Design of Binary Quantizers for Distributed Detection under Secrecy Constraints

V. Sriram Siddhardh Nadendla, Student Member, IEEE, and Pramod K. Varshney, Fellow, IEEE

Abstract—In this paper, we consider the problem of designing binary quantizers at the sensors for a distributed detection network in the presence of an eavesdropper. We propose to design these quantizers under a secrecy constraint imposed on the eavesdropper. The performance metric chosen in this paper is the KL Divergence at both the fusion center (FC) and the eavesdropper (Eve). First, we consider the problem of secure distributed detection in the presence of identical sensors and channels. We prove that the optimal quantizer can be implemented as a likelihood ratio test, whose threshold depends on the specified secrecy constraint on the Eve. We present an algorithm to find the optimal threshold in the case of Additive White Gaussian Noise (AWGN) observation models at the sensors. In the numerical results, we discuss the tradeoff between the distributed detection performance and the secrecy constraint on the eavesdropper. We show how the system behavior varies as a function of the secrecy constraint imposed on Eve. Finally, we also investigate the problem of designing the quantizers for a distributed detection network with non-identical sensors and channels. We decompose the problem into $N$ sequential problems using dynamic programming, where each individual problem has the same structure as the scenario with identical sensors and channels. Optimum binary quantizers are obtained. Numerical results are presented for illustration.

Index Terms—Distributed Detection, Sensor Networks, Eavesdropping Attacks, Kullback-Leibler Divergence, Receiving Operating Characteristics.

I. INTRODUCTION

Distributed detection is a well-studied topic over the past three decades, with a wide range of applications ranging from civilian to military purposes [1]–[5]. A distributed detection network comprises of a network of spatially distributed sensors that observe the phenomenon-of-interest (PoI) and send processed information to a fusion center (FC) where a global decision is made regarding the presence or absence of the PoI. In general, the design of a distributed detection network is shown to be NP-Hard [6]. Under the conditional independence assumption, the optimal decision rule at the FC is given by the Chair-Varshney rule [7]. Decision of quantizers at the sensors has also been considered. In particular, Tsitsiklis [3] proved that the optimal decision rules are likelihood ratio tests (LRTs). Later, in [9], Tsitsiklis investigated the extremal properties of set of all possible likelihood-ratio quantizers (LRQs) and characterized the design of these decision rules, where the design metric is an Ali-Silvey distance measure. In almost all the work on distributed detection, secrecy and the presence of eavesdroppers was not considered. In this paper, we address the problem of designing secure, optimal local quantizers in the presence of eavesdroppers, with KL Divergence (KLD) as a design metric.

Secrecy in the context of distributed detection networks is an important problem, especially when the network is a subsystem within a larger cyber-physical system. Following are some examples where confidentiality plays a very important role in the context of distributed inference. First, consider an example of a distributed radar network where the radars observe the presence or absence of an enemy aircraft. Any information about the radar decisions at the enemy aircraft can help it to adapt its strategy so as to remain invisible to the radar and in clandestine pursuit of its mission. Another example is the case of a cognitive-radio (CR) network where a third-party CR may compete with the CR network in selfishly using a given vacant PU channel, without paying any participation costs to the network moderator. Thus, selfishness and maliciousness can be two motives of any eavesdropper to compromise the confidentiality of any inference network. In this paper, we address confidentiality in distributed inference networks and focus on the design of the network such that the eavesdropper may not acquire any information beyond tolerable limits.

In the past, a few attempts have been made to address the problem of eavesdropping threats by designing ciphers in the broader context of sensor networks. For example, Aysal et al. in [10] investigated the problem of secure distributed estimation by incorporating a stochastic cipher as an additional block to the existing sensor networks to improve secrecy. They showed a significant deterioration in the Eve’s performance (in terms of bias and mean squared error) at the cost of a marginal increase in the estimation variance at the FC. Similar attempts have been made in the context of distributed detection in sensor networks by Nadendla in [11], where the author presented an optimal network (sensor quantizers, flipping probabilities in the stochastic cipher and the fusion rule) that minimizes the error probability at the FC in the presence of a constraint on Eve’s error probability. In [12], Jeon et al. proposed a cooperative transmission scheme for a sensor network where the sensors are partitioned into non-flipping, flipping and dormant sets, based on the thresholds dictated by the FC. The non-flipping set of sensors quantize the sensed data and transmit them to the FC, while the flipping sensors transmit flipped decisions in order to confuse the Eve. The sensors within the dormant set sleep, in order to conserve energy and have an energy-efficient sensor network with longer lifetime.

In all of the above attempts mentioned in the context of
securing distributed detection systems, security was incorporated as an afterthought in that, separate security blocks were added after the original system had been designed without considering the possible security threats. Marano et al. in [13], on the other hand, investigated the problem of designing optimal decision rules for a censoring sensor network in the presence of eavesdroppers. Although their framework of censoring sensor networks is more general, they assume that the Eve can only determine whether an individual sensor transmits its decision or not. In reality, Eve can extract more information than just merely determining the presence or absence of transmission, and hence can make a reasonably good decision based on its receptions. Therefore, in our preliminary work to address this problem, in [14], we investigated the problem of designing sensor quantizers for a distributed detection network under an asymptotic regime that maximize the difference in the KLDs at the FC and Eve.

In this paper, we consider a distributed detection network with all the channels between the sensors, FC and Eve modelled as binary symmetric channels (BSCs), whose transition probabilities are known to the network designer. We design optimal sensor quantizers that maximize KL divergence at the FC while constraining the Eve’s performance. We consider two scenarios, one where the channels between the sensors and the FC (likewise, channels between sensors and the Eve) are identical, and the second where the channels are non-identical. In the identical channel scenario, we assume that the Eve has noisier channels than the FC’s channels, and show that the optimal quantizer at the local sensors is a likelihood ratio test (LRT), irrespective of the presence or absence of Eve. We present an illustrative example where we assume that the sensors make noisy observations of a known deterministic signal. We present an algorithm to find the optimal threshold using which the KL Divergence at the FC is maximized within the tolerable bounds on the Eve’s KL Divergence. In the scenario where channels are non-identical, we decompose the problem into N subproblems to be solved sequentially using dynamic programming. Consequently, we decouple the Eve’s constraint into N individual constraints, thus allowing us to solve each of these decoupled problems as in the identical sensor case.

