TANDEM DISTRIBUTED BAYESIAN DETECTION WITH PRIVACY CONSTRAINTS

Zuxing Li and Tobias J. Oechtering

School of Electrical Engineering and the ACCESS Linnaeus Centre
KTH Royal Institute of Technology, Stockholm, Sweden

ABSTRACT

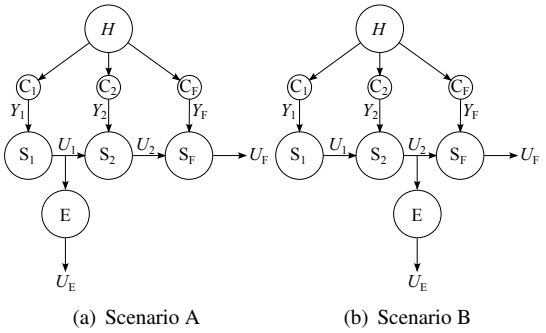
In this paper, the privacy problem of a tandem distributed detection system vulnerable to an eavesdropper is proposed and studied in the Bayesian formulation. The privacy risk is evaluated by the detection cost of the eavesdropper which is assumed to be informed and greedy. For the sensors whose operations are constrained to suppress the privacy risk, it is shown that the optimal detection strategies are likelihood-ratio tests. This fundamental insight allows for the optimization to reuse known algorithms extended to incorporate the privacy constraint. The trade-off between the detection performance and privacy risk is illustrated in an example.

Index Terms— Likelihood-ratio test, person-by-person optimization, physical-layer security

1. INTRODUCTION

Because of their wide-range of applications, sensor networks have attracted much attention recently. Although a large number of fruitful studies have been done, there are still some challenges in the development of sensor network technologies. Among them, the privacy problem strongly influences users' acceptance of some sensor network applications, e.g., for health monitoring. In face of multiple privacy threats [1], many efforts have been made to design secure sensor networks, e.g., protecting the confidential data by cryptography [2], attack detection approaches in the centralized and neighbors' cooperative ways [3, 4], and routing security based on reputation-based scheme [5] and broadcast authentication [6]. Recently, a novel idea has been proposed to take the privacy issue into account in the design of physical-layer distributed detection. In [7], Byzantine attacks in distributed detections were discussed in the game-theoretic framework. In [8], the eavesdropper was assumed to be interested in the data transmission state of the system. However, an eavesdropper in practice can be more aggressive. In [9], the privacy risk was assessed by an entropy-based metric to measure the difference between Kullback-Leibler distances of the fusion node and eavesdropper.

In this work, we propose a detection-operational privacy metric and study the tandem distributed Bayesian detection problem subject to a physical-layer privacy constraint in the privacy-utility framework. Related problems in a parallel distributed detection system and with the Neyman-Pearson criterion are studied in [10, 11]. From a broader perspective, privacy-utility problems have been discussed in many other fields. The differential privacy problem [12] and conic privacy problem [13] are studied to guarantee the statistic privacy by sanitizing mechanisms. Information-theoretic tools are used in [14, 15].



(a) Scenario A (b) Scenario B

Fig. 1. The studied system model consists of a binary hypothesis H, three independent sensing channels C_1, C_2, and C_F, three sensors S_1, S_2, and S_F which make binary decisions U_1, U_2, and U_F (the final decision) based on their observations Y_1, (U_1, Y_2), and (U_2, Y_F) independently, and an eavesdropper E which intercepts the decision U_1 (Scenario A) or U_2 (Scenario B) and makes its decision U_E.

2. TANDEM DISTRIBUTED DETECTION WITH AN EAVESDROPPER

As shown in Figure 1, the studied system consists of a binary-hypothesis phenomenon H with known prior probabilities $p_H(0)$ and $p_H(1)$, three tandem-connected sensors S_1, S_2, and S_F (the fusion node), and an eavesdropper E. For $i \in \{1, 2, \mathrm{F}\}$, each sensor makes a binary decision U_i based on the decision of the previous sensor (if available) and an observation Y_i which is corrupted by the sensing channel C_i. We assume that sensing channels are independent and their likelihood ratios contain no point masses of probability. The eavesdropper E is supposed to overhear the link $\mathrm{S}_1 - \mathrm{S}_2$ (Scenario A) or $\mathrm{S}_2 - \mathrm{S}_\mathrm{F}$ (Scenario B) and to make its own binary

978-1-4799-2893-4/14/$31.00 ©2014 IEEE

Table 1. Detection rule candidates of the eavesdropper.

