilon_k \sim \text{iid } N(0, \sigma^2_k)
$$

(8)

The Kalman covariance $\Sigma_k$ is deterministic and fully determined by the model parameters. Hence, we only need to estimate $\hat{x}_k$ at each time $k$ given $a_{1:k}, x_{0:k}$ to estimate the belief $\pi_k = N(\hat{x}_k, \Sigma_k)$. Substituting $\hat{x}_k = \phi(\Sigma_k) \hat{x}_k$ for $y_{k+1}$ in (7), we see that (7), (8) constitute a linear Gaussian system with unobserved state $\hat{x}_k$, observations $a_k$, and known exogenous input $x_k$:

$$
\hat{x}_{k+1} = (I - \psi_k(1)C)A\hat{x}_k + \psi_k(1)C x_{k+1} + \psi_k(1+C)x_{k+1}
$$

$$
a_k = \phi(\Sigma_k) \hat{x}_k + \epsilon_k, \quad \epsilon_k \sim \text{iid } N(0, \sigma^2_k)
$$

(9)

where $\psi_k(1) = \Sigma_{k+1|k} C^T S_{k+1}^{-1}$.

$\psi_{k+1}$ is called the Kalman gain and $I$ is the identity matrix.

To summarize, our filtered estimate of the adversary’s filtered estimate $\hat{x}_k$ given measurements $a_{1:k}, x_{0:k}$ is achieved by running “our” Kalman filter on the linear Gaussian state space model (9), where $\hat{x}_k, \psi_k, \Sigma_k$ in (9) are generated by the adversary’s Kalman filter. Therefore, our Kalman filter uses the parameters

$$
\tilde{A}_k = (I - \psi_{k+1} C)A, \quad \tilde{F}_k = \psi_{k+1} C, \quad \tilde{C}_k = \phi(\Sigma_k),
$$

$$
\tilde{Q}_k = \psi_{k+1} \psi_{k+1} + \sigma^2_k
$$

(10)

The equations of our inverse Kalman filter for estimating the adversary’s estimate of our state are:

$$
\Sigma_{k+1|k} = \tilde{A}_k \Sigma_k \tilde{A}_k^T + \tilde{Q}_k
$$

$$
S_{k+1} = \tilde{C}_k \Sigma_{k+1|k} \tilde{C}_k^T + \tilde{R}_k
$$

$$
\hat{x}_{k+1} = \tilde{A}_k \hat{x}_k + \Sigma_{k+1|k} \tilde{C}_k^T (y_{k+1} - \tilde{C}_k \hat{x}_k)
$$

$$
\Sigma_{k+1} = \Sigma_{k+1|k} - \Sigma_{k+1|k} \tilde{C}_k^T S_{k+1}^{-1} \tilde{C}_k \Sigma_{k+1|k}
$$

(11)

Note $\hat{x}_k$ and $\Sigma_k$ denote our conditional mean estimate and covariance of the adversary’s conditional mean $\hat{x}_k$. The computational cost of the inverse Kalman filter is identical to the classical Kalman filter, namely $O(N^2)$ computations at each time step.

**Remarks:**

1) As discussed in [29], inverse Hidden Markov model (HMM) filters and inverse particle filters can also be derived to solve the inverse tracking problem. For example, the inverse HMM filter deals with the case when $\pi_k$ is computed via an HMM filter and the estimates of the HMM filter are observed in noise. In this case the inverse filter has a computational cost that grows exponentially with the size of the observation alphabet.

2) A general approximate solution for (3) involves sequential Markov chain Monte-Carlo (particle filtering). In particle filtering, cases where it is possible to sample from the so called optimal importance function are of significant interest [36], [31]. In inverse filtering, [29] shows that the optimal importance function can be determined explicitly due to the structure of the inverse filtering problem. Specifically, in our case, the “optimal” importance density is $\pi^* = p(\pi_k, y_k | \pi_{k-1}, y_{k-1}, x_k, a_k)$. Note that in our case

$$
\pi^* = \frac{p(\pi_k | \pi_{k-1}, y_k) p(y_k | x_k, a_k)}{\delta(\pi_k - T(\pi_{k-1}, y_k)) p(y_k | x_k)}
$$

(12)

is straightforward to sample from. There has been a substantial amount of recent research in finite sample concentration bounds for the particle filter [13], [31]. In future work such results can be used to evaluate the sample complexity of the inverse particle filter.

**C. Estimating the Adversary’s Sensor Gain**

In this section, we discuss how to estimate the adversary’s sensor observation kernel $B$ in (1) which quantifies the accuracy of the adversary’s sensors. We assume that $B$ is parameterized by an $M$-dimensional vector $\theta \in \Theta$ where $\Theta$ is a compact subset of $\mathbb{R}^M$. Denote the parameterized observation kernel as $B^\theta$. Assume that both us and the adversary know $P$ (state transition kernel and $G$ (probabilistic map from adversary’s belief to its action). As mentioned earlier, the stochastic kernel $G$ in (1) is a composition of two stochastic kernels: 1) the map from the adversary’s belief $\pi_k$ to its action $u_k$, and 2) the map from the adversary’s action $u_k$ to our measurement $a_k$ of this action.

Then, given our state sequence $x_{0:N}$ and adversary’s action sequence $u_{1:N}$, our aim is to compute the maximum likelihood estimate (MLE) of $\theta$. That is, with $L_N(\theta)$ denoting the log-likelihood, the aim is to compute

$$
\theta^* = \arg\max_{\theta \in \Theta} L_N(\theta), \quad L_N(\theta) = \log p(x_{0:N}, a_{1:N} | \theta)
$$

(13)

4In general the action $a_k$ is a function of the state estimate and covariance matrix. Choosing the action $a_k$ as a linear function of the state estimate is for convenience and motivates the inverse Kalman filter discussed below. Moreover it mimics linear quadratic Gaussian (LQG) control where the feedback is a linear function of the state estimate. In LQG control, the feedback gain is obtained from backward Riccati equation. Here we weigh by a nonlinear function of the Kalman covariance matrix (forward Riccati equation) to allow for incorporating uncertainty of the estimate into the choice of the action $a_k$.