The remainder of the paper is organized as follows. In Section II we present the system framework and introduce the design metrics considered in this paper. Before we delve into the problem statement, we present all the necessary tools required to solve the problem of designing optimal sensor quantizers in a distributed detection network in Section III. Then, in Section IV we consider the scenario where all the channels to the FC as well as to Eve are identical as a group. Here, we present an illustrative example where we assume that the sensors make noisy observations of a deterministic signal, and present an algorithm to find the optimal threshold for the LRT in the presence of Eve. Numerical results are also presented where we discuss the tradeoff between the network performance and tolerable secrecy. In Section V we present our design and analysis for a more general scenario where the sensors and channels are both non-identical. Our concluding remarks are presented in Section VI.
(x_i, y_i) in the i-th sensor’s receiver operating characteristic (ROC) plot to represent a quantizer rule γ_i. In other words, two quantizers γ_1 and γ_2 are considered identical (equivalent), if their operating points (x_1, y_1) and (x_2, y_2) are the same. Given the operating point (x_i, y_i), the Kullback-Leibler (KL) Divergence of the i-th sensor is defined as follows.

\[ D_i = x_i \log \frac{x_i}{y_i} + (1 - x_i) \log \frac{1 - x_i}{1 - y_i} \]  

(2)

When u_i is transmitted over the channels at each time t, the operating point of the i-th sensor, the i-th sensor’s operating point (x_i, y_i) is transformed into (x_{fci}, y_{fci}) and (x_i, y_i) at the FC and Eve respectively, which are given as follows.

\[ x_{fci} = P(v_i,t = 1|H_0) = \rho_{fci} + (1 - 2\rho_{fci})x_i \]  

(3a)

\[ y_{fci} = P(v_i,t = 1|H_1) = \rho_{fci} + (1 - 2\rho_{fci})y_i \]  

(3b)

\[ x_i = P(w_i,t = 1|H_0) = \rho_{ci} + (1 - 2\rho_{ci})x_i \]  

(3c)

\[ y_i = P(w_i,t = 1|H_1) = \rho_{ci} + (1 - 2\rho_{ci})y_i \]  

(3d)

Let \( A_{FC}^r, A_{E}^r \in \mathcal{Y}^T \) denote the acceptance regions of the hypothesis H1 at FC and Eve respectively, over a time-window \( t = 1, \ldots, T \). Then, the global probabilities of false alarm and detection at the FC and Eve are given by

\[ \alpha_{FC} = Pr(v_1 \in A_{FC}^r | H_0), \quad \beta_{FC} = Pr(A_{FC}^r | H_1). \]  

\[ \alpha_{E} = Pr(w_1 \in A_{E}^r | H_0), \quad \beta_{E} = Pr(w_1 \in A_{E}^r | H_1). \]  

(4)

where \( v_1 = \{v_{1,1}, \ldots, v_{1,T}\} \) and \( w_1 = \{w_{1,1}, \ldots, w_{1,T}\} \) are the received symbols at the FC and Eve respectively, transmitted by the i-th sensor over a time window of length T.

**Theorem 1 (Stein’s Lemma)**. For any \( 0 < \delta, \varphi < \frac{1}{2} \), let \( \beta_{\delta,\varphi} = \min_{\alpha_{\delta,\varphi} < \delta} \beta_{F,C}^\delta \) and \( \beta_{\delta,\varphi} = \min_{\alpha_{\delta,\varphi} < \delta} \beta_{E,\varphi} \).

Then,

\[ \lim_{\delta \to 0} \lim_{T \to \infty} -\frac{1}{T} \log \beta_{\delta,\varphi} = \mathbb{D}_{FC} \]  

(5)

\[ \lim_{\varphi \to 0} \lim_{T \to \infty} -\frac{1}{T} \log \beta_{\delta,\varphi} = \mathbb{D}_{E} \]

where \( \mathbb{D}_{FC} \) and \( \mathbb{D}_{E} \) are KL divergences at the FC and Eve respectively, which are defined as follows.

\[ \mathbb{D}_{FC} = \sum_{i=1}^{N} x_{fci} \log \left( \frac{x_{fci}}{y_{fci}} \right) + (1 - x_{fci}) \log \left( \frac{1 - x_{fci}}{1 - y_{fci}} \right) \]

\[ \mathbb{D}_{E} = \sum_{i=1}^{N} x_i \log \left( \frac{x_i}{y_i} \right) + (1 - x_i) \log \left( \frac{1 - x_i}{1 - y_i} \right) \]

(6)

In short, KL Divergence is the error exponent for the probability of missed-detection when the probability of false alarm is constrained (and diminishing to zero with time). Therefore, as a surrogate to the probability of missed-detection, we choose KL Divergence as the performance metric in our paper. For the sake of convenience, we denote

\[ D_{FC,i} = x_{fci} \log \left( \frac{x_{fci}}{y_{fci}} \right) + (1 - x_{fci}) \log \left( \frac{1 - x_{fci}}{1 - y_{fci}} \right) \]

\[ D_{E,i} = x_i \log \left( \frac{x_i}{y_i} \right) + (1 - x_i) \log \left( \frac{1 - x_i}{1 - y_i} \right) \]

(7)

where \( D_{FC,i} \) and \( D_{E,i} \) denote the i-th sensor’s contribution to the overall performance (KL Divergence) at the FC and Eve respectively. Note that \( D_{FC} \) and \( D_{E} \) are both convex functions of \( x_i \) and \( y_i \) over a compact space \([0,1]^2\).

In our model, we restrict our attention to the operating points that are above the line \( y_i = x_i \), due to the symmetry of the KL Divergence. Within this set of decision rules, one can choose any arbitrary family of feasible tests \( \Gamma_i \) at the i-th sensor. Caratheodory’s theorem [13] states that this feasible set can be expanded into its convex hull by allowing randomization (linear stochastic combination of operating points) between a bounded (finite) number of operating points within the set. In practice, this convex hull can be computed efficiently using the quickhull algorithm proposed by Barber et al. in [16]. Therefore, for the sake of tractability, we, henceforth, assume that the feasible region \( \Gamma_i \) is convex. Of course, if the boundary of \( \Gamma_i \) consists only of LRTs, then \( \Gamma_i \) is convex as LRTs are optimal and form a convex-hull.

In this paper, we design a distributed detection network where the FC’s KLD is maximized while, the Eve’s KLD is constrained to a prescribed tolerance, denoted as \( \alpha \). Before we delve into the problem of designing the optimal distributed detection network, we first present some basic properties and transformations of operating points which are essential in our ROC-based design presented later in the paper.

### III. ANALYSIS OF ROC TRANSFORMATIONS

In this section, we focus our attention on the transformation of the operating point of a single sensor due to a binary symmetric channel (BSC) at both the FC and Eve. Let the operating point of a given quantizer be \( A = (x,y) \). As mentioned earlier, the sensor’s quantizer characteristics \( (x,y) \) are represented using its operating point in the ROC plot. Also, consider two BSCs with transition probabilities \( \rho_1 \) and \( \rho_2 \), each of which transforms the operating point \( A = (x,y) \) into \( B_1 = (x_1, y_1) \) and \( B_2 = (x_2, y_2) \). Let \( C = \{x,y\} \). In the following lemma, we present a useful relationship between \( A, B_1, B_2 \) and \( C \).