	u_{E}			
u_1 or u_2	Φ_{E}^1	Φ_{E}^2	Φ_{E}^3	Φ_{E}^4
0	0	1	0	1
1	0	1	1	0

decision U_{E} based on the local decision U_1 or U_2. Detection and fusion tests of sensors, fusion node, and eavesdropper are functions of their own observations and are denoted by $\Phi_1(y_1)$, $\Phi_2(u_1, y_2)$, $\Phi_{\mathrm{F}}(u_2, y_{\mathrm{F}})$, and $\Phi_{\mathrm{E}}(u_i)$, $i = 1$ or 2. Since Φ_{E}'s input and output are binary variables, it has four candidates as listed in Table 1. In this work, we assume that the eavesdropper is *informed* and *greedy*, i.e., the eavesdropper has a full knowledge of the distributed detection system and always employs the best detection strategy which causes the worst privacy problem.

3. DISTRIBUTED BAYESIAN DETECTION

Denote the detection cost of the fusion node to make a decision u_{F} given the hypothesis realization h by $c_{U_{\mathrm{F}},H}(u_{\mathrm{F}}, h)$ and assume that $c_{U_{\mathrm{F}},H}(u_{\mathrm{F}}, h)|_{u_{\mathrm{F}}\neq h} > c_{U_{\mathrm{F}},H}(u_{\mathrm{F}}, h)|_{u_{\mathrm{F}}=h} \geq 0$. The average detection cost of making a fusion decision is expressed as $c_{\mathrm{F}} = \sum_{u_{\mathrm{F}},h} p_{U_{\mathrm{F}},H}(u_{\mathrm{F}}, h) c_{U_{\mathrm{F}},H}(u_{\mathrm{F}}, h)$. The distributed Bayesian detection problem aims to design the optimal system which minimizes c_{F} and consists of detection and fusion tests Φ_1^*, Φ_2^*, and Φ_{F}^*:

$$\min_{\Phi_1,\Phi_2,\Phi_{\mathrm{F}}} c_{\mathrm{F}}. \tag{1}$$

The method of person-by-person optimization (PBPO) [16] has been used as an indirect method to approach Φ_1^*, Φ_2^*, and Φ_{F}^* by iteratively refining local person-by-person optimal tests Φ_1^Δ, Φ_2^Δ, and Φ_{F}^Δ.

According to [17, Section 4.2], given Φ_2 and Φ_{F}, c_{F} can be rewritten as

$$c_{\mathrm{F}} = c_1 + a_1 p_1^{\mathrm{F}} - b_1 p_1^{\mathrm{D}}, \tag{2}$$

where a_1, b_1, and c_1 are constant coefficients determined by Φ_2 and Φ_{F}; the false alarm and detection probabilities are defined as $p_1^{\mathrm{F}} = p_{U_1|H}(1|0)$ and $p_1^{\mathrm{D}} = p_{U_1|H}(1|1)$ respectively. Then Φ_1^Δ can be a likelihood-ratio test (LRT). We can conclude that it is sufficient to consider a LRT for Φ_1^*.

Let $i, j \in \{2, \mathrm{F}\}$ with $i \neq j$. Denote the previous node of S_i as S_k. When Φ_1 and Φ_j are fixed, c_{F} can be rewritten as

$$c_{\mathrm{F}} = c_i + a_i p_{i|u_k=0}^{\mathrm{F}} - b_i p_{i|u_k=0}^{\mathrm{D}} + c_i' + a_i' p_{i|u_k=1}^{\mathrm{F}} - b_i' p_{i|u_k=1}^{\mathrm{D}}, \tag{3}$$

where constants a_i, b_i, c_i, a_i', b_i', and c_i' are determined by the given Φ_1 and Φ_j; the conditional false alarm and detection probabilities are defined as $p_{i|u_k=0}^{\mathrm{F}} = p_{U_i|U_k,H}(1|0,0)$, $p_{i|u_k=0}^{\mathrm{D}} = p_{U_i|U_k,H}(1|0,1)$, $p_{i|u_k=1}^{\mathrm{F}} = p_{U_i|U_k,H}(1|1,0)$, and $p_{i|u_k=1}^{\mathrm{D}} = p_{U_i|U_k,H}(1|1,1)$. With different observations of u_k, $\Phi_i^\Delta(0, y_i)$ and $\Phi_i^\Delta(1, y_i)$ can be solved independently as LRTs. Therefore, it is sufficient to consider LRTs for Φ_2^Δ, Φ_{F}^Δ, Φ_2^*, and Φ_{F}^*.