5Otherwise the adversary estimates $\pi$ as $\hat{\pi}$ and we need to estimate the adversary’s estimates of us, namely $\hat{\pi}$. This makes the estimation task substantially more complex. In future work we will examine conditions under which the MLE in this setup is identifiable and consistent.
The likelihood can be evaluated from the un-normalized inverse filtering recursion \(^3\)

\[
L_N(\theta) = \log \int_{\Pi} q^\theta_N(\pi) d\pi,
\]

\[
q^\theta_{t+1}(\pi) = G_{\pi,a_{t+1}} \int_{\Pi} B_{\pi_{t+1},y^\theta_{t+1}} q^\theta_t(\pi_t) d\pi_t,
\]

initialized by setting \(q^\theta_0(\pi_0) = \pi_0\). Here \(y^\theta_{t+1}\) is the observation such that \(\pi = T(\pi_t, y)\) where \(T\) is the adversary’s filter \(^2\) with variable \(B\) parametrized by \(\theta\). Given (14), a local stationary point of the likelihood can be computed using a general purpose numerical optimization algorithm.

\[\frac{\partial^2 L_N(\theta)}{\partial \theta^2} \bigg|_{\theta = \theta^0}\]

\[\frac{\partial^2 L_N(\theta)}{\partial \theta^2} \bigg|_{\theta = \theta^0}\]

D. Example. Estimating Adversary’s Gain in Linear Gaussian case

The aim of this section is to provide insight into the nature of estimating the adversary’s sensor gain via numerical examples. Consider the setup in Sec.II-B where our dynamics are linear Gaussian and the adversary observes our state linearly in Gaussian noise \(^4\). The adversary estimates our state using a Kalman filter, and we estimate the adversary’s estimate using the inverse Kalman filter \(^9\). Using \(^9\), (10), the log-likelihood for the adversary’s observation gain matrix \(\theta = C\) based on our measurements is \(^4\)

\[
L_N(\theta) = \text{const} - \frac{1}{2} \sum_{k=1}^{N} \log |S^\theta_k| - \frac{1}{2} \sum_{k=1}^{N} \tau_k (S^\theta_k)^{-1} \tau_k
\]

\[
\tau_k = a_k - C^\theta_k A^\theta_{k-1} \hat{x}_{k-1} - F^\theta_{k-1} x_{k-1}
\]

where \(\tau_k\) are the innovations of the inverse Kalman filter \(^11\). In \(^15\), our state \(x_{k-1}\) is known to us and therefore is a known exogenous input. Also note from \(^10\) that \(\hat{A}_k, \hat{F}_k\) are explicit functions of \(C\), while \(\hat{C}_k\) and \(\hat{Q}_k\) depend on \(C\) via the adversary’s Kalman filter.

The log-likelihood for the adversary’s observation gain matrix \(\theta = C\) can be evaluated using \(^15\). To provide insight, Figure \(\ref{fig:3}\) displays the log-likelihood versus adversary’s gain matrix \(C\) in the scalar case for 1000 equally spaced data points over the interval \(C = (0,10]\). The four sub-figures correspond to true values \(C^\theta = 2.5, 3.5\) of \(C\), respectively.

Each sub-figure in Figure \(\ref{fig:3}\) has two plots. The plot in red is the log-likelihood of \(\theta = C\) evaluated based on the adversary’s observations using the standard Kalman filter. (This is the classical log-likelihood of the observation gain of a Gaussian state space model.) The plot in blue is the log-likelihood of \(\theta = C\) computed using our measurements of the adversary’s action using the inverse Kalman filter (where the adversary first estimates our state using a Kalman filter) - we call this the inverse case.

Figure \(\ref{fig:3}\) shows that the log-likelihood in the inverse case (blue plots) has a less pronounced maximum compared to the standard case (red plots). Therefore, numerical algorithms for computing the MLE of the adversary’s gain \(C^\theta\) using our observations of the adversary’s actions (via the inverse Kalman filter) will converge much more slowly than the classical MLE (based on the adversary’s observations). This is intuitive since our estimate of the adversary’s parameter is based on the adversary’s estimate of our state and so has more noise.

Sensitivity of MLE. It is important to evaluate the sensitivity of the MLE of \(C\) with covariance matrices \(Q_k, R_k\) in the state space model \(^4\). For example, the sensitivity w.r.t \(Q_k\) reveals how sensitive the MLE is w.r.t our maneuver covariance since from \(^4\), \(Q_k\) determines our maneuvers. Our sensitivity analysis evaluates the variation of the second derivative of the log-likelihood of \(C\) computed at the true gain \(C^\theta\) to small changes in \(Q_k\) and \(R_k\). Table \(\ref{table1}\) displays our sensitivity results w.r.t the scalar setup of Figure \(\ref{fig:3}\) Table \(\ref{table1}\) comprises two sensitivity values.

\[
\eta_Q = \frac{\partial}{\partial Q_k} \left( \frac{\partial^2 L_N(\theta)}{\partial \theta^2} \right) \bigg|_{\theta = C^\theta}
\]

and

\[
\eta_R = \frac{\partial}{\partial R_k} \left( \frac{\partial^2 L_N(\theta)}{\partial \theta^2} \right) \bigg|_{\theta = C^\theta},
\]

evaluated for both the inverse case (that uses the inverse Kalman filter \(^15\)) and the classic case where the adversary’s observations are known. \(\eta(\cdot)\) measures the change in the sharpness of the log-likelihood plot around the true sensor gain wrt change in the noise covariance. Note that the experimental setup of Figure \(\ref{fig:3}\) assumes the covariances \(Q_k, R_k\) are constant over time index \(k\), hence we drop the subscript in the LHS of \(^16\).
The previous section was concerned with estimating the adversary’s posterior belief and sensor accuracy. This section discusses detecting utility maximization behavior and estimating the adversary’s utility function in the context of cognitive radars. As described in the introduction, inverse tracking, identifying utility maximization and designing interference to confuse the radar constitute our adversarial setting.

Cognitive radars \( \textit{19} \) use the perception-action cycle of cognition to sense the environment and learn from it relevant information about the target and the environment. The cognitive radars then tune the radar sensor to optimally satisfy their mission objectives. Based on its tracked estimates, the cognitive radar adaptively optimizes its waveform, aperture, dwell time and revisit rate. In other words, a cognitive radar is a constrained utility maximizer.

This section is motivated by the next logical step, namely, \textit{identifying a cognitive radar} from the actions of the radar. The adversary cognitive radar observes our state in noise; it uses a Bayesian estimator (target tracking algorithm) to update its posterior distribution of our state and then chooses an action based on this posterior. From the intercepted emissions of an adversary’s radar, we address the following question: Are the adversary sensor’s actions consistent with optimizing a monotone utility function (i.e., is the cognitive sensor behavior rational in an economics sense)? If so how can we estimate a utility function of the adversary’s cognitive sensor that is consistent with its actions? The main synthesis/analysis framework we will use is that of revealed preferences \( \textit{40}, \textit{16}, \textit{14} \) from microeconomics which aims to determine preferences by observing choices. The results presented below are developed in detail in the recent work \( \textit{25} \); however, the SINR constraint formulation in Sec. III-C for detecting waveform optimization is new. Related work that develops adversarial inference strategies at a higher level of abstraction than tracking level (like the Bayesian filter level in Sec.II) includes \( \textit{30} \). \( \textit{30} \) places counter unmanned autonomous systems at a level of abstraction above the physical sensors/actuators/weapons and datalink layers; and below the human controller layer.