**Lemma 1.** Let \( 0 \leq \rho_1 \leq \rho_2 \leq \frac{1}{2} \). Then, \( B_1 \) and \( B_2 \) always lie on the line segment joining \( A \) and \( C \). In addition, the following inequality holds true.

\[ \frac{x}{y} \leq \frac{x_1}{y_1} \leq \frac{x_2}{y_2} \leq \frac{1 - x_2}{1 - y_2} \leq \frac{1 - x_1}{1 - y_1} \leq \frac{1 - x}{1 - y} \]

(8)

**Proof:** Consider a BSC with transition probability \( \rho \), which transforms the operating point \( A = (x,y) \) into \( B = (x_1, y_1) \).
In fact, as \( \rho \rightarrow \frac{1}{2} \), \( B \rightarrow C \). In other words, for a given sensor’s operating point \( A \), the transformed operating point \( B \) slides along the line segment joining \( A \) and \( C \), in terms of increasing \( \rho \), as shown in Figure 2. We denote the Euclidean distance between \( B \) and \( C \) as \( \phi_{BC} = \sqrt{\left( \hat{x} - \frac{1}{2} \right)^2 + \left( \hat{y} - \frac{1}{2} \right)^2} \). Differentiating \( \phi_{BC} \) with respect to \( \rho \), we have

\[
\frac{d\phi_{BC}}{d\rho} = \frac{1}{\phi_{BC}} \left[ \left( \hat{x} - \frac{1}{2} \right) (1 - 2x) + \left( \hat{y} - \frac{1}{2} \right) (1 - 2y) \right] - (1 - 2\rho) \left[ x(1 - x) + y(1 - y) \right] \frac{1}{\phi_{BC}} \leq 0,
\]

since the function \( x(1 - x) + y(1 - y) \) is concave and attains a maximum value of \( \frac{1}{4} \) at \( (\frac{1}{2}, \frac{1}{2}) \). In other words, \( B \) slides towards \( C \) as \( \rho \) increases. Consequently, as shown in Figure 2, \( B_1 \) is farther away from \( C \) than \( B_2 \) on the line joining \( A \) and \( C \), since \( 0 \leq \rho_1 \leq \rho_2 \leq 1 \).

Note that the slope of the line joining \((0, 0)\) and \( B_1 \) is \( \frac{\hat{y}}{\hat{x}} \), and similarly, \( \frac{\hat{y}}{\hat{x}} \) in the case of \( B_2 \). Since \( B_2 \) is closer to \( B_1 \) to \( C \), as shown in Figure 2, \( \frac{\hat{y}}{\hat{x}} \geq \frac{\hat{y}}{\hat{x}} \) and the slope tends to 1 as the transition probability approaches \( \frac{1}{2} \). A similar argument holds for the slope of the lines that join \( B_1 \) and \( B_2 \) with \( (1, 1) \). Therefore, the inequality given in Equation 13 holds.

In order to understand the impact of this transformation on the performance of the network, let us now analyze the KL Divergence at some arbitrary operating point \( B = (\hat{x}, \hat{y}) \) due to a BSC with transition probability \( \rho \) operating on the sensor operating point \( A \). In the following lemma, we show that the KL Divergence decreases with increasing \( \rho \).

\[\text{Lemma 2.} \quad \text{Given the sensor operating point } A = (x, y), \text{ let } B = (\hat{x}, \hat{y}) \text{ denote the transformed operating point due to a BSC with transition probability } \rho. \text{ Let } D_B \text{ denote the KL Divergence at } B. \text{ Then, for } 0 \leq \rho \leq \frac{1}{2}, D_B \text{ is a monotonically decreasing function of } \rho \text{ whenever } y \geq x.\]

\[\text{Proof:} \quad \text{The KL Divergence at the transformed operating point } B \text{ is defined as follows.} \]

\[
D_B = \hat{x} \log \frac{\hat{x}}{y} + (1 - \hat{x}) \log \frac{1 - \hat{x}}{1 - y}. \quad (14)
\]

Differentiating \( D_B \) with respect to \( \rho \), we have

\[
\frac{dD_B}{d\rho} = (1 - 2y) \left[ \frac{1 - \hat{x}}{1 - y} - \frac{\hat{x}}{y} \right] - (1 - 2x) \left[ \log \left( \frac{1 - \hat{x}}{1 - y} \right) - \log \left( \frac{\hat{x}}{y} \right) \right] \]

\[
= \left( \frac{1 - \hat{x}}{1 - y} - \frac{\hat{x}}{y} \right) \left[ (1 - 2y) \right] - (1 - 2x) \left( \log \left( \frac{1 - \hat{x}}{1 - y} \right) - \log \left( \frac{\hat{x}}{y} \right) \right) \]

\[
\leq 0, \quad (15)
\]

From Lemma 1, we have

\[
\frac{\hat{x}}{y} \leq \frac{1 - \hat{x}}{1 - y}. \quad (16)
\]
In other words, \( 1 - \frac{\hat{x}}{\hat{y}} - \frac{x}{y} \geq 0 \). Therefore, the sign of \( \frac{dD_B}{d\rho} \) does not depend on \( \frac{1 - \hat{y}}{1 - \hat{x}} - \frac{y}{x} \).

Also, using the properties of the \( \log() \) function shown in Figure 3, we have

\[
1 - \hat{y} \leq \log\left(\frac{1 - \hat{x}}{1 - \hat{y}}\right) - \log\left(\frac{\hat{x}}{y}\right) \leq \frac{\hat{y}}{\hat{x}}.
\]

Substituting Equation 17 in Equation 15, we have

\[
\left(\frac{1 - \hat{x}}{1 - \hat{y}} - \frac{x}{y}\right)^{-1} \frac{dD_B}{d\rho} \leq (1 - 2y) - (1 - 2x) \left\{\frac{1 - \hat{y}}{1 - \hat{x}}\right\}
\]

\[
\left(\frac{1 - \hat{x}}{1 - \hat{y}} - \frac{x}{y}\right)^{-1} \frac{dD_B}{d\rho} \leq -(y - x) \frac{1 - \hat{x}}{1 - \hat{y}}.
\]

Since \( \frac{dD_B}{d\rho} \leq 0 \), \( D_B \) is a monotonically decreasing function of \( \rho \), for all \( \rho \in [0, \frac{1}{2}] \).

Having analyzed the impact of BSCs on the ROC, let us now shift our focus on finding those quantizers that maximize the KL Divergence at the sensor or the FC. Given any operating point \( A = (x, y) \) at the sensor, we investigate the behavior of \( D_A \) with respect to \( y \), for a fixed value of \( x \).

**Lemma 3.** The optimal quantizer always lies on the boundary of the set of all feasible quantizer designs.

**Proof:** For a fixed value of \( x \), we differentiate \( D_A \) with respect to \( y \) as follows.

\[
\frac{dD_A}{dy}\bigg|_{\text{fixed } x} = \frac{1 - x}{1 - y} - \frac{x}{y}.
\]

From Lemma 1, we have \( \frac{dD_A}{dy}\bigg|_{\text{fixed } x} \geq 0 \). In other words, \( D_A \) is a monotonically increasing function of \( y \), for a fixed value of \( x \) (as shown in Figure 4). Hence, we are always interested in quantizer rules whose operating points lie on the boundary of the set of all feasible quantizers.