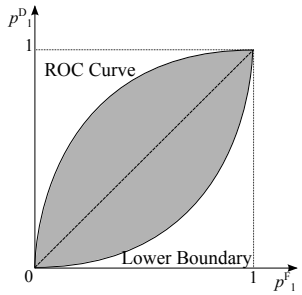


Fig. 2. Illustration of a typical operation region $\mathcal{R}_1$.

Any detection test $\Phi_1(y_1)$, $\Phi_2(0, y_2)$, $\Phi_2(1, y_2)$, $\Phi_{\mathrm{F}}(0, y_{\mathrm{F}})$, or $\Phi_{\mathrm{F}}(1, y_{\mathrm{F}})$ can be represented as an operation point $(p_1^{\mathrm{F}}, p_1^{\mathrm{D}})$, $(p_{2|u_1=0}^{\mathrm{F}}, p_{2|u_1=0}^{\mathrm{D}})$, $(p_{2|u_1=1}^{\mathrm{F}}, p_{2|u_1=1}^{\mathrm{D}})$, $(p_{\mathrm{F}|u_2=0}^{\mathrm{F}}, p_{\mathrm{F}|u_2=0}^{\mathrm{D}})$, or $(p_{\mathrm{F}|u_2=1}^{\mathrm{F}}, p_{\mathrm{F}|u_2=1}^{\mathrm{D}})$ in the (conditional) operation region $\mathcal{R}_1$, $\mathcal{R}_{2|u_1=0}$, $\mathcal{R}_{2|u_1=1}$, $\mathcal{R}_{\mathrm{F}|u_2=0}$, or $\mathcal{R}_{\mathrm{F}|u_2=1}$. All (conditional) operation regions have the properties:

1. A (conditional) operation region is a convex set whose upper and lower boundaries are point symmetric with respect to $(0.5, 0.5)$ and intersect at $(0, 0)$ and $(1, 1)$.
2. Points on upper and lower boundaries represent LRTs.
3. The upper boundary, also known as the receiver operating characteristics (ROC) curve, is increasing, concave, and above the line of equal (conditional) false alarm and detection probabilities [18, Chapter 2].

4. PRIVACY IN DISTRIBUTED BAYESIAN DETECTION

Due to the space limitation, we will first focus on Scenario B and then give results about Scenario A directly.

4.1. Privacy Metric

The eavesdropper is assumed to be informed of the distributed detection system and curious about the binary hypothesis. In this work, we consider a Bayesian scenario where the eavesdropper minimizes its average detection cost by manipulating the local detection rule candidates listed in Table 1. Then, the privacy metric in this distributed Bayesian detection problem is the minimum average detection cost of the eavesdropper,

$$c_{\mathrm{E}}^{\min} = \min_{i\in\{1,2,3,4\}} c_{\mathrm{E}}^i, \tag{4}$$

where c_{E}^i represents the average detection cost when Φ_{E}^i is employed. A higher $c_{\mathrm{E}}^{\min}$ indicates a more secure detection system, and vice versa. Similarly, denote the detection

cost of the eavesdropper to make a decision u_{E} given the hypothesis realization h as $c_{U_{\mathrm{E}},H}(u_{\mathrm{E}},h)$ and assume that $c_{U_{\mathrm{E}},H}(u_{\mathrm{E}},h)|_{u_{\mathrm{E}}\neq h} > c_{U_{\mathrm{E}},H}(u_{\mathrm{E}},h)|_{u_{\mathrm{E}}=h} \geq 0$. Then,

$$\begin{aligned}
c_{\mathrm{E}}^1 &= p_H(0)c_{U_{\mathrm{E}},H}(0,0) + p_H(1)c_{U_{\mathrm{E}},H}(0,1),\\
c_{\mathrm{E}}^2 &= p_H(0)c_{U_{\mathrm{E}},H}(1,0) + p_H(1)c_{U_{\mathrm{E}},H}(1,1),\\
c_{\mathrm{E}}^3 &= +p_{2|u_1=0}^{\mathrm{F}}(1-p_1^{\mathrm{F}})p_H(0)\{c_{U_{\mathrm{E}},H}(1,0) - c_{U_{\mathrm{E}},H}(0,0)\}\\
&\quad - p_{2|u_1=0}^{\mathrm{D}}(1-p_1^{\mathrm{D}})p_H(1)\{c_{U_{\mathrm{E}},H}(0,1) - c_{U_{\mathrm{E}},H}(1,1)\}\\
&\quad + p_{2|u_1=1}^{\mathrm{F}}p_1^{\mathrm{F}}p_H(0)\{c_{U_{\mathrm{E}},H}(1,0) - c_{U_{\mathrm{E}},H}(0,0)\}\\
&\quad - p_{2|u_1=1}^{\mathrm{D}}p_1^{\mathrm{D}}p_H(1)\{c_{U_{\mathrm{E}},H}(0,1) - c_{U_{\mathrm{E}},H}(1,1)\} + c_{\mathrm{E}}^1\\
c_{\mathrm{E}}^4 &= c_{\mathrm{E}}^1 + c_{\mathrm{E}}^2 - c_{\mathrm{E}}^3.
\end{aligned} \tag{5}$$