### A. Background. Revealed Preferences and Afriat’s Theorem

Non-parametric detection of utility maximization behavior is studied in the area of revealed preferences in microeconomics. A key result is the following:

\textbf{Definition III.1} \( \textit{11}, \textit{2} \). A system is a utility maximizer if for every probe \( \alpha_n \in \mathbb{R}_+^m \), the response \( \beta_n \in \mathbb{R}^m \) satisfies

\[
\beta_n \in \text{argmax}_{\alpha_n'} U(\beta) \quad \text{for } \alpha_n' \beta \leq 1
\]

where \( U(\beta) \) is a monotone utility function.

In economics, \( \alpha_n \) is the price vector and \( \beta_n \) the consumption vector. Then \( \alpha_n' \beta \leq 1 \) is a natural budget constraint\( \textit{6} \) for

\begin{table}
\begin{tabular}{|c|c|c|}
\hline
\( C^\theta \) & Classic & Inverse \\
\hline
\hline
\( \eta Q \) & 2.5 & -43.45 & -6.46 \\
\hline
3.5 & -25.16 & -2.77 \\
\hline
\hline
\( \eta R \) & 2.5 & -189.39 & -50.04 \\
\hline
3.5 & -65.27 & -30.55 \\
\hline
\end{tabular}
\caption{Comparison of sensitivity values \( \textit{16} \) for log-likelihood of \( C \) wrt noise covariances \( Q_k \), \( R_k \) \( \textit{4} \) - classical model vs inverse Kalman filter model.}
\end{table}

### III. Identifying Utility Maximization in a Cognitive Radar

Table I shows that the second derivative of the log-likelihood is more sensitive (in magnitude) to the adversary’s observation covariance \( R_k \) than the maneuver covariance \( Q_k \). Also, it is observed that the sensitivity of the log-likelihood is higher for lower sensor gain \( C^\theta \). This observation is consistent with intuition since a larger gain \( C \) implies a larger SNR (signal-to-noise ratio) of the observation \( y \) which intuitively suggests the estimate of \( C \) is more robust to changes in maneuver covariance and observation noise covariance.

\textbf{Cramér-Rao (CR) bounds.} It is instructive to compare the CR bounds for MLE of \( C \) for the classic model versus that of the inverse Kalman filter model. Table II displays the CR bounds (reciprocal of expected Fisher information) for the four examples considered above evaluated using via the algorithm in \( \textit{9} \). It shows that the covariance lower bound for the inverse case is substantially higher than that for the classic case. This is consistent with the intuition that estimating the adversary’s parameter based on its actions (which is based on its estimate of us) is more difficult than directly estimating \( C \) in a classical state space model based on the adversary’s observations of our state that determines its actions.

\textbf{Consistency of MLE.} The above example (Figure \( \textit{3} \)) shows that the likelihood surface of \( L_N(\theta) = \log p(x_{0:N}, a_{1:N} | \theta) \) is flat and hence computing the MLE numerically can be difficult. Even in the case when we observe the adversary’s actions perfectly, \( \textit{34} \) shows that non-trivial observability conditions need to be imposed on the system parameters.

For the linear Gaussian case where we observe the adversary’s Kalman filter in noise, strong consistency of the MLE for the adversary’s gain matrix \( C \) can be established fairly straightforwardly. Specifically, if we assume that state matrix \( A \) is stable, and the state space model is an identifiable minimal realization, then the adversary’s Kalman filter variables converge to steady state values geometrically fast in \( k \) \( \textit{4} \) implying that asymptotically the inverse Kalman filter system is stable linear time invariant. Then, the MLE \( \theta^* \) for the adversary’s observation matrix \( C \) is unique and strongly consistent \( \textit{6} \).
a consumer with 1 dollar. Given a dataset of price and consumption vectors, the aim is to determine if the consumer is a utility maximizer (rational) in the sense of [17].

The key result is the following theorem due to Afriat [14], [2], [1], [40], [38].

**Theorem III.2 (Afriat’s Theorem)**. Given a data set \( D = \{(\alpha_n, \beta_n), n \in \{1, 2, \ldots, N\}\} \), the following statements are equivalent:

1) The system is a utility maximizer and there exists a monotonically increasing, continuous, and concave utility function that satisfies (17).

2) There exist positive reals \( u_t, \lambda_t > 0, t = 1, 2, \ldots, N, such that the following inequalities hold:

\[
u_s - u_t - \lambda_t \alpha'_t (\beta_s - \beta_t) \leq 0 \forall t, s \in \{1, 2, \ldots, N\}.
\]  

The monotone, concave utility function \( U(\beta) = \min_{t \in \{1, 2, \ldots, N\}} \{u_t + \lambda_t \alpha'_t (\beta - \beta_t)\}\) given by

\[
U(\beta) = \sum_{t \in \{1, 2, \ldots, N\}} \left\{ u_t + \lambda_t \alpha'_t (\beta - \beta_t) \right\}
\]  

constructed using \( u_t \) and \( \lambda_t \) defined in (18) rationalizes the dataset by satisfying (17).

3) The data set \( D \) satisfies the Generalized Axiom of Revealed Preference (GARP) also called cyclic consistency, namely for any \( t \leq N \), \( \alpha'_t \beta_t \geq \alpha'_t \beta_{t+1} \) \( \forall t \leq k-1 \implies \alpha'_k \beta_k \leq \alpha'_k \beta_{i-1} \).

Afriat’s theorem tests for economics-based rationality; its remarkable property is that it gives a necessary and sufficient condition for a system to be a utility maximizer based on the system’s input-output response. Although GARP in statement 4 in Theorem III.2 is not critical to the developments in this paper, it is of high significance in micro-economic theory and is stated here for completeness. The feasibility of the set of inequalities (18) can be checked using a linear programming solver; alternatively GARP can be checked using Warshall’s algorithm with \( O(N^3) \) computations.

The recovered utility using (19) is not unique; indeed any positive monotone increasing transformation of (19) also satisfies Afriat’s Theorem; that is, the utility function constructed is ordinal. This is the reason why the budget constraint \( \alpha'_t \beta_k \leq 1 \) is without generality; it can be scaled by an arbitrary positive constant and Theorem III.2 still holds. In signal processing terminology, Afriat’s Theorem can be viewed as set-valued system identification of an argmax system; set-valued since (19) yields a set of utility functions that rationalize the finite dataset \( D \).