In summary, the sensor operating point chosen on the LRT boundary slides towards the point \( (\frac{1}{2}, \frac{1}{2}) \) as the channel deteriorates (increasing \( \rho \)), which, in turn, degrades the KLD of any decision rule \( \gamma \) to zero. Therefore, we address the problem of finding the operating point on the boundary which maximizes \( D_{FC} \), where the boundary is dictated by the Eve’s constraint \( D_E = \alpha \).

## IV. Optimal Quantizer Design in the Presence of Identical Sensors and Channels

In this section, we address the problem of designing the optimal quantizers in the sensor network, and consider a special setting where all the sensors and the channels between the sensors and the FC (likewise, channels between sensors and the Eve) are identical. This can be stated formally as follows.

For all \( i = 1, \ldots, N \), we have

\[
\begin{align*}
& p_{i,0}(x) = p_0(x), \quad p_{i,1}(x) = p_1(x) \\
& x_i = x, \quad y_i = y \\
& \rho_{f_{ci}} = \rho_{f_{c}}, \quad \rho_{e_i} = \rho_e
\end{align*}
\]

Since all the sensors and their corresponding channels are identical, we have \( x_{f_{ci}} = x_{f_c}, \ y_{f_{ci}} = y_{f_c}, \ x_e = x_e \) and \( y_e = y_e \) for all \( i = 1, \ldots, N \). Because of this, \( D_i = D, \ D_{F_{C_i}} = D_{FC} \) and \( D_{E_i} = D_E \) for all \( i = 1, \ldots, N \), and consequently, the KLD at the FC and Eve reduces to \( D_{FC} = N D_{FC} \) and \( D_E = N D_E \).

With the assumption of identical sensors and channels, the global problem can be reduced to the design of the quantizer at a single sensor, which is mathematically formulated as follows.

**Problem 1.** Find

\[
\arg\max_\gamma D_{FC} \quad \text{s.t.}
\]

1. \( D_E \leq \alpha \)
2. \( (x, y) \in \mathcal{R} \).
where $\tilde{\alpha} = \frac{\alpha}{N}$. Note that $D_{FC}$ and $D_E$ are both convex functions of $x$ and $y$. Since, Constraint 1 in Problem 4 induces a convex level-set, Problem 4 is a convex optimization problem and the optimal solution is an extreme point within the feasibility set $[15]$. In other words, we focus our attention on the boundary of the Eve’s constraint, i.e. $D_E = \tilde{\alpha}$. Therefore, we initiate our investigation of finding the optimal quantizers with the necessary conditions for guaranteeing $D_E = \tilde{\alpha}$.

**Lemma 4.** The two necessary conditions for guaranteeing $D_E = \tilde{\alpha}$ when transition probability of the Eve’s BSC is given as $\rho_e < \frac{1}{2}$, are as follows.

\[
\frac{dy}{dx} = \frac{\log \left( \frac{1 - x_e}{1 - ye} \right) - \log \left( \frac{x_e}{ye} \right)}{1 - x_e - \frac{x_e}{ye}} \quad (21)
\]

and

\[
\left( \frac{1 - x_e}{1 - ye} \frac{x_e}{ye} \right) \frac{d^2 y}{dx^2} = (1 - 2\rho_e) \left[ - \left( \frac{1 - x_e}{(1 - ye)^2} + \frac{x_e}{ye} \right) \left( \frac{dy}{dx} \right)^2 \right. \\
+ 2 \left( \frac{1}{ye} + \frac{1}{1 - ye} \right) \frac{dy}{dx} - \left( \frac{1}{x_e} + \frac{1}{1 - x_e} \right). \quad (22)
\]

Therefore, from Equation (22), we have

\[
\frac{x_e}{ye} \leq \frac{dy}{dx} \leq \frac{1 - x_e}{1 - ye}. \quad (23)
\]

**Proof:** Since $\tilde{\alpha}$ is a constant (fixed design-parameter), we differentiate $D_E$ with respect to $x$ and equate it to zero, as follows.

\[
\frac{dD_E}{dx} = \frac{d}{dx} \left[ x_e \log \frac{x_e}{ye} + (1 - x_e) \log \left( \frac{1 - x_e}{1 - ye} \right) \right] \\
= (1 - 2\rho_e) \left\{ \left( \frac{1 - x_e}{1 - ye} - \frac{x_e}{ye} \right) \frac{dy}{dx} \\
- \left\{ \log \left( \frac{1 - x_e}{1 - ye} \right) - \log \left( \frac{x_e}{ye} \right) \right\} \right\} \\
= 0. \quad (24)
\]

In other words, we have Equation (21).

Given two points $a \geq b$, due to the concavity of the $\log(\cdot)$ function, the slope of the line joining $(a, \log a)$ and $(b, \log b)$ always lies between the slopes of the $\log(\cdot)$ at points $a$ and $b$ respectively (Refer to Figure 3). Hence, we have Equation (23).

Furthermore, we differentiate Equation (24) again with respect to $x$ as follows, in order to find a closed-form expression for $\frac{d^2 y}{dx^2}$.

\[
\frac{d^2 D_E}{dx^2} = (1 - 2\rho_e) \frac{d}{dx} \left[ \left( \frac{1 - x_e}{1 - ye} - \frac{x_e}{ye} \right) \frac{dy}{dx} \\
- \left\{ \log \left( \frac{1 - x_e}{1 - ye} \right) - \log \left( \frac{x_e}{ye} \right) \right\} \right] \\
= (1 - 2\rho_e) \left( \frac{1 - x_e}{1 - ye} - \frac{x_e}{ye} \right) \frac{d^2 y}{dx^2} \\
+ (1 - 2\rho_e) \left( \frac{1}{ye} + \frac{1}{1 - ye} \right) \frac{dy}{dx} \\
- 2(1 - 2\rho_e) \left( \frac{1}{x_e} + \frac{1}{1 - x_e} \right) \frac{dy}{dx} \\
+ (1 - 2\rho_e) \left( \frac{1}{x_e} + \frac{1}{1 - x_e} \right) \frac{d^2 y}{dx^2} \quad (25)
\]

In other words, we have Equation (22) [Lemma 4 provides us the necessary conditions in order to ensure that the Eve’s performance is constrained to $D_E = \alpha$. These necessary conditions are useful in analyzing the behavior of the sensor’s KL divergence $D$, along with FC’s KL Divergence, $D_{FC}$, in terms of $x$.

First, we consider the case where the channels between the sensors and the FC are ideal. In other words, $\rho_{fc} = 0$. Consequently, we have $x_{fc} = x$, $y_{fc} = y$ and $D_{FC} = D$. In the following theorem, we prove that $D_{FC} = D$ is a convex function of $x$ whenever $D_E(x, y) = \alpha$.

**Theorem 2.** Given that the Eve’s channel is a BSC with transition probability $\rho_e < \frac{1}{2}$, $D$ is a strict convex function of $x$, for all $x$ such that $(x, y) \in \mathcal{R}_{ach}$, and $D_E(x, y) = \alpha$.