The first two terms in (5) are constants and lead to the upper bound of the privacy metric that $c_{\mathrm{E}}^{\min} \leq \min\{c_{\mathrm{E}}^1, c_{\mathrm{E}}^2\}$.

4.2. Privacy-Constrained Distributed Bayesian Detection

Next, we take the threat of the eavesdropper into account. The privacy-constrained distributed Bayesian detection problem is formulated as

$$\begin{aligned}
&\min_{\Phi_1,\Phi_2,\Phi_{\mathrm{F}}} c_{\mathrm{F}},\\
&\text{s.t.}\quad c_{\mathrm{E}}^{\min} \geq \beta.
\end{aligned} \tag{6}$$

Similar to the problem (1), the privacy-constrained problem aims to find the optimal distributed detection design with the minimum c_{F}. The condition $c_{\mathrm{E}}^{\min} \geq \beta$ guarantees the privacy of the obtained design. Because of the upper bound of $c_{\mathrm{E}}^{\min}$, this privacy-constrained problem is feasible only if $\beta \leq \min\{c_{\mathrm{E}}^1, c_{\mathrm{E}}^2\}$. Notice that the condition $c_{\mathrm{E}}^{\min} \geq \beta$ is equivalent to $c_{\mathrm{E}}^i \geq \beta, \forall i$. By substituting terms in (5) into this equivalent condition, the privacy-constrained optimization problem can be rewritten as

$$\begin{aligned}
&\min_{\Phi_1,\Phi_2,\Phi_{\mathrm{F}}} c_{\mathrm{F}},\\
&\text{s.t.}\quad c_{\mathrm{E}}^1, c_{\mathrm{E}}^2 \geq \beta \Rightarrow \beta \leq c_{\mathrm{E}}^1 \leq c_{\mathrm{E}}^1 + c_{\mathrm{E}}^2 - \beta,\\
&\qquad c_{\mathrm{E}}^3, c_{\mathrm{E}}^4 \geq \beta \Rightarrow \beta \leq c_{\mathrm{E}}^3 \leq c_{\mathrm{E}}^1 + c_{\mathrm{E}}^2 - \beta.
\end{aligned} \tag{7}$$

Denote detection and fusion tests of the optimal privacy-constrained tandem distributed detection system by $\Phi_1^{\#}$, $\Phi_2^{\#}$, and $\Phi_{\mathrm{F}}^{\#}$. For $i \in \{1, 2, \mathrm{F}\}$, some properties of $\Phi_i^{\#}$ can be derived by studying its corresponding local person-by-person optimal test $\Phi_i^{\square}$.

Remark 1. *Since the operation of* $\mathrm{S_F}$ *is not constrained, the conclusion of it remains the same, i.e., it is sufficient to consider LRTs for* $\Phi_{\mathrm{F}}^{\square}$ *and* $\Phi_{\mathrm{F}}^{\#}$.

When Φ_2 and Φ_{F} are fixed, the privacy-constrained operation region $\mathcal{R}_1^{\mathrm{P}}$ is the available region in $\mathcal{R}_1$ confined by $\beta \leq c_{\mathrm{E}}^3 \leq c_{\mathrm{E}}^1 + c_{\mathrm{E}}^2 - \beta$. Such a condition, when substituting c_{E}^3 by the function of p_1^{F} and p_1^{D} shown in (5), can be rewritten as parallel linear constraints:

$$g_1 p_1^{\mathrm{F}} + \theta_1^{\mathrm{L}} \leq p_1^{\mathrm{D}} \leq g_1 p_1^{\mathrm{F}} + \theta_1^{\mathrm{U}}, \tag{8}$$

where the constant coefficients g_1, θ_1^{L}, and θ_1^{U} are determined by Φ_2. Then the optimization of Φ_1 (or the equivalent operation point $(p_1^{\mathrm{F}}, p_1^{\mathrm{D}})$) to minimize c_{F} reduces to

$$\min_{\mathcal{R}_1^{\mathrm{P}}} c_{\mathrm{F}}. \tag{9}$$

Lemma 1. *It is sufficient to consider LRTs for* $\Phi_1^{\square}$ *and* $\Phi_1^{\#}$.

