<http://www.diva-portal.org>

Postprint

This is the accepted version of a paper presented at *IEEE Global Conference on Signal and Information Processing (GlobalSIP) 2014, Atlanta, USA, Dec. 3-5, 2014*.

Citation for the original published paper:

Li, Z., Oechtering, T. (2014)

Privacy-Concerned Parallel Distributed Bayesian Sequential Detection

In: *Proceedings of the IEEE Global Conference on Signal and Information Processing (GlobalSIP) 2014* (pp. 928-932). IEEE Signal Processing Society

<https://doi.org/10.1109/GlobalSIP.2014.7032256>

N.B. When citing this work, cite the original published paper.

Permanent link to this version:

<http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-151262>

Privacy-Concerned Parallel Distributed Bayesian Sequential Detection

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, eavesdropping in parallel distributed sequential detections is considered. The privacy risk is evaluated by the minimal achievable Bayesian risk of a greedy and informed eavesdropper who is curious about the hypothesis realization. We propose a novel metric based on Bayesian risk to take the detection performance and privacy risk with different weights into account. We formulate and study the privacy-concerned parallel distributed Bayesian sequential detection problem under a finite time-horizon assumption. Solving this problem will lead to the optimal distributed sequential detection design which achieves the minimal privacy-concerned Bayesian risk. The study shows that it is not sufficient to consider a deterministic likelihood-ratio test for a remote decision maker at an active time index in the optimal privacy-concerned system design. However, properties of the optimal design indicate that the standard method can be extended to solve the proposed problem.

Index Terms—dynamic programming, eavesdropper, person-by-person optimization, physical-layer secrecy

I. INTRODUCTION

Internet of things (IoT) has attracted much attention recently as a revolutionary idea which envisions smart environments where machines are connected via a network [1]. Sensor networks will be needed to enable the smart environments and new applications. A big challenge in the development of sensor network technologies is the privacy problem which strongly influences users' acceptance of some sensor network applications. In face of multiple privacy threats, many efforts have been made to design secure sensor networks, e.g., privacy schemes deployed above the physical-layer [2]–[6].

Recently, a novel idea has been proposed to take the privacy issue into account in the design of physical-layer distributed detection. For instance, a countermeasure to Byzantine attacks in the distributed detection design was discussed in [7]. In [8], the eavesdropper was assumed to be interested in the data transmission state of the system which had a power constraint on data transmissions. In [9], the privacy leakage was assessed by an information-theoretic metric measuring the difference between Kullback-Leibler divergences of the fusion node and eavesdropper. In [10] and [11], we have shown that it is sufficient to consider deterministic *likelihood-ratio tests* (LRTs) for the optimal design of privacy-constrained distributed Bayesian detection problems where a local decision is intercepted. These problems are studied from a privacy-utility perspective. Related works have been done in other fields, e.g., the differential privacy [12] and conic privacy [13] problems in computer science, and problems considered in [14], [15] where information-theoretic arguments are used.

Fig. 1. The studied system model consists of a binary hypothesis H , two remote decision makers DM_1 and DM_2 , a fusion node F , and an eavesdropper E . At an active time index t , each decision maker DM_i makes a local binary decision U_{it} based on its observation Y_{it} and a feedback of previous local decisions $\{U_1^{t-1}, U_2^{t-1}\}$. On receiving local decisions $\{U_{1t}, U_{2t}\}$, the fusion node may make a final binary decision U_F or wait for future local decisions based on $\{U_{1t}, U_{2t}\}$. The eavesdropper overhears both DM-F links and can intercept all local decisions until the fusion decision is made. At any time index t' before the distributed sequential detection system terminates, the eavesdropper can decide to make a binary decision U_E or to wait for future local decisions based on $\{U_1^{t'}, U_2^{t'}\}$.

Distributed sequential detection systems [16], [17] are widely used in practice. In this work, we extend the distributed sequential detection problem to include an eavesdropper. To this end, we propose a new detection operational metric, the privacy-concerned Bayesian risk, which takes both the detection performance and privacy risk into account. Therewith, the privacy-concerned parallel distributed Bayesian sequential detection problem is formulated and analyzed to find the optimal design which achieves the minimal privacy-concerned Bayesian risk.

Here, we assume that the eavesdropper overhears both¹ remote decision makers. Thus, the eavesdropper receives as much information as the fusion center, which however decides when the remote decision makers stop sensing and transmission. This setup can be also interpreted from a perspective where the eavesdropper is a *competitor* to the fusion who has access to the same information and the goal of the optimal privacy-concerned design is to guarantee that the fusion outperforms its competitor. We therefore believe that the studied problem and results will be interesting for financial industry related applications.