**B. Beam Allocation: Revealed Preference Test**

This section constructs a test to identify a cognitive radar that switches its beam adaptively between targets. This example is based on [25] and is presented here for completeness. The setup is schematically shown in Figure 4. We view each component \( i \) of the probe signal \( \alpha_n(i) \) as the trace of the information matrix (inverse covariance) of target \( i \). We use the trace of the information matrix of each target in our probe signal – this allows us to consider multiple targets. Since the adversarial radar is assumed to be stationary, the target covariance used to define the probe for the radar is indeed the maneuver covariance.

The setup in Figure 4 differs significantly from the setup of Figure 2 considered in the previous section. First, the adversary in the current setup is an economically rational agent. In Figure 2 the adversary is only specified at a lower level of abstraction as using a Bayesian filter to track our maneuvers. Second, this section abstracts adversary’s actions at the fast time scale indexed by \( k \) by an appropriately defined response at the slow time scale indexed by \( n \). The previous section’s analysis was confined to the actions generated only at the fast time scale \( k \). Lastly, Figure 4 assumes the abstracted response \( \beta_k \) of the adversary is measured accurately by us as opposed to a noisy measurement \( a_k \) of the adversary’s action \( u_k \) in Figure 2.

Suppose a radar adaptively switches its beam between \( m \) targets where these \( m \) targets are controlled by us. As in (4), on the fast time scale indexed by \( k \), each target \( i \) has linear Gaussian dynamics and the adversary radar obtains linear Gaussian measurements:

\[
x_{k+1} = A x_k + w_k, \quad x_0 \sim \pi_0
\]

\[
y_{ik} = C x_k + v_{ik}, \quad i = 1, 2, \ldots, m
\]  

Here \( w_k \sim N(0, Q_n(i)) \), \( v_{ik} \sim N(0, R_n(i)) \). Recall from Figure 4 that \( n \) indexes the epoch (slow time scale) and \( k \)
indexes the fast time scale within the epoch. We assume that both $Q_n(i)$ and $R_n(i)$ are known to us and the adversary.

The adversary’s radar tracks our $m$ targets using Kalman filter trackers. The fraction of time the radar allocates to each target $i$ in epoch $n$ is $\beta_n(i)$. The price the radar pays for each target $i$ at the beginning of epoch $n$ is the trace of the predicted accuracy of target $i$. Recall that this is the trace of the inverse of the predicted covariance at epoch $n$ using the Kalman predictor

$$\alpha_n(i) = \text{Tr}(\Sigma_{n|n-1}(i)^{-1}), \quad i = 1, \ldots, m \quad (21)$$

The predicted covariance $\Sigma_{n|n-1}(i)$ is a deterministic function of the maneuver covariance $Q_n(i)$ of target $i$. We abstract the target’s covariance by its trace denoted by $\alpha_n(i)$. Note also that the observation noise covariance $R_n(i)$ depends on the adversary’s radar response $\beta_n(i)$, i.e., the fraction of time allocated to target $i$. We assume that each target $i$ can estimate the fraction of time $\beta_n(i)$ the adversary’s radar allocates to it using a radar detector.

Given the time series $\alpha_n, \beta_n, n = 1, \ldots, N$, our aim is to detect if the adversary’s radar is cognitive. We assume that a cognitive radar optimizes its beam allocation as the following constrained optimization:

$$\beta_n = \arg\max_\beta U(\beta) \quad \text{s.t.} \quad \beta' \alpha_n \leq p_*,$$  

where $U(\cdot)$ is the adversary radar’s utility function (unknown to us) and $p_* \in \mathbb{R}_+$ is a pre-specified average accuracy of all $m$ targets.

The economics-based rationale for the budget constraint is natural: For targets that are cheaper (lower accuracy targets), the radar has incentive to devote more time $\beta_n(i)$. However, given its resource constraints, the radar can achieve at most an average accuracy of $p_*$ over all targets.

The setup in (22) is directly amenable to Afriat’s Theorem [III.2]. Thus (18) can be used to test if the radar satisfies utility maximization in its beam scheduling (22) and also estimate the set of utility functions (19). Furthermore (as in Afriat’s theorem) since the utility is ordinal, $p_*$ can be chosen as 1 without loss of generality (and therefore does not need to be known by us).

C. Waveform adaptation: Revealed Preference Test for Non-linear budgets

In the previous subsection, we tested for cognitive optimizes its waveform based on the SINR of the target measurement. By using a generalization of Afriat’s theorem (Theorem [III.2]) to non-linear budgets, our main aim is to detect if a radar intelligently chooses its waveform to maximize an underlying utility subject to signal processing constraints. Our setup below differs from [25] since we introduce the SINR as a non-linear budget constraint; in comparison [25] uses a spectral budget constraint.

We start by briefly outlining the generalized utility maximization setup.

**Definition III.3 (16).** A system is a generalized utility maximizer if for every probe $\alpha_n \in \mathbb{R}_+^m$, the response $\beta_n \in \mathbb{R}_+^m$ satisfies

$$\beta_n \in \text{argmax}_\beta U(\beta) \quad (23)$$

where $U(\beta)$ is a monotone utility function and $g_n(\cdot)$ is monotonically increasing in $\beta$.

The above utility maximization model generalizes Definition [III.1] since the budget constraint $g_n(\beta) \leq 0$ can accommodate non-linear budgets and includes the linear budget constraint of Definition [III.1] as a special case. The result below provides an explicit test for a system that maximizes utility in the sense of Definition [III.3] and constructs a set of utility functions that rationalizes the decisions $\beta_n$ of the utility maximizer.

**Theorem III.4** (Test for rationality with non-linear budget [16]). Let $B_n = \{\beta \in \mathbb{R}_+^m \mid g_n(\beta) \leq 0\}$ with $g_n : \mathbb{R}_+^m \to \mathbb{R}$ an increasing, continuous function and $g_n(\beta_n) = 0$ for $n = 1, \ldots, N$. Then the following conditions are equivalent:

1) There exists a monotone continuous utility function $U$ that rationalizes the data set $\{\beta_n, B_n\}, n = 1, \ldots, N$. That is

$$\beta_n = \text{argmax}_\beta U(\beta), \quad g_n(\beta) \leq 0$$

2) There exist positive reals $u_t, \lambda_t > 0, \ t = 1, 2, \ldots, N$, such that the following inequalities hold.

$$u_s - u_t - \lambda_t g_t(\beta_s) \leq 0 \ \forall t, s \in \{1, 2, \ldots, N\} \quad (24)$$

The monotone, concave utility function given by

$$U(\beta) = \min_{t \in \{1, \ldots, N\}} \{u_t + \lambda_t g_t(\beta)\} \quad (25)$$

constructed using $u_s$ and $\lambda_t$ defined in (24) rationalizes the data set by satisfying (24).