Proof. Define a set $\mathcal{L}_1(\theta_1)$ and its subset $\mathcal{I}_1(\theta_1)$ as

$$\begin{aligned}
\mathcal{L}_1(\theta_1) &= \{(p_1^{\mathrm{F}}, p_1^{\mathrm{D}}) : p_1^{\mathrm{D}} = g_1 p_1^{\mathrm{F}} + \theta_1\} \cap \mathcal{R}_1,\\
\mathcal{I}_1(\theta_1) &= \{(p_1^{\mathrm{F}}, p_1^{\mathrm{D}}) : p_1^{\mathrm{D}} = g_1 p_1^{\mathrm{F}} + \theta_1\} \cap \partial\mathcal{R}_1,
\end{aligned} \tag{10}$$

where $\partial\mathcal{R}_1$ denotes the boundary of $\mathcal{R}_1$. Then, we have $\mathcal{R}_1^{\mathrm{P}} = \bigcup_{\theta_1^{\mathrm{L}} \leq \theta_1 \leq \theta_1^{\mathrm{U}}} \mathcal{L}_1(\theta_1)$. The optimization problem in (9) can be rewritten as

$$\min_{\theta_1^{\mathrm{L}} \leq \theta_1 \leq \theta_1^{\mathrm{U}}} \min_{\mathcal{L}_1(\theta_1)} c_{\mathrm{F}}. \tag{11}$$

Given any $\theta_1 \in [\theta_1^{\mathrm{L}}, \theta_1^{\mathrm{U}}]$, we focus on the inner optimization. By substituting c_{F} by the function of p_1^{F} and p_1^{D} shown in (2), the inner optimization can be rewritten as

$$\min_{\mathcal{L}_1(\theta_1)} c_1 + a_1 p_1^{\mathrm{F}} - b_1 p_1^{\mathrm{D}}. \tag{12}$$

Since $\mathcal{R}_1$ is a convex set, there are at most two elements in $\mathcal{I}_1(\theta_1)$ which are the intersection points of the line $p_1^{\mathrm{D}} = g_1 p_1^{\mathrm{F}} + \theta_1$ with $\partial\mathcal{R}_1$. Let us discuss the optimization of (12) in different cases:

1. If $\mathcal{I}_1(\theta_1) = \emptyset$, $\mathcal{L}_1(\theta_1) = \emptyset$.
2. If $\mathcal{I}_1(\theta_1)$ is a singleton consisting of only one intersection point, $\mathcal{L}_1(\theta_1) = \mathcal{I}_1(\theta_1)$ and the single intersection point is the optimal operation point.
3. If there are two intersection points in $\mathcal{I}_1(\theta_1)$, $\mathcal{L}_1(\theta_1)$ is a line segment between the two intersection points. By substituting $p_1^{\mathrm{D}} = g_1 p_1^{\mathrm{F}} + \theta_1$ in (12), the inner optimization problem becomes

$$\min_{\mathcal{L}_1(\theta_1)} c_1 - b_1\theta_1 + (a_1 - b_1 g_1)p_1^{\mathrm{F}}. \tag{13}$$

   In this case, the optimal point in $\mathcal{L}_1(\theta_1)$ is the point with the maximum or minimum p_1^{F} which corresponds to one of the two intersection points in $\mathcal{I}_1(\theta_1)$.