The remaining of this paper is organized as follows: An

¹Results of the case where only one remote decision maker is eavesdropped can be similarly derived. But this is out of the scope of this work.

introduction to the studied system model is provided in Section II; the privacy-concerned distributed Bayesian sequential detection problem along with its main results are presented in Section III; simulation results of a numerical example are shown in Section IV; and conclusions are given in Section V.

II. PARALLEL DISTRIBUTED SEQUENTIAL DETECTION SUSCEPTIBLE TO AN EAVESDROPPER

As shown in Figure 1, the studied detection network consists of a binary hypothesis H , two remote decision makers DM_1 and DM_2 , and a fusion node F . Suppose that the system is perfectly synchronized and the maximal time-horizon is T . At an active time index $t \leq T$, each remote decision maker DM_i produces a local binary decision U_{it} based on its observation Y_{it} and the feedback of all previous local decisions $\{U_1^{t-1}, U_2^{t-1}\}$ from the fusion node. Given any hypothesis realization h , we assume that Y_i^T is generated conditionally i.i.d. in time and Y_1^T, Y_2^T are conditionally independent sequences. On receiving $\{U_{1t}, U_{2t}\}$, the fusion node decides to make a final binary fusion decision U_F or to wait for future local decisions based on $\{U_1^t, U_2^t\}$. After making the fusion decision, the fusion node will stop sending feedbacks to remote decision makers and the distributed sequential detection system will terminate its operation. An eavesdropper E can intercept all local decisions of remote decision makers until the detection system terminates. At any active time index t' before the final fusion decision is made, it similarly may make a binary decision U_E or wait to intercept more data based on $\{U_1^{t'}, U_2^{t'}\}$.

Decision strategies of remote decision makers at a time index t , the fusion node, and eavesdropper are denoted by Φ_{1t} , Φ_{2t} , Φ_F , and Φ_E such that

- $\Phi_{1t}(y_{1t}, u_1^{t-1}, u_2^{t-1})$ is a randomized decision strategy and can be described by a conditional p.m.f. $p_{U_{1t}|Y_{1t}, U_1^{t-1}, U_2^{t-1}}(u_{1t}|y_{1t}, u_1^{t-1}, u_2^{t-1})$ where $u_{1t} \in \{0, 1\}$, $u_1^{t-1} \in \{0, 1\}^{t-1}$, $u_2^{t-1} \in \{0, 1\}^{t-1}$, and $y_{1t} \in \mathbb{R}$;
- $\Phi_{2t}(y_{2t}, u_1^{t-1}, u_2^{t-1})$ is a randomized decision strategy and can be described by a conditional p.m.f. $p_{U_{2t}|Y_{2t}, U_1^{t-1}, U_2^{t-1}}(u_{2t}|y_{2t}, u_1^{t-1}, u_2^{t-1})$ where $u_{2t} \in \{0, 1\}$, $u_1^{t-1} \in \{0, 1\}^{t-1}$, $u_2^{t-1} \in \{0, 1\}^{t-1}$, and $y_{2t} \in \mathbb{R}$;
- Φ_F is a deterministic sequential detection test;
- Φ_E is a deterministic sequential detection test.

We only consider deterministic Φ_F and Φ_E here since randomized strategies cannot improve the Bayesian detection performances of the fusion node and eavesdropper [18] discussed later. Note that the operation of the eavesdropper is constrained by that of the fusion node, i.e., candidates of Φ_E are determined by a given Φ_F . In addition, we assume that the implementation of a randomized strategy Φ_{it} is unknown to other nodes, i.e., randomized strategies cannot be coordinated.

In this work, we consider the *worst* privacy problem where the eavesdropper is *greedy* and *informed*, i.e., the eavesdropper always employs the optimal decision strategy to infer H given a distributed sequential detection design.

III. PRIVACY-CONCERNED DISTRIBUTED BAYESIAN SEQUENTIAL DETECTION PROBLEM

A. Problem Formulation

Denote the non-negative detection cost of the fusion node to make a decision u_F given the hypothesis realization h by $c_{U_F, H}(u_F, h)$. The Bayesian risk of inferring H is expressed as

$$c_F = \sum_{u_F, h} p_{U_F, H}(u_F, h) c_{U_F, H}(u_F, h). \quad (1)$$

In a similar way, we denote the non-negative detection cost of the eavesdropper by $c_{U_E, H}(u_E, h)$ and its Bayesian risk to infer H by

$$c_E = \sum_{u_E, h} p_{U_E, H}(u_E, h) c_{U_E, H}(u_E, h). \quad (2)$$

For both the fusion node and eavesdropper, a reasonable assumption is made here that the detection cost of making a wrong decision is higher than that of making any correct decision.