**Proof:** Proof is provided in Appendix A [Lemma 4 provides us the necessary conditions in order to ensure that the Eve’s performance is constrained to $D_E = \alpha$. These necessary conditions are useful in analyzing the behavior of the sensor’s KL divergence $D$, along with FC’s KL Divergence, $D_{FC}$, in terms of $x$.

Now, we consider non-ideal channels between the sensors and the FC, i.e., $\rho_{fc} \neq 0$. Having proved the convexity for the ideal-channel case, since $(x_{fc}, y_{fc})$ is a linear transformation of $(x, y)$, we now show that $D_{FC}$ is also a convex function of $x$, whenever $D_E = \alpha$.

**Theorem 3.** Let the BSCs corresponding to the FC and Eve have transition probabilities $0 < \rho_{fc}, \rho_e < \frac{1}{2}$. Then, $D_{FC}$ is a strict convex function of $x$, for all $x$ such that $(x, y) \in \mathcal{R}_{ach}$, and $D_E(x, y) = \alpha$.  

**Proof:** Note that $(x_{fc}, y_{fc})$ is a linear transformation of $(x, y)$. This can be mathematically expressed as follows.

\[
\begin{bmatrix} x_{fc} \\ y_{fc} \end{bmatrix} = \rho_{fc} \begin{bmatrix} 1 \\ 1 \end{bmatrix} + (1 - 2\rho_{fc}) \begin{bmatrix} x \\ y \end{bmatrix}. \quad (26)
\]

In other words, a composition of $D$ with an affine transformation, as given in Equation (25), results in $D_{FC}$. Consequently, since $D$ is a convex function, $D_{FC}$ is also a convex function [Theorem 3 provides us the necessary conditions in order to ensure that the Eve’s performance is constrained to $D_E = \alpha$. These necessary conditions are useful in analyzing the behavior of the sensor’s KL divergence $D$, along with FC’s KL Divergence, $D_{FC}$, in terms of $x$.

Thus, for any BSC with transition probability $\rho_{fc}$ corresponding to the FC, $D_{fc}$ is a convex function of $x$. Therefore,
the optimum quantizer that maximizes $D_{FC}$ is on the boundary of the set of feasible quantizers $\Gamma$.

Let $y = g_{LRT}(x)$ denote the ROC curve determined only by LRT rules. Therefore, due to Theorem 2 the optimal quantizer is always on the boundary of $y = g_{LRT}(x)$. Let us define $\mathcal{R}$ as the set of all feasible quantizers in the ROC, in the presence of Eve’s constraint $D_{E} \leq \bar{\alpha}$. Then, $\mathcal{R} \triangleq \{(x, y) \mid y \leq g_{LRT}(x)\} \cup \{(x, y) \mid D_{E} \leq \bar{\alpha}\}$. Note that, the optimal quantizer lies on the intersection of the two curves, $y = g_{LRT}(x)$ and $D_{E} = \bar{\alpha}$, in which case, the problem reduces to finding the intersection of these two curves. This can happen under some necessary conditions, as stated in the following claim.

**Claim 1.** Let $f(x) \triangleq D_{FC}(x, y = g_{LRT}(x))$. If $f(x)$ is a quasi-concave function of $x$, then there are at most two intersection points for the curves $y = g_{LRT}(x)$ and $D_{E} = \bar{\alpha}$. The optimal quantizer corresponds to one of the two intersection points.

Let $f(x)$ be a quasi-concave function of $x$. Then, from Theorem 2 since $D_{FC}$ is a strict convex function of $x$, there are at most two points of intersection for the curves $y = g_{LRT}(x)$ and $D_{E} = \bar{\alpha}$, of which, one of them corresponds to the optimal quantizer.

Having restricted our attention to $f(x)$ that is quasi-concave in $x$, the problem now reduces to finding these two intersection points on the ROC. More importantly, since we are interested in the optimal quantizer design, we need to find the threshold for the LRT that maximizes $D_{FC}$. Since, both $x$ and $y$ are tail-probabilities where the start of the tail is the threshold, $x$ and $y$ are both monotonically decreasing functions of the threshold $\lambda$. Therefore, we have the following claim.

**Claim 2.** The two intersection points can be found by investigating the zeros of the function $h(\lambda) \triangleq D_{E}(x(\lambda), y(\lambda)) - \bar{\alpha}$, where $x$ and $y$ are parameterized by the LRT threshold $\lambda$.

Let $\bar{\alpha}_{\text{max}}$ denote the value of KL Divergence at which $D_{E}$ reaches its maximum value. In other words, the optimal quantizer design in the absence of Eve (equivalent to $\bar{\alpha} = \infty$), denoted $(x_{\infty}, y_{\infty})$, is the same as the optimal quantizer for any $\bar{\alpha} \geq \bar{\alpha}_{\text{max}}$. Obviously, the function $h(\lambda)$ has two real zeros only when $\bar{\alpha} < \bar{\alpha}_{\text{max}}$. Note that only one of them provides the maximum KL Divergence at the FC.

In order to find both zeros of the function $h(\lambda) = 0$, we use the bisection method where we first find the point $\lambda^{*}$ at which $h(\lambda)$ attains its maximum value. Then, consider two points, one on either side of $\lambda^{*}$ (which are at a significant distance from $\lambda^{*}$) as initial points and use the bisection algorithm to find the roots of $h(\lambda) = 0$. We call these two zeros as $\lambda_{1}$ and $\lambda_{2}$. Then, we compute and compare $D_{FC}$ at the operating points $(x(\lambda_{1}), y(\lambda_{1}))$ and $(x(\lambda_{2}), y(\lambda_{2}))$. We choose that threshold as the optimal choice, which results in the maximum $D_{FC}$.

**A. Illustrative Example**

We have so far shown that the optimal quantizer lies at the intersection of the curves $D_{E} = \bar{\alpha}$ and the LRT boundary in the ROC. But, the structure of the LRT is specific to the observation model, and therefore, is difficult to characterize the optimal sensor quantizer, in general. Therefore, in this paper, we choose to illustrate the design methodology for an example, where the sensors observe the presence or absence of a known deterministic signal, which is corrupted by additive Gaussian noise.

For the sake of illustration, we elaborate on the above arguments in the context of an example where the sensors observe the presence or absence of a known deterministic signal, which is corrupted by additive Gaussian noise.

\[
\begin{align*}
\text{Let } D_{E} &= \bar{\alpha} \text{ and the LRT boundary in the ROC.}
\end{align*}
\]

Fig. 5: KLD at the sensor, as a function of $x$

1Note that

\[
\lim_{x \to \infty} f(x) = 0, \quad \lim_{x \to -\infty} f(x) = 0
\]

Since, KLD is always non-negative, we always have $f(x) \geq 0$. Also, since any LRT curve $y = g_{LRT}(x)$ cuts through the level-sets of $D_{FC}$ and is concave, $f(x)$ is a quasi-concave function of $x$.\n
\[
\begin{align*}
\text{SNR = 0.5} & \quad \text{SNR = 1} \\
\text{SNR = 2}
\end{align*}
\]
constraint $D_E = \tilde{\alpha}$, we substitute $x_e = \rho_e + (1 - 2\rho_e)Q\left(\frac{\lambda}{\sigma}\right)$ and $y_e = \rho_e + (1 - 2\rho_e)Q\left(\frac{\lambda - \theta}{\sigma}\right)$ in $D_E$ to obtain $h(\lambda) = D_E(x(\lambda), y(\lambda)) - \tilde{\alpha}$.