Therefore, the optimal point in any non-empty $\mathcal{L}_1(\theta_1)$, $\theta_1 \in [\theta_1^{\mathrm{L}}, \theta_1^{\mathrm{U}}]$, is an intersection point in $\mathcal{I}_1(\theta_1)$. Since points on the boundary of $\mathcal{R}_1$ represent LRTs, the optimal operation point in any non-empty $\mathcal{L}_1(\theta_1)$ can represent a LRT. All solution candidates of the outer optimization in (11) can be LRTs. Thus, it is sufficient to consider LRTs for $\Phi_1^{\square}$ and $\Phi_1^{\#}$. □

When Φ_1 and Φ_{F} are fixed, $\Phi_2^{\square}$ consists of jointly optimal $\Phi_2^{\square}(0, y_2)$ and $\Phi_2^{\square}(1, y_2)$ which are coupled through the privacy constraint $\beta \leq c_{\mathrm{E}}^3 \leq c_{\mathrm{E}}^1 + c_{\mathrm{E}}^2 - \beta$. When substituting

c_{E}^3 by the function of $p_{2|u_1=0}^{\mathrm{F}}$, $p_{2|u_1=0}^{\mathrm{D}}$, $p_{2|u_1=1}^{\mathrm{F}}$, and $p_{2|u_1=1}^{\mathrm{D}}$ shown in (5), the privacy constraint can be rewritten as:

$$\begin{aligned} f_2 p_{2|u_1=0}^{\mathrm{F}} - h_2 p_{2|u_1=0}^{\mathrm{D}} + f_2' p_{2|u_1=1}^{\mathrm{F}} - h_2' p_{2|u_1=1}^{\mathrm{D}} &\geq \beta - c_{\mathrm{E}}^1, \\ f_2 p_{2|u_1=0}^{\mathrm{F}} - h_2 p_{2|u_1=0}^{\mathrm{D}} + f_2' p_{2|u_1=1}^{\mathrm{F}} - h_2' p_{2|u_1=1}^{\mathrm{D}} &\leq c_{\mathrm{E}}^2 - \beta, \end{aligned} \tag{14}$$

where the constant coefficients f_2, f_2', h_2, and h_2' are determined by Φ_1. Define the joint privacy-constrained operation region $\mathcal{R}_2^{\mathrm{P}}$ as a set of $\Big((p_{2|u_1=0}^{\mathrm{F}}, p_{2|u_1=0}^{\mathrm{D}}), (p_{2|u_1=1}^{\mathrm{F}}, p_{2|u_1=1}^{\mathrm{D}})\Big)$ where $(p_{2|u_1=0}^{\mathrm{F}}, p_{2|u_1=0}^{\mathrm{D}}) \in \mathcal{R}_{2|u_1=0}$, $(p_{2|u_1=1}^{\mathrm{F}}, p_{2|u_1=1}^{\mathrm{D}}) \in \mathcal{R}_{2|u_1=1}$, and they jointly satisfy the privacy constraint in (14). Then the optimization of Φ_2 to minimize c_{F} reduces to

$$\min_{\mathcal{R}_2^{\mathrm{P}}} c_{\mathrm{F}}. \tag{15}$$

Lemma 2. *It is sufficient to consider LRTs for $\Phi_2^{\square}$ and $\Phi_2^{\#}$.*

Proof. Define $l_2(d_2)$, $l_2'(d_2')$, $\mathcal{L}_2(d_2)$, $\mathcal{L}_2'(d_2')$, and $\mathcal{C}_2(d_2, d_2')$:

$$\begin{aligned} l_2(d_2) &= \{(p_{2|u_1=0}^{\mathrm{F}}, p_{2|u_1=0}^{\mathrm{D}}) : f_2 p_{2|u_1=0}^{\mathrm{F}} - h_2 p_{2|u_1=0}^{\mathrm{D}} = d_2\}, \\ l_2'(d_2') &= \{(p_{2|u_1=1}^{\mathrm{F}}, p_{2|u_1=1}^{\mathrm{D}}) : f_2' p_{2|u_1=1}^{\mathrm{F}} - h_2' p_{2|u_1=1}^{\mathrm{D}} = d_2'\}, \\ \mathcal{L}_2(d_2) &= l_2(d_2) \cap \mathcal{R}_{2|u_1=0},\ \mathcal{L}_2'(d_2') = l_2'(d_2') \cap \mathcal{R}_{2|u_1=1}, \\ \mathcal{C}_2(d_2, d_2') &= \mathcal{L}_2(d_2) \times \mathcal{L}_2'(d_2'). \end{aligned} \tag{16}$$

We can express $\mathcal{R}_2^{\mathrm{P}} = \bigcup_{\beta - c_{\mathrm{E}}^1 \leq d_2 + d_2' \leq c_{\mathrm{E}}^2 - \beta} \mathcal{C}_2(d_2, d_2')$. The optimization problem in (15) can be rewritten as

$$\min_{\beta - c_{\mathrm{E}}^1 \leq d_2 + d_2' \leq c_{\mathrm{E}}^2 - \beta} \ \min_{\mathcal{C}_2(d_2, d_2')} c_{\mathrm{F}}. \tag{17}$$