3) The data set $\{\beta_n, B_n\}, n = 1, \ldots, N$ satisfies GARP:

$$g_n(\beta_j) \leq g_n(\beta_i) \implies g_j(\beta_i) \geq 0 \quad (26)$$

Like Afriat’s theorem, the above result provides a necessary and sufficient condition for a system to be a utility maximizer based on the system’s input-output response. In spite of a non-linear budget constraint, it can be easily verified that the constructed utility function $U(\beta)$ is ordinal since any positive monotone increasing transformation of (25) satisfies the GARP inequalities (26).

We now justify the non-linear budget constraint in (23) in the context of the cognitive radar by formulating an optimization problem the radar solves equivalent to Definition [III.3].
Suppose we observe the radar over \( n = 1, 2, \ldots, N \) time epochs (slow varying time scale). At the \( n \)th epoch, we probe the radar with an interference vector \( \alpha_n \in \mathbb{R}^M \). The radar responds with waveform \( \beta_n \in \mathbb{R}^M \). We assume the chosen waveform \( \beta_n \) maximizes the radar's underlying utility function while ensuring the radar's SINR exceeds a particular threshold \( \delta > 0 \), where the SINR of the radar given probe \( \alpha \) and response \( \beta \) is defined as

\[
\text{SINR}(\alpha, \beta) = \frac{\beta^T Q \beta}{\beta^T P(\alpha) \beta + \gamma}.
\]

In (27), the radar's signal power (numerator) and interference power (first term in denominator) are assumed to be quadratic forms of \( Q, P(\alpha) \) respectively, where \( Q, P(\alpha) \in \mathbb{R}^{M \times M} \) are positive definite matrices known to us. The term \( \gamma > 0 \) is the noise power. The SINR definition in (27) is a more general formulation of the SCNR of a cognitive radar derived in Sec. IV using clutter response models. The matrices \( Q, P(\alpha) \) are analogous to the covariance of the channel impulse response matrices \( H_t(\cdot) \) and \( H_p(\cdot) \) corresponding to the target and clutter (external interference) channels, respectively (see Sec. IV-A for a discussion).

Having defined the SINR above in (27), we now formalize the radar's response \( \beta_n \) given probe \( \alpha_n \), \( n = 1, 2, \ldots \) as the solution of the following constrained optimization problem.

\[
\beta_n \in \operatorname{argmax}_\beta U(\beta) \\
\text{s.t.} \quad \text{SINR}(\alpha_n, \beta) \geq \delta
\]

Clearly, the above setup falls under the non-linear utility maximization setup in Definition 

\[
\text{Theorem III.5. Suppose that the adversary radar uses the SINR constraint (28). Then } g_n(\beta) = \delta - \text{SIR}(\alpha_n, \beta) \text{ is monotonically increasing in } \beta \text{ if the following two conditions hold.}
\]

1) The matrix \( Q \) is a diagonal matrix with off-diagonal elements equal to zero.
2) The matrix \( \left( \frac{c_{P(\alpha_n)}}{d_Q} P(\alpha_n) - Q \right) \) is component-wise less than 0 for all \( n \in \{1, 2, \ldots, N\} \), where \( c_{P(\alpha_n)} > 0 \) and \( d_Q > 0 \) denote the smallest and largest eigenvalues of \( P(\alpha_n) \) and \( Q \) respectively.

IV. DESIGNING SMART INTERFERENCE TO CONFUSE COGNITIVE RADAR

This section discusses how we can engineer (design) external interference (a probing signal) at the physical layer level to confuse a cognitive radar. By abstracting the probing signal to a channel in the frequency domain, our objective is to minimize the signal power of the interference generated by us while ensuring the SCNR of the radar does not exceed a pre-defined threshold. The setup is schematically shown in Figure 3. Note that the level of abstraction used in this section is at the Wiener filter pulse/waveform level; whereas the previous two sections were at the systems level (which uses the utility maximization framework) and tracker level (which uses the Kalman filter formalism), respectively. This is consistent with the design theme of sense globally (high level of abstraction) and act locally (lower level of abstraction).

As can be seen in the SCNR expression (33), the interference signal power manifests as additional clutter perceived by the radar in the denominator thus forcing the SCNR to go down. The radar then re-designs its waveform to maximize its SCNR given our interference signal. We observe the adversarial radar’s chosen waveform in noise. Our task can thus be re-formulated as choosing the interference signal with minimal power while ensuring that with probability at least \( 1 - \epsilon \), the optimized SCNR lies below a threshold level \( \Delta \). Here, \( \epsilon \) and \( \Delta \) are user-defined parameters. This approach closely follows the formulation in Sec. III-C where the cognitive radar chooses the optimal waveform while ensuring the SINR exceeds a threshold value. Further, the SCNR of the adversary’s radar defined in (24) below can be interpreted as a monotone function of the radar’s utility function in the abstracted setup of Sec. III-C since in complete analogy to the utility maximization model of Sec. III-C this section assumes the radar maximizes its SCNR in the presence of smart interference signals (probes).

A. Interference Signal Model

We first characterize how a cognitive radar optimally chooses its waveform based on its perceived interference. The radar's objective is to choose the optimal waveform that maximizes its signal-to-interference-plus-noise (SINR) ratio.

Suppose we observe the adversarial radar over \( l = 1, 2, \ldots, L \) pulses, where each pulse comprises \( n = 1, 2, \ldots, N \) discrete time steps. A single-input single-output (SISO) radar system has two channel impulse responses, one for the target and the other for clutter. Let \( w(n) \) denote the radar transmit waveform and \( h_t(n), h_c(n) \) denote the target and clutter channel impulse responses, respectively. Then, the radar measurements corresponding to the \( t \)-th pulse can be expressed as

\[
x(n, l) = h_t(n, l) \odot w(n, l) + h_c(n, l) \odot w(n, l) + e_r(n, l)
\]
electromagnetic channel is modeled using a physics based impulse response.

Since convolution in the time domain can be expressed as multiplication in the frequency domain (with notation in upper case), we can express the measurements in the frequency domain as:

\[ X(k, l) = H_t(k, l)W(k, l) + H_c(k, l)W(k, l) + E_r(k, l) \]  

(30)

where \( k \in K = \{1, \ldots, K\} \) is the frequency bin index. Eq. (30) can be extended to an \( I \times J \) MIMO radar and the received signal at the \( j \)-th receiver is given by

\[ X_j(k, l) = \sum_{i=1}^{I} H_{t_{ij}}(k, l)W_i(k, l) + H_{c_{ij}}(k, l)W_i(k, l) + E_{r_{ij}}(k, l), \]  

(31)

\[ \forall k \in \{1, \ldots, K\}. \] Using matrices and vectors obtained by stacking and concatenating (31) for all \( i,j \) and \( k \), the MIMO radar measurement model at the \( l \)-th pulse in vector-matrix form can be expressed as

\[ X(l) = H_t(l)W(l) + H_c(l)W(l) + E_r(l) \]  

(32)

where \( X(l) \in \mathbb{C}^{(J \times K) \times 1} \) is the received signal vector, \( H_t(l), H_c(l) \in \mathbb{C}^{(J \times K) \times (J \times J \times K)} \) are the effective transmit and clutter channel impulse response matrices respectively, \( W(l) \in \mathbb{C}^{(I \times J \times K) \times 1} \) is the radar’s effective waveform vector. \( E_r(l) \in \mathbb{C}^{(J \times K) \times 1} \) is the effective additive noise vector modeled as a zero mean i.i.d random variable (independent over pulses) with covariance matrix \( C_r \in \mathbb{R}^{(J \times K) \times (J \times K)}, C = \sigma_r^2 I \). The block diagram in Fig. 5 shows the entire procedure for this model.