It is obvious that the Bayesian risk c_F is a function of the distributed sequential detection design $\{\Phi_1^T, \Phi_2^T, \Phi_F\}$. As discussed before, the optimal decision strategy of the greedy and informed eavesdropper Φ_E^* is constrained and determined by the distributed sequential detection design, and so is its Bayesian risk $c_E^{\min}$. Therefore, we have two concerns when designing the distributed sequential detection system: minimizing c_F and maximizing $c_E^{\min}$.

In this paper, we introduce a novel detection-theoretic operational metric, the *privacy-concerned Bayesian risk*,

$$c_P = \alpha c_F - (1 - \alpha) c_E^{\min}, \quad \alpha \in [0, 1]. \quad (3)$$

Therewith, the privacy-concerned parallel distributed Bayesian sequential detection problem is formulated as

$$\min_{\Phi_1^T, \Phi_2^T, \Phi_F} c_P. \quad (4)$$

By adjusting the parameter α , solving the proposed optimization problem will lead to the optimal distributed sequential detection design which concerns more about the detection performance when α increases or system privacy when α decreases.

In the following, properties of the optimal distributed sequential detection design $\{\Phi_1^T, \Phi_2^T, \Phi_F\}^*$ will be obtained by studying the person-by-person optimal decision strategies $\Phi_{11}^\Delta, \dots, \Phi_{1T}^\Delta, \Phi_{21}^\Delta, \dots, \Phi_{2T}^\Delta$, and Φ_F^Δ . Note that person-by-person optimality is a necessary but not sufficient condition for global optimality.

B. Optimal Strategy of a Remote Decision Maker

To employ the person-by-person optimality argument, we first suppose that all decision strategies except Φ_{it} have been fixed. The strategy Φ_{it} can be seen as a set of strategies depending on their feedback realizations and only $\Phi_{it|u_1^{t-1}, u_2^{t-1}}$ corresponding to a particular feedback $\{u_1^{t-1}, u_2^{t-1}\}$ has to

be determined. Define conditional false alarm and detection probabilities of the randomized strategy $\Phi_{it|u_1^{t-1}, u_2^{t-1}}$ as

$$\begin{aligned} p_{it|u_1^{t-1}, u_2^{t-1}}^F &= p_{U_{it}|H, U_1^{t-1}, U_2^{t-1}}(1|0, u_1^{t-1}, u_2^{t-1}), \\ p_{it|u_1^{t-1}, u_2^{t-1}}^D &= p_{U_{it}|H, U_1^{t-1}, U_2^{t-1}}(1|1, u_1^{t-1}, u_2^{t-1}). \end{aligned} \quad (5)$$

Any $\Phi_{it|u_1^{t-1}, u_2^{t-1}}$ can be represented by an operation point $(p_{it|u_1^{t-1}, u_2^{t-1}}^F, p_{it|u_1^{t-1}, u_2^{t-1}}^D)$ in the operation region $\mathcal{R}_{it|u_1^{t-1}, u_2^{t-1}}$. Properties of this convex operation region have been discussed in [10], [19]. Then, solving the following optimization problem will lead to the local person-by-person optimal strategy $\Phi_{it|u_1^{t-1}, u_2^{t-1}}^\Delta$ with its corresponding operation point $(p_{it|u_1^{t-1}, u_2^{t-1}}^F, p_{it|u_1^{t-1}, u_2^{t-1}}^D)^\Delta$.

$$\min_{(p_{it|u_1^{t-1}, u_2^{t-1}}^F, p_{it|u_1^{t-1}, u_2^{t-1}}^D) \in \mathcal{R}_{it|u_1^{t-1}, u_2^{t-1}}} c_P. \quad (6)$$

The result in [17] shows that c_F here is a linear function of $(p_{it|u_1^{t-1}, u_2^{t-1}}^F, p_{it|u_1^{t-1}, u_2^{t-1}}^D)$ with the following structure

$$c_F = a_{itF} \cdot p_{it|u_1^{t-1}, u_2^{t-1}}^F + b_{itF} \cdot p_{it|u_1^{t-1}, u_2^{t-1}}^D + e_{itF}, \quad (7)$$

where constant coefficients a_{itF} , b_{itF} , and e_{itF} are determined by the remaining fixed decision strategies.