As shown in Figure 6, $h(\lambda)$ is a quasi-concave function of $\lambda$, with the tails converging to $-\tilde{\alpha}$. Therefore, there are at most two solutions to the equation $h(\lambda) = 0$. The optimum sensor threshold can be found by investigating the two zeros of $h(\lambda)$, as suggested in Claim 2 and comparing them in terms of $D_{FC}$.

B. Discussion and Results

In this subsection, we first discuss the impact of the secrecy constraint on the performance of the sensor network. Obviously, when we consider $\tilde{\alpha} = 0$, the network achieves perfect secrecy. But, this also forces the network to be blind in that $D_{FC} \to 0$. On the other extreme, consider a scenario where $\tilde{\alpha} \to \infty$. This is equivalent to the case where there is no eavesdropper present in the network. In other words, the optimal quantizer is given by $(x_\infty, y_\infty)$. For any finite $\tilde{\alpha} > 0$, we numerically investigate the tradeoff between secrecy and performance of a given distributed detection system.

Since $\tilde{\alpha}$ is the tolerable limit on the performance of Eve, the greater the information leakage we can tolerate, the better the performance of the distributed detection network. This tradeoff is captured by Figure 7, where the maximum $D_{FC}$ in the presence of a constrained Eve increases with increasing $\tilde{\alpha}$. Note that, beyond a certain value of $\tilde{\alpha}$, the max $D_{FC}$ gets saturated. Note that the value of $D_{FC}$ at the saturation level is the same as the optimal KLD at the FC in the absence of Eve. This saturation level is dictated by the fundamental limits enforced by the imperfect observations and channel models within the network.

Next, we demonstrate the impact of the Eve's constraint on the ROC plot, as well as the KL Divergence at the FC, in Figure 8 when the FC's channels are ideal ($\rho_{fc} = 0$). Note that this argument can be carried over to any general BSC at the FC, as the operating point $(x_{fc}, y_{fc})$ is a linear transformation of $(x, y)$. In the Figure 8 we assume $\rho_e = 0.1$ and consider two different values of $\tilde{\alpha}$. Note that, as $\tilde{\alpha}$ decreases, $D_{FC}$ becomes deeper and flat-bottomed as a function of $x$ over the Eve’s constraint boundary $D_e = \tilde{\alpha}$. Another important observation to be made is the fact that the optimal solution in the presence and absence of Eve (red curves) always is on the boundary of the LRT curve, although the thresholds vary depending on the scenario. Since the sufficient test-statistic is the same irrespective of the presence or absence of Eve, the network designer may implement the system in terms of a threshold that can be varied.

V. OPTIMAL QUANTIZER DESIGN IN THE PRESENCE OF NON-IDENTICAL SENSORS AND CHANNELS

In Section IV, we investigated the case of identical sensors and channels. Note that this is similar to the case of designing the quantizer at a single sensor. In this section, we investigate the problem of designing the quantizers in the sensor network with non-identical sensors and channels. This is formally stated as follows.

**Problem 2. Find**

$$\arg\max_{\gamma=(\gamma_1, \ldots, \gamma_N)} D_{fc}, \text{ s.t.}$$

1. $D_e \leq \alpha$
2. $(x_i, y_i) \in R_i, \forall i = 1, \ldots, N$.

Since the sensor observations are conditionally independent, $D_{FC}$ is separable. In other words, we have $D_{FC} = \sum_{i=1}^{N} D_{FC_i}$. Therefore, we solve the problem using the approach of dynamic programming [18], where we decouple the problem into $N$ sequential problems.

Let $D_{FC_i}$ denote the maximum KL Divergence achievable at the FC in the absence of Eve, due to the $i^{th}$ sensor. Also, let $D_{E_i}$ denote the KL Divergence at the Eve due to the $i^{th}$ sensor. We define the quality of the FC’s and the Eve’s channels corresponding to the $i^{th}$ sensor as $k_i = \frac{D_{FC_i}}{D_{E_i}}$. The quality

![Fig. 6: Plot of $h(\lambda)$ as a function of $\lambda$](image1)

![Fig. 7: Tradeoff between max $D_{FC}$ and $\tilde{\alpha}$.](image2)
$k_i$ represents the tradeoff between the detection performance and secrecy. In order to achieve the tradeoff in the presence of Eve, we define an order among the sensors based on the quality $k_i$ of the corresponding FC’s and Eve’s channels. In this paper, we assume that the sensors are ordered such that $k_1 \geq \cdots \geq k_N$. Therefore, we let $\alpha_i = \max\{\alpha_i - D_{E_i}^*\}$. This allows us to select the(s) with lower indices to achieve better tradeoff in terms of the sensor quality by considering the order of decreasing quality in our sequential allocation mechanism.

Let us define the following function:

$$\Psi_n = \Psi_{n-1} + D_{FCn}, \quad \forall \ n = 2, \cdots, N. \quad (30)$$

where $\Psi_1 = D_{FC1}$ is the initial stage of the proposed sequential allocation mechanism. The following theorem, based on dynamic programming approach, presents the optimal choice of $\alpha = \{\alpha_1, \cdots, \alpha_N\}$ that maximizes $D_{FC}$. Note that this decoupling of $\alpha$ into $\alpha_i$ allows us to solve each of the individual problems using the same method as presented in Section IV.

**Theorem 4.** There exists an $N^* \leq N$ such that the elements of the optimal $\alpha$ are given as follows:

$$\alpha_i = \begin{cases} D_{E_i}^*, & \forall i = 1, \cdots, N^* \\ \alpha - \sum_{i=1}^{N^*} D_{E_i}^*, & \text{if } i = N^* + 1 \\ 0, & \text{otherwise.} \end{cases} \quad (31)$$

**Proof:** Having ordered the nodes in terms of decreasing $k_i^*$, we know that node $i$ achieves better tradeoff than node $j$, if $i > j$. This allows us to select nodes with lower indices to achieve the best tradeoffs between detection performance and secrecy until the resource (constraint on Eve, $\alpha$) is completely utilized. The decomposition, the composition of $D_{FC}$, as shown in Equation (30), allows us to sequentially select the individual sensors in an increasing order of indices. Therefore, for index $i = 1$, we allocate $\alpha_1 = D_{E_i}^*$ if $\alpha \geq D_{E_i}^*$. Otherwise, $\alpha_1 = \alpha$.