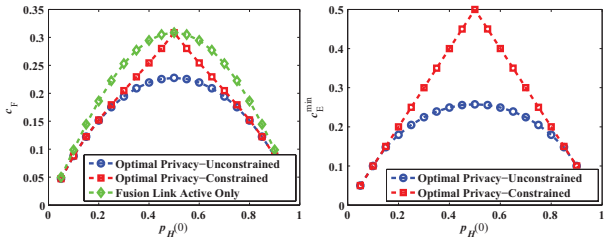
Given any (d_2, d_2') which satisfies $\beta - c_{\mathrm{E}}^1 \leq d_2 + d_2' \leq c_{\mathrm{E}}^2 - \beta$, we again focus on the inner optimization. By substituting c_{F} by the function of $p_{2|u_1=0}^{\mathrm{F}}$, $p_{2|u_1=0}^{\mathrm{D}}$, $p_{2|u_1=1}^{\mathrm{F}}$, and $p_{2|u_1=1}^{\mathrm{D}}$ shown in (3), the inner optimization can be divided into two independent optimization problems as

$$\begin{aligned} &\min_{\mathcal{L}_2(d_2)} c_2 + a_2 p_{2|u_1=0}^{\mathrm{F}} - b_2 p_{2|u_1=0}^{\mathrm{D}}, \\ &\min_{\mathcal{L}_2'(d_2')} c_2' + a_2' p_{2|u_1=1}^{\mathrm{F}} - b_2' p_{2|u_1=1}^{\mathrm{D}}. \end{aligned} \tag{18}$$

Following a similar proof as Lemma 1, the optimal point combination in any non-empty $\mathcal{C}_2(d_2, d_2')$ can be a combination of two LRTs. That means all solution candidates of the outer optimization in (17) can be combinations of LRTs. Therefore, it is sufficient to consider LRTs for $\Phi_2^{\square}(0, y_2)$, $\Phi_2^{\square}(1, y_2)$, $\Phi_2^{\square}$, and $\Phi_2^{\#}$. □

Theorem 1. *When U_2 is intercepted by the eavesdropper, it is sufficient to consider LRTs for $\Phi_1^{\#}$, $\Phi_2^{\#}$, and $\Phi_{\mathrm{F}}^{\#}$.*

Theorem 1 is a summary of Remark 1 and Lemmas 1-2. When the local decision U_1 is intercepted by the eavesdropper, another privacy-constrained tandem distributed Bayesian detection problem can be formulated. Following a similar analysis, we can obtain the same conclusion as



(a) Comparison of c_{F} (b) Comparison of $c_{\mathrm{E}}^{\min}$

Fig. 3. The enhancement of privacy (higher $c_{\mathrm{E}}^{\min}$) is at the cost of degeneration of detection performance (higher c_{F}). The optimal privacy-constrained design has a better performance than the design which has only the fusion link $H - \mathrm{S_F}$ active.

Theorem 2. *When U_1 is intercepted by the eavesdropper, it is sufficient to consider LRTs for $\Phi_1^{\#}$, $\Phi_2^{\#}$, and $\Phi_{\mathrm{F}}^{\#}$.*

Remark 2. *The method of PBPO can be extended to incorporate the privacy constraint and approach $\Phi_1^{\#}$, $\Phi_2^{\#}$, and $\Phi_{\mathrm{F}}^{\#}$ by iteratively refining $\Phi_1^{\square}$, $\Phi_2^{\square}$, and $\Phi_{\mathrm{F}}^{\square}$.*

5. AWGN EXAMPLE

Here, we specify the independent sensing channels in Figure 1 and model C_i as $Y_i = H + N_i$ where the additive white Gaussian noise $N_i \sim \mathcal{N}(0, 1)$ and $i \in \{1, 2, \mathrm{F}\}$. The detection costs of the fusion node and eavesdropper are assigned as [17, Example 4.2]. Then, c_{F} reduces to the average detection error probability of $\mathrm{S_F}$ and $c_{\mathrm{E}}^{\min}$ represents the minimum average detection error probability of the eavesdropper.

In Scenario B, optimal privacy-unconstrained and privacy-constrained tandem distributed detection designs are obtained by PBPO methods. For the privacy-constrained problem, the highest level of privacy is guaranteed by setting $c_{\mathrm{E}}^{\min} \geq \beta = \min\{c_{\mathrm{E}}^1, c_{\mathrm{E}}^2\}$. As shown in Figure 3, optimal distributed detection system designs are compared in terms of the detection performance c_{F} and privacy risk $c_{\mathrm{E}}^{\min}$.