**B. Smart Interference to confuse the adversary radar**

The aim of this section is to design optimal interference signals (to confuse the adversary cognitive radar) by solving a probabilistically constrained optimization problem.

At the beginning of the \( l \)-th pulse, the adversary radar transmits a pilot signal to estimate the transmit and clutter channel impulse responses \( H_t(l) \) and \( H_c(l) \) respectively. Assuming it has a perfect estimate of \( H_t(l) \) and \( H_c(l) \), the radar then chooses the optimal waveform \( W^*(l) \) such that SCNR defined below in (33) is maximized. The radar’s waveform \( W^*(l) \) is the solution to the following optimization problem

\[ W^*(l) = \arg\max_{W(l):\|W(l)\|_2=1} \text{SCNR}(H_t(l), H_c(l), W(l)), \]  

(33)

where the SCNR is defined as

\[ \text{SCNR}(H_t, H_c, W) = \frac{\|H_tW\|^2_2}{\mathbb{E}\left\{\|H_tW + E_r\|^2_2\right\}}. \]  

(34)

Denote the maximum SCNR achieved in (33) as

\[ \text{SCNR}_{\text{max}}(H_t(l), H_c(l), \sigma_r^2) = \text{SCNR}(H_t(l), H_c(l), W^*(l)). \]  

(35)

Given \( H_t(l), H_c(l) \) and the radar’s measurement noise power \( \sigma_r^2 \), the radar generates an optimal waveform at the \( l \)-th pulse using (33) as the solution to the following eigenvector problem (5):

\[ \text{A} W^*(l) = \lambda_l W^*(l) \]

\[ \text{A} = \left( (H_c(l)'H_c(l) + \sigma_r^2 I)^{-1} H_t(l)'H_t(l) \right). \]

Here \((\cdot)'\) denotes the Hermitian transpose operator.

As an external observer, we send a sequence of probe signals \( P = \{H_p(l), l \in \{1, 2, \ldots, L\}\} \) over \( L \) pulses to confuse the adversary radar and degrade its performance. The interference signal \( H_p(l-1) \) at the \((l-1)\)-th affects only radar’s clutter channel impulse response \( H_c(l) \) at the \( l \)-th pulse which subsequently results in change of optimal waveform (33) chosen by the radar \( W^*(l) \). We measure the optimal waveform at the \( l \)-th pulse in noise as \( Y(l) \). We assume constant transmit and clutter channel impulse responses \( H_t, H_c \) in the absence of the probe signals \( P \). The dynamics of our interaction with the adversary radar due to probe \( P \) are as follows and
schematically shown in Fig.6
\[ H_c(l) = H_c + H_p(l - 1) \]  
\[ H_t(l) = H_t \]  
\[ \left( (H_c(l)'H_c(l) + \sigma_c^2 I)^{-1}H_t(l)'H_t(l) \right)W^*(l) = \lambda_l W^*(l) \]  
\[ Y(l) = W^*(l) + E_o(l). \]

In (39), \( E_o(l) \) is our measurement noise modeled as a zero mean i.i.d random variable (independent over pulses) sampled from a known pdf \( f_o \) with zero mean and covariance \( C_o = (\sigma_o^2/K)I = \tilde{\sigma}_o^2I. \)

![Diagram of smart interference design to confuse the cognitive radar](image)

Fig. 6: Schematic of smart interference design to confuse the cognitive radar. The interference signal at the \( l \)th pulse affects the waveform choice of the radar in the \( (l+1) \)th pulse. We record the noisy waveform measurement \( Y(l+1) \) and generate the interference signal for the \( (l+2) \)th pulse.

Our objective is to optimally design the probe signals \( P^* = \{H_p(l), l \in \{1, \ldots, L\}\} \) that minimizes the interference signal power such that for a pre-defined \( \Delta > 0 \), there exists \( \epsilon \in [0, 1) \) such that the probability the SCNR of the radar lies below \( \Delta \) exceeds \( 1 - \epsilon \), for all \( l = 1, 2, \ldots, L \).

\[ \min_{\{H_p(l), l \in \{1,2, \ldots L\}\}} \sum_{l=1}^{L} H_p(l)'H_p(l) \]

s.t. \( \mathbb{P}_{f_o}(\text{SCNR}(H_t(l), H_c(l), Y(l)) \leq \Delta) \geq 1 - \epsilon, \forall l \in \{1,2,3, \ldots L\}. \) (40)

Here, \( \mathbb{P}_f(\cdot) \) denotes the probability wrt pdf \( f \). The design parameter \( \Delta \) is the SCNR (performance) upper bound of the cognitive radar. To confuse the radar, our task is to ensure the SCNR of the radar is less than \( \Delta \) with probability at least \( 1 - \epsilon \). Hence, \( \epsilon \) is the maximum probability of failure to confuse the radar with our smart interference signals. Although not explicitly shown, the SCNR\textsubscript{max} expression in (40) depends on our interference signal \( H_p \) as depicted in (36).

Solving the non-convex optimization problem (40) is challenging except for trivial cases. It involves two inter-related components (i) Estimating the transmit and clutter channel impulse responses \( H_t, H_c \) from observation \( Y(l) \) and (ii) Using the estimated value of channel impulse responses to generate the interference signal \( H_p(l) \). Moreover, solving for \( H_c \) and \( H_t \) from recursive equations (36) through (39) for \( l = 1, \ldots, L \) is a challenging problem since it does not have an analytical closed form solution.

With the above formulation, we can now discuss construction of smart interference to confuse the adversary radar. The cognitive radar maximizes its energy in the direction of its target impulse response and transfer function. As soon as we have an accurate estimate of the target channel transfer function from the \( L \) pulses, we can immediately generate signal dependent interference that nulls the target returns. Even if the clutter channel impulse response changes after we perform our estimation, since the target channel is stationary for longer durations, the signal dependent interference will work successfully for several pulses after we compute the estimate. The main take away from this approach is that we are exploiting the fact that the cognitive radar provides information about its channel by optimizing the waveform with respect to its environment.