Having allocated the Eve’s constraint to sensor-1, we move to sensor-2. Now, the remaining tolerable leakage information at the Eve is given by $[\alpha - D_{E_i}^*]_+$, where $[x]_+ = x$ if $x \geq 0$, or, 0 otherwise. Therefore, we solve the problem at sensor-2 with a new constraint $[\alpha - D_{E_i}^*]_+$. As the process of selecting the nodes progresses, we reach a point where $N^*$ sensors are already selected and the remaining resource left, given by $\alpha - \sum_{i=1}^{N^*} D_{E_i}^*$, is less than $D_{E_{N^* + 1}}$. Therefore, we let $\alpha_{N^* + 1} = \alpha - \sum_{i=1}^{N^*} D_{E_i}^*$ and let the remaining sensors sleep in order to secure the confidentiality of the inference task.

Note that Theorem 4  decouples the problem into the design of the individual sensor quantizers separately. Each of these decoupled problems have the same structure as Problem 1. Therefore, each of these decoupled problems can be solved using our proposed algorithm in Section IV.

**VI. Conclusion**

In this paper, we investigated the problem of designing local quantizers for a distributed detection network in the presence of binary symmetric channels and constrained eavesdropper’s performance. First, we investigated the case where the sensors are identical and the channels between the sensors and the FC (likewise, channels between sensors and the Eve) are identical. We proved that the optimal solutions lie on the intersection of the two curves, $D_E = \hat{\alpha}$ and the LRT boundary. In order to find these intersection points, we presented an algorithm to find the two intersection points, which we later compared in terms of the FC’s performance $D_{FC}$. Some numerical results were presented for further discussion on the optimal design of the local quantizers. Furthermore, we also considered the problem of non-identical sensors and channels, where we showed that the problem can be decomposed into $N$ sequential problems, where the decomposition can be achieved through
dynamic programming. In our future work, we will investigate various mitigation schemes that enhance the secrecy of a distributed detection network.

APPENDIX A
PROOF FOR THEOREM 1

To show that $D$ is a convex function of $x$ in the presence of a constraint on Eve, we investigate the second-order differential of $D$ with respect to $x$.

The closed-form expression for the first-order differential of $D$ with respect to $x$

\[ \frac{dD}{dx} = \frac{d}{dx} \left[ x \log \frac{x}{y} + (1-x) \log \left( \frac{1-x}{1-y} \right) \right] \]

(32)

The second-order differential of $D$ can therefore be obtained by differentiating Equation (32) with respect to $x$ as follows.

\[ \frac{d^2D}{dx^2} = \left( \frac{1-x}{1-y} \right) \frac{dy}{dx} \left[ \log \left( \frac{1-x}{1-y} \right) \right] \]

(33)

Substituting Equation (22) from the Lemma 4 in Equation (33), we have

\[ \frac{d^2D}{dx^2} = \frac{y(1-y)}{(1-y)2} \left( \frac{dy}{dx} \right)^2 + \frac{1}{xy} \left( \frac{dx}{dy} \right) \]

(34)

Substituting Equation (22) from the Lemma 4 in Equation (34), and using this in Equation (33), we have

\[ \frac{d^2D}{dx^2} = T_1 \left( \frac{dy}{dx} \right)^2 - 2T_2 \frac{dy}{dx} + T_3 \]

(35)

where

\[ T_1 = \left( \frac{1-x}{y^2} + \frac{x}{y^2} \right) - \frac{\hat{y}(1-\hat{y})}{y(1-y)} \left( \frac{1-\hat{x}}{1-\hat{y}} + \frac{\hat{x}}{\hat{y}} \right) \]

(36a)

\[ T_2 = \left( \frac{1}{y} + \frac{1}{1-y} \right) - \frac{\hat{y}(1-\hat{y})}{y(1-y)} \left( \frac{1}{y} + \frac{1}{1-y} \right) \]

(36b)

\[ T_3 = \left( \frac{1}{x} + \frac{1}{1-x} \right) - \frac{\hat{y}(1-\hat{y})}{y(1-y)} \left( \frac{1}{\hat{x}} + \frac{1}{1-\hat{x}} \right) \]

(36c)

It is easy to show that $T_2 = 0$.

So, let us first consider $T_1$. Expanding Equation (36a) we have

\[ T_1 = \frac{1}{y^2(1-y)^2} \left[ (x\hat{y} - \hat{x}y) - (xy^2 - \hat{x}y^2) \right] + y\hat{y} \left[ (y - \hat{y}) - 2(x - \hat{x}) + 2(x\hat{y} - \hat{x}y) \right] \]

(37)

\[ = \frac{1}{y^2(1-y)^2} \left[ -\rho(y - x) \right] - \left\{ \rho^2 x - \rho y^2 + 2\rho(1-2\rho)xy - 2\rho(1-2\rho)xy^2 \right\} + y\hat{y}(\rho - 2\rho x) \]

(38)

\[ = \frac{\rho(1-\rho)(y - x)(2y - 1)}{y^2(1-y)^2} \]

Similarly, expanding Equation (36a) for $T_3$, we have

\[ T_3 = \frac{1}{y(1-y)} \left[ \frac{y(1-y)}{x(1-x)} - \frac{\hat{y}(1-\hat{y})}{\hat{x}(1-\hat{x})} \right] \]

(39)

Substituting Equations (37) and (38) in Equation (35), we have

\[ \frac{d^2D}{dx^2} = \frac{\rho(1-\rho)(y - x)}{y(1-y)} \cdot T_4 \]

(40)

where

\[ T_4 = \frac{2y - 1}{y\hat{y}(1-y)(1-\hat{y})} \left( \frac{dy}{dx} \right)^2 + \frac{1}{x\hat{x}(1-x)(1-\hat{x})} \]

(41)

Since we are interested in the region where $y \geq x$ and $\rho < \frac{1}{2}$, the convexity properties of $D$ with respect to $x$ is decided by the sign of $T_4$. In order to analyse the sign of $T_4$, we divide the achievable region in the receiver-operating characteristics into three regions, as shown in Figure 9

\[ \mathcal{R}_1: \left( \frac{y}{2} \right) \& (x + y \leq 1) \]

(42)

\[ \mathcal{R}_2: \left( \frac{y}{2} \leq \frac{1}{2} \right) \& (x + y \leq 1) \]

(43)

\[ \mathcal{R}_3: \left( \frac{y}{2} \geq \frac{1}{2} \right) \& (x + y \geq 1) \]

(44)

Obviously, in region $\mathcal{R}_2$, $2y - 1 \geq 0$ and $1 - x - y \geq 0$. Therefore, $\frac{d^2D}{dx^2} \geq 0$. Henceforth, we analyse the sign of $T_4$ in the remaining regions $\mathcal{R}_1$ and $\mathcal{R}_3$.