6. CONCLUSION

In this work, we propose the minimum Bayesian detection cost of the eavesdropper as the privacy metric. The privacy-constrained tandem distributed Bayesian detection problem is formulated to find the optimal detection system design with a privacy guarantee. We show that it is sufficient to consider LRTs for detection and fusion tests in the optimal privacy-constrained design. This conclusion is helpful to simplify the privacy-constrained optimization problem since the standard PBPO method can be easily extended. Besides the trade-off between the privacy risk and detection performance, results of the example show that the detection performance is improved when the remote sensor sends decisions which are useful for the fusion node while nonsense for the eavesdropper.

7. REFERENCES

[1] A. K. Pathan, H.-W. Lee, and C. S. Hong, "Security in wireless sensor networks: issues and challenges," in *Proceedings of ICACT 2006*, vol. 2, 2006, pp. 1043–1048.

[2] S. Schmidt, H. Krahn, S. Fischer, and D. Wätjen, "A security architecture for mobile wireless sensor networks," in *Proceedings of the First European Conference on Security in Ad-hoc and Sensor Networks*. Springer-Verlag, 2005, pp. 166–177.

[3] C. Jaikaeo, C. Srisathapornphat, and C.-C. Shen, "Diagnosis of sensor networks," in *Proceedings of ICC 2001*, vol. 5, 2001, pp. 1627–1632.

[4] M. Ding, D. Chen, K. Xing, and X. Cheng, "Localized fault-tolerant event boundary detection in sensor networks," in *Proceedings of INFOCOM 2005*, vol. 2, 2005, pp. 902–913.

[5] Z. Cao, J. Hu, Z. Chen, M. Xu, and X. Zhou, "Feedback: towards dynamic behavior and secure routing for wireless sensor networks," in *Proceedings of AINA 2006*, vol. 2, 2006, pp. 160–164.

[6] D. Liu, P. Ning, S. Zhu, and S. Jajodia, "Practical broadcast authentication in sensor networks," in *Proceedings of MobiQuitous 2005*, 2005, pp. 118–129.

[7] B. Kailkhura, S. Brahma, Y. S. Han, and P. K. Varshney, "Optimal distributed detection in the presence of Byzantines," in *Proceedings of ICASSP 2013*, 2013, pp. 2925–2929.

[8] S. Marano, V. Matta, and P. K. Willett, "Distributed detection with censoring sensors under physical layer secrecy," *Signal Processing, IEEE Transactions on*, vol. 57, no. 5, pp. 1976–1986, 2009.

[9] V. S. S. Nadendla, H. Chen, and P. K. Varshney, "Secure distributed detection in the presence of eavesdroppers," in *Proceedings of ASILOMAR 2010*, 2010, pp. 1437–1441.

[10] Z. Li, T. J. Oechtering, and K. Kittichokechai, "Parallel distributed Bayesian detection with privacy constraints," accepted by ICC 2014.

[11] Z. Li, T. J. Oechtering, and J. Jaldén, "Parallel distributed Neyman-Pearson detection with privacy constraints," accepted by ICC 2014 Workshop.

[12] C. Dwork, "Differential privacy," in *Proceedings of ICALP 2006*. Springer, 2006, pp. 1–12.

[13] B.-R. Lin and D. Kifer, "Geometry of privacy and utility," in *Proceedings of GlobalSIP 2013*, 2013, pp. 281–284.

[14] L. Sankar, S. R. Rajagopalan, and H. V. Poor, "Utility-privacy tradeoffs in databases: an information-theoretic approach," *Information Forensics and Security, IEEE Transactions on*, vol. 8, no. 6, pp. 838–852, 2013.

[15] F. du Pin Calmon and N. Fawaz, "Privacy against statistical inference," in *Proceedings of Allerton 2012*, 2012, pp. 1401–1408.

[16] I. Y. Hoballah and P. K. Varshney, "Distributed Bayesian signal detection," *Information Theory, IEEE Transactions on*, vol. 35, no. 5, pp. 995–1000, 1989.

[17] P. K. Varshney, *Distributed Detection and Data Fusion*. Springer-Verlag New York, Inc., 1996.

[18] H. L. V. Trees, *Detection, Estimation, and Modulation Theory, Part I*. Wiley-Interscience, 2001.