C. Numerical example illustrating design of smart interference

We conclude this section with a numerical example that illustrates the smart interference framework developed above. The simulation setup is as follows:

- \( L = 2 \) pulses (optimization horizon in (40)).
- Impulse response matrices for transmit channel \( H_t = [7 \ 7] \), clutter channel \( H_c = [1 \ 1] \), and adversary radar noise covariance \( \sigma^2_c = 1 \) (32).
- Design parameters: SCNR upper bound \( \Delta = \{2.8, 3.2\} \), minimum probability of success \( \epsilon = 0.2, 0.3 \) (40).
- Probe signals for pulse index:
  \[ l = 1, H_p(1) = [0.2r \ 0.5r], \]
  \[ l = 2, H_p(2) = [0.4r \ 0.4r]. \] (41)

The smart interference parameter \( r > 0 \) parametrizes the magnitude of the probe signals. The aim is to find the optimal probe signals \( H_p(l), l = 1, 2 \) parametrized by \( r \) in (41) that solves (40). The corresponding value of \( r \) is our optimal smart interference parameter.

- Our measurement noise covariance is \( \sigma^2_o = 0.1 \) (39).

Figure 7 displays the performance of the cognitive radar as our smart interference parameter \( r \) is varied. It shows that increasing \( r \) leads to increased confusion (worse SCNR performance) of the cognitive radar. Specifically, we plot the LHS of (40), namely, \( \mathbb{P}_{f_o}(\text{SCNR}(H_t(l), H_c(l), Y(l)) \leq \Delta) \), for SCNR upper bound \( \Delta \in \{2.8, 3.3, 3.2\} \). Recall that this is the probability with which the maximum SCNR of the radar (35) lies below \( \Delta \).

To glean insight from Figure 7, let \( r^*(\Delta, \epsilon) \) denote the optimal smart interference parameter that solves (40) for design parameters \( \Delta \) and \( \epsilon \). Figure 7 shows that \( r^*(\Delta, \epsilon) \) decreases with both design parameters \( \Delta \) and \( \epsilon \). This can be justified as follows. For a fixed value of failure probability \( \epsilon \), increasing the upper bound \( \Delta \) implies the constraint (40) is satisfied for smaller \( r \), hence the optimal interference parameter \( r^*(\Delta, \epsilon) \) decreases with \( \Delta \). Recall \( \epsilon \) upper bounds the probability with which the maximum SCNR of the radar exceeds \( \Delta \). Increasing \( \epsilon \) (or equivalently, relaxing the maximum probability of failure) allows us to decrease the magnitude of the probe signals without violating the constraint in (40) for a fixed \( \Delta \). Hence, \( r^*(\Delta, \epsilon) \) decreases with both \( \Delta \) and \( \epsilon \).
the smart interference problem (40) as a stochastic control problem; since dynamic programming is intractable we will explore limited look-ahead policies and open-loop feedback control.

Regarding identifying cognitive radars, it is worthwhile developing statistical tests for utility maximization when the response of the utility maximizing adversarial radar is observed in noise; see Varian’s work [59] on noisy revealed preference. Ongoing research in developing a dynamic revealed preference framework will be used to extend the beam allocation problem of Sec. III-B to a multi-horizon setup where we analyze batches of adversary responses over multiple slow time scale epochs. Another natural extension is to a Bayesian context, namely, identifying a radar that is a Bayesian utility maximizer. We refer to [7] for seminal work in this area stemming from behavioral economics.

Finally, in the design of controlled inference, it is worthwhile considering a game-theoretic setting where the cognitive radar (adversary) and us interact dynamically. In previous work [52] we studied simpler versions of the problem in the context of cross-polarized jamming. Also, in future work, it is worthwhile to develop a stochastic gradient algorithm for estimating the optimal probe signal.

References

[1] S. Afriat. The construction of utility functions from expenditure data. International economic review, 8(1):67–77, 1967.
[2] S. Afriat. Logic of choice and economic theory. Clarendon Press Oxford, 1987.
[3] B. D. O. Anderson and J. B. Moore. Optimal filtering. Prentice Hall, Englewood Cliffs, New Jersey, 1979.
[4] G. Angioletos, C. Hellwig, and A. Pavan. Dynamic global games of regime change: Learning, multiplicity, and the timing of attacks. Economometrica, 75(3):711–756, 2007.
[5] J. S. Bergin, J. R., R. M. Guerci, and M. Rangaswamy. MIMO Clutter Discrete Probing for Cognitive Radar. In IEEE International Radar Conference, pages 1666–1670, April 2015.
[6] P. Caines. Linear Stochastic Systems. Wiley, 1988.
[7] A. Caplin and M. Dean. Revealed preference, rational inattention, and costly information acquisition. The American Economic Review, 105(7):2183–2203, 2015.
[8] O. Cappe, E. Moulines, and T. Ryden. Inference in Hidden Markov Models. Springer-Verlag, 2005.
[9] J. Cavanaugh and R. Shumway. On computing the expected fisher information matrix for state space model parameters. Statistics & Probability Letters, 26:347–355, 1996.
[10] C. Chamley. Rational herds: Economic Models of Social Learning. Cambridge University Press, 2004.
[11] E. K. P. Chong, C. Kreucher, and A. Hero. Partially observable Markov decision process approximations for adaptive sensing. Discrete Event Dynamic Systems, 19(3):377–422, 2009.
[12] D. Ciuonzo, P. K. Willett, and Y. Bar-Shalom. Tracking the tracker from its passive sonar ml-pda estimates. IEEE Transactions on Aerospace and Electronic Systems, 50(1):573–590, 2014.
[13] P. Del Moral, E. Rio, et al. Concentration inequalities for mean field particle models. Annals of Applied Probability, 21(3):1017–1052, 2011.
[14] W. Diewert. Afriat’s theorem and some extensions to choice under uncertainty. The Economic Journal, 122(560):305–331, 2012.
[15] R. J. Elliott, L. Aggoun, and J. B. Moore. Hidden Markov Models – Estimation and Control. Springer-Verlag, New York, 1995.
[16] F. Forges and E. Minelli. Afriat’s theorem for general budget sets. Journal of Economic Theory, 144(1):135–145, 2009.
[17] J. Guerci, J. Bergin, R. Guerci, M. Khanin, and M. Rangaswamy. A new MIMO clutter model for cognitive radar. In 2016 IEEE Radar Conference (RadarConf), pages 1–6. IEEE, 2016.
[18] J. R. Guerci, J. S. Bergin, R. J. Guerci, M. Khanin, and M. Rangaswamy. A New MIMO Clutter Model for Cognitive Radar. In IEEE Radar Conference, May 2016.