Region $\mathcal{R}_1$: In this region, $2y - 1 \leq 0$. Therefore, we use the upper bound on $\frac{dy}{dx}$, presented in Equation (23), to find the sign of $T_4$ as follows.
Substituting Equation (23) in Equation (40), we have
\[
T_4 \geq \frac{1 - x - y}{x\hat{x}(1 - x)(1 - \hat{x})} - \frac{1 - 2\rho}{y\hat{y}(1 - y)(1 - \hat{y})} \frac{y\hat{y}}{x\hat{x}}
\]
\[
= \frac{1}{x\hat{x}(1 - x)(1 - \hat{x})(1 - y)(1 - \hat{y})} [(1 - x - y)(1 - \hat{y}) - \frac{(2 - 1)(1 - x) - y^2}{x\hat{x}(1 - x)(1 - y)(1 - \hat{y})}] + y(1 - x)(1 - \hat{x})
\]
Equation (42) can be lower-bounded as follows.
\[
T_4 \geq \frac{(y - x)}{x\hat{x}(1 - x)(1 - y)(1 - \hat{y})} \left[ y(1 - \rho) + (1 - 2\rho) \left\{ (2y - 1)(1 - x) - y^2 \right\} \right]
\]
Since \(1 - x - y \geq 0\) in region \(R_1\), we have \(1 - x \geq y\). Therefore, substituting this inequality in Equation (43), we have
\[
T_4 \geq \frac{(y - x)}{x\hat{x}(1 - x)(1 - y)(1 - \hat{y})} \left[ y(1 - \rho) + (1 - 2\rho) \left\{ (2y - 1)(1 - x) - y^2 \right\} \right]
\]
\[
= \frac{(y - x)[(1 - \rho) + (1 - 2\rho)(y - 1)]}{x\hat{x}(1 - x)(1 - \hat{x})(1 - y)(1 - \hat{y})}
\]
\[
= \frac{(y - x)[(1 - \rho) + (1 - 2\rho)(y - 1)]}{x\hat{x}(1 - x)(1 - \hat{x})(1 - y)(1 - \hat{y})}
\]
\[
\geq 0.
\]
Region \(R_3\): In this region, since \(2y - 1 \geq 0\), we use the lower bound on \(\frac{dy}{dx}\), presented in Equation (23), in order to find the sign of \(T_4\).

Substituting Equation (23) in Equation (40), we have
\[
T_4 \geq \frac{2y - 1}{y\hat{y}(1 - y)(1 - \hat{y})(1 - x)(1 - \hat{x})} - \frac{x + y - 1}{x\hat{x}(1 - x)(1 - \hat{x})}
\]
\[
= \frac{1}{(1 - x)(1 - \hat{x})} \left[ \frac{2y - 1}{y\hat{y}} \right] - \frac{x + y - 1}{x\hat{x}}
\]
\[
= \frac{(y\hat{y} - x\hat{y}) - y(y\hat{y} - x\hat{y}) - xy(\hat{y} - \hat{x})}{x\hat{y}\hat{y}(1 - x)(1 - \hat{x})}
\]
\[
= \frac{1}{x\hat{y}\hat{y}(1 - x)(1 - \hat{x})} [(1 - y) \{ \rho(y - x) 
\]
\[
+ (1 - 2\rho)(y^2 - x^2) \} - xy(1 - 2\rho)(y - x) \]
\[
= \frac{1}{x\hat{y}\hat{y}(1 - x)(1 - \hat{x})} [(1 - y) \{ \rho(y - x) 
\]
\[
+ (1 - 2\rho)(y - x)(1 - 2\rho) - (1 - 2\rho)x(1 - 2\rho) \} \]
\[
\geq 0.
\] (46)

Hence, for BSCs with \(\rho < \frac{1}{2}\), \(D\) is a convex function of \(x\) along the constraint \(D_E = \alpha\).

REFERENCES

[1] A. Swami, Q. Zhao, Y.-W. Hong, and L. Tong, Wireless Sensor Networks: Signal Processing and Communications. U.S.A: John Wiley & Sons Ltd., 2007.
[2] R. Viswanathan and P. K. Varshney, “Distributed detection with multiple sensors i. fundamentals,” Proc. IEEE, vol. 85, no. 1, pp. 54–63, 1997.
[3] R. S. Blum, S. A. Kassam, and H. V. Poor, “Distributed detection with multiple sensors ii. advanced topics,” Proc. IEEE, vol. 85, no. 1, pp. 64–79, 1997.
[4] P. K. Varshney, Distributed Detection and Data Fusion. Springer, New York, 1997.
[5] J.-F. Chamberland and V. V. Veeravalli, “Decentralized detection in sensor networks,” IEEE Trans. Signal Process., vol. 51, no. 2, pp. 407–416, 2003.
[6] J. Tatsiklis and M. Athans, “On the complexity of decentralized decision making and detection problems,” IEEE Transactions on Automatic Control, vol. 30, no. 5, pp. 440–446, May 1985.
[7] Z. Chair and P. Varshney, “Optimal data fusion in multiple sensor detection systems,” Aerospace and Electronic Systems, IEEE Transactions on Automatic Control, vol. AES-22, no. 1, pp. 98–101, Jan 1986.
[8] J. Tatsiklis, “On threshold rules in decentralized detection,” in Decision and Control, 1986 25th IEEE Conference on, Dec 1986, pp. 232–236.
[9] ———, “Extremal properties of likelihood-ratio quantizers,” Communications, IEEE Transactions on, vol. 41, no. 4, pp. 550–558, Apr 1993.
[10] T. C. Aysal and K. E. Barner, “Sensor data cryptography in wireless sensor networks,” IEEE Trans. Inf. Forensics Security, vol. 3, no. 2, pp. 273–289, 2008.
[11] V. S. S. Nandendla, “Secure distributed detection in wireless sensor networks via encryption of sensor decisions,” Master’s thesis, Louisiana State University, 2009.
[12] H. Jeon, S. W. McLaughlin, and J. Ha, “Cooperative secure transmission for distributed detection in wireless sensor networks,” in Proc. IEEE 54th Int Circuits and Systems (MWSCAS) Midwest Symp, 2011, pp. 1–4.

[13] S. Marano, V. Matta, and P. K. Willett, “Distributed detection with censoring sensors under physical layer secrecy,” IEEE Trans. Signal Process., vol. 57, no. 5, pp. 1976–1986, May 2009.

[14] V. S. S. Nadendla, H. Chen, and P. K. Varshney, “Secure distributed detection in the presence of eavesdroppers,” in Proc. Conf Signals, Systems and Computers (ASILOMAR) Record of the Forty Fourth Asilomar Conf, 2010, pp. 1437–1441.

[15] R. T. Rockafellar, Convex Analysis, ser. Princeton Landmarks in Mathematics and Physics. Princeton University Press, 1996.

[16] C. B. Barber, D. P. Dobkin, and H. Huhdanpaa, “The quickhull algorithm for convex hulls,” ACM Trans. Math. Softw., vol. 22, no. 4, pp. 469–483, Dec. 1996. [Online]. Available: http://doi.acm.org/10.1145/235815.235821

[17] S. P. Boyd and L. Vandenberghe, Convex Optimization. Cambridge University Press, 2004.

[18] R. Bellman, Dynamic Programming. Dover Publications, 2003.