Fig. 7: The figure illustrates the performance of the cognitive radar as our smart interference parameter $r$ in (41) is varied. The plots display the LHS of (40), namely, probability that the radar’s maximum SCNR (which depends on $r$ (41)) is smaller than threshold $\Delta$. The probability curves are plotted for $\Delta = 2.8, 3.0, 3.2$ and signify the extent of SCNR degradation as a function of the magnitude of the probe signal.

V. Conclusion

This paper considered three important inter-related aspects of adversarial inference involving cognitive radars. First we discussed inverse tracking (estimating the adversary tracker’s estimate based on the radar’s actions) and calibration of the adversary’s sensor accuracy. Then we presented a revealed preferences methodology for identifying cognitive radars; i.e., identifying a constrained utility maximizer. Finally, we discussed designing interference to confuse the cognitive radar.

The above three aspects are inter-related as depicted in Figure 1. The levels of abstraction range from smart interference design based on Wiener filters (at the pulse/waveform level), inverse Kalman filters at the tracking level and revealed preferences for identifying utility maximization at the systems level.

Extensions: The results in this paper lead to several interesting future extensions. There is strong motivation to determine analytic performance bounds for inverse tracking/filtering and estimation of the adversary’s sensor gain. Another aspect (not considered here) is when the adversary does not know the transition kernel of our dynamics; the adversary then needs to estimate this transition kernel, and we need to estimate the estimate of this transition kernel. In future work we will design
Vikram Krishnamurthy (F’05) received the Ph.D. degree from the Australian National University in 1992. He is a professor in the School of Electrical & Computer Engineering, Cornell University. From 2002-2016 he was a Professor and Canada Research Chair at the University of British Columbia, Canada. His research interests include statistical signal processing and stochastic control in social networks and adaptive sensing. He served as Distinguished Lecturer for the IEEE Signal Processing Society and Editor-in-Chief of the IEEE Journal on Selected Topics in Signal Processing. In 2013, he was awarded an Honorary Doctorate from KTH (Royal Institute of Technology), Sweden. He is author of two books Partially Observed Markov Decision Processes and Dynamics of Engineered Artificial Membranes and Biosensors published by Cambridge University Press in 2016 and 2018, respectively.

Kunal Pattanayak (S’21) received the integrated Bachelors and Masters in Technology degrees in Electronics and Electrical Communication Engineering from Indian Institute of Technology, Kharagpur in 2018. He is currently a graduate student in the department of Electrical and Computer Engineering at Cornell University. His research interests include inverse reinforcement learning, behavioral economics, statistical signal processing, design of counter-autonomous systems for radar applications and interpretable AI. He is a recipient of the McMillen graduate fellowship by Cornell University, and has been a speaker at the 2020 Sloan-NOMIS Conference on Attention and Applied Economics.

Sanddeep Gogineni (BTech, Electronics and Communications Engineering, IIIT, India, MS, PhD, Electrical Engineering, Washington University in St. Louis) is a Research Scientist for Information Systems Laboratories with over 12 years of experience working on radar and wireless communications systems. He has worked for 6 years as an on-site contractor for Air Force Research Laboratory (AFRL), developing novel signal processing algorithms and performance analysis for passive radar systems. He received the IEEE Dayton Section Aerospace and Electronics Systems Society Award for these contributions to passive radar signal processing. Prior to his time at AFRL, during his graduate studies at Washington University in St. Louis, Dr. Gogineni developed optimal waveform design techniques for adaptive MIMO radar systems and demonstrated improved target detection and estimation performance. At ISL, Dr. Gogineni has been working on channel estimation algorithms and optimal probing strategies for MIMO radar systems in the context of Cognitive Fully Adaptive Radar (CoFAR). Additionally, Dr. Gogineni and his colleagues at ISL have demonstrated the feasibility of using neural networks and artificial intelligence techniques to solve extremely challenging radio frequency (RF) sensing problems. His expertise includes statistical signal processing, detection and estimation theory, deep learning, artificial intelligence, performance analysis, and optimization techniques with applications to active and passive RF sensing systems.
Boung Kang (S’12-M’16) received the B.S. and M.S. degrees in Electrical and Electronic Engineering from Yonsei University, Seoul, South Korea, in 2005 and 2007, respectively, and the Ph.D. degree in Electrical Engineering from the Pennsylvania State University, University Park, PA, USA, in 2015. He is currently an onsite contractor for Air Force Research Laboratory, WPAFB, OH and a radar research engineer at University of Dayton Research Institute, Dayton, OH. He worked at LG Electronics as a research engineer, Seoul, Korea, from 2007 to 2011. He developed image and video signal processing algorithms in mobile camera and monitor applications. He has served as a reviewer for several reputed IEEE journals and conferences. His research interests include statistical signal processing, detection and estimation, convex optimization, and radar signal processing with applications to radar and communication systems. Dr. Kang was a recipient of the First Place in the Student Paper Competition at the IEEE Radar Conference, Cincinnati, OH, in 2014. He also won the 2015 Robert T. Hill Best Dissertation Award presented by the IEEE Aerospace and Electronic Systems Society (AESS).

Muralidhar Rangaswamy (Fellow, IEEE) received the B.E. degree in electronics engineering from Bangalore University, Bangalore, India, in 1985, and the M.S. and Ph.D. degrees in electrical engineering from Syracuse University, Syracuse, NY, USA, concurrently in 1992. He is currently the Technical Lead for Radar Sensing with the RF Technology Branch within the Sensors Directorate, Air Force Research Laboratory (AFRL), Wright-Patterson Air Force Base, OH, USA. Prior to this, he has held industrial and academic appointments. He is a contributor to eight books and is a co-inventor on three U.S. patents. He has coauthored more than 280 refereed journal and conference record papers in the areas of his research interests, which include radar signal processing, spectrum estimation, modeling non-Gaussian interference phenomena, and statistical communication theory. Dr. Rangaswamy is a member of the Radar Systems Panel (RSP) in the IEEE-AES Society. He was on the Technical Committee of the IEEE Radar Conference series in a myriad of roles. He was the recipient of the IEEE Warren White Radar Award in 2013, the 2013 Affiliate Societies Council Dayton (ASC-D) Outstanding Scientist and Engineer Award, the 2007 IEEE Region 1 Award, the 2006 IEEE Boston Section Distinguished Member Award, and the 2005 IEEE-AESS Fred Nathanson Memorial Outstanding Young Radar Engineer Award. He was also the recipient of the 2012 and 2005 Charles Ryan Basic Research Award from the Sensors Directorate, AFRL, in addition to more than 40 scientific achievement awards. Most recently, he received the International Society for Information Fusion Jean-Pierre Le Cadre Best Paper Award at the 2019 FUSION Conference, the 2019 Technical Cooperation Panel Award from the Office of Secretary of Defense, and the 2019 IEEE Dayton Section Fritz Russ Memorial Award.