The optimal decision strategy of the greedy and informed eavesdropper Φ_E^* is characterized by the system design or more exactly the unfixed $\Phi_{it|u_1^{t-1}, u_2^{t-1}}$ here. Confined by the given sequential fusion decision strategy Φ_F , the set of candidates of Φ_E^* consists of sequential detection strategies which utilize all available intercepted data. That means the greedy and informed eavesdropper would not make its decision U_E until the final fusion decision U_F is made and the distributed sequential detection system terminates.

Suppose that there are K sequential detection tests to be considered as the candidates for Φ_E^* and denote each of the candidates by Φ_{Ek} with $k \in \{1, 2, \dots, K\}$. For any $\Phi_{it|u_1^{t-1}, u_2^{t-1}}$ and the remaining fixed decision strategies, we have $\Phi_E^* = \Phi_{Ek}$ iff

$$c_{Ek} \leq c_{E1}, \dots, c_{Ek} \leq c_{EK}. \quad (8)$$

Similar to c_F in (7), c_{Ek} is also a linear function of $(p_{it|u_1^{t-1}, u_2^{t-1}}^F, p_{it|u_1^{t-1}, u_2^{t-1}}^D)$ as follows

$$c_{Ek} = a_{itEk} \cdot p_{it|u_1^{t-1}, u_2^{t-1}}^F + b_{itEk} \cdot p_{it|u_1^{t-1}, u_2^{t-1}}^D + e_{itEk}. \quad (9)$$

Therefore, the greedy and informed eavesdropper will employ Φ_{Ek} as Φ_E^* iff $(p_{it|u_1^{t-1}, u_2^{t-1}}^F, p_{it|u_1^{t-1}, u_2^{t-1}}^D) \in \mathcal{R}_{itk|u_1^{t-1}, u_2^{t-1}}$ where

$$\mathcal{R}_{itk|u_1^{t-1}, u_2^{t-1}} = \left\{ (p_{it|u_1^{t-1}, u_2^{t-1}}^F, p_{it|u_1^{t-1}, u_2^{t-1}}^D) \left| \begin{array}{l} c_{Ek} \leq c_{E1} \\ \vdots \\ c_{Ek} \leq c_{EK} \end{array} \right. \right\}. \quad (10)$$

Note that the constraints in (10) are linear inequalities of $(p_{it|u_1^{t-1}, u_2^{t-1}}^F, p_{it|u_1^{t-1}, u_2^{t-1}}^D)$. Another implicit constraint here is that $(p_{it|u_1^{t-1}, u_2^{t-1}}^F, p_{it|u_1^{t-1}, u_2^{t-1}}^D) \in \mathcal{R}_{it|u_1^{t-1}, u_2^{t-1}}$. Based

Fig. 2. An illustration of sub-regions corresponding to $K = 4$ candidates of Φ_E^* .

on these conditions, it can be concluded that $\mathcal{R}_{itk|u_1^{t-1}, u_2^{t-1}}$ is a convex set and its boundary consists of line segments or boundary segments of $\mathcal{R}_{it|u_1^{t-1}, u_2^{t-1}}$. In this way, we can divide the convex operation region $\mathcal{R}_{it|u_1^{t-1}, u_2^{t-1}}$ into at most K exclusive non-empty convex sub-regions, each of which corresponds to a candidate of Φ_E^* . An example is illustrated in Figure 2.

By using the idea of dividing sub-regions, the optimization problem in (6) can be rewritten as

$$\min_k \left(p_{it|u_1^{t-1}, u_2^{t-1}}^F, p_{it|u_1^{t-1}, u_2^{t-1}}^D \right) \in \mathcal{R}_{itk|u_1^{t-1}, u_2^{t-1}} \quad \alpha c_F - (1-\alpha) c_{Ek}. \quad (11)$$

Remark 1. An inner optimization of (11) is to minimize a linear function over a convex set. Therefore, it is a convex optimization problem.

Theorem 1. The local person-by-person optimal operation point $(p_{it|u_1^{t-1}, u_2^{t-1}}^F, p_{it|u_1^{t-1}, u_2^{t-1}}^D)^\Delta$ will be on the boundary of a sub-region $\mathcal{R}_{itk|u_1^{t-1}, u_2^{t-1}}$ for $k \in \{1, 2, \dots, K\}$. Thus, it is sufficient to consider the boundary of $\mathcal{R}_{it|u_1^{t-1}, u_2^{t-1}}$ and the vertices of sub-regions as the optimal point candidates.

Proof: Based on the operation meaning of the two-layer optimization, candidates of $(p_{it|u_1^{t-1}, u_2^{t-1}}^F, p_{it|u_1^{t-1}, u_2^{t-1}}^D)^\Delta$ are the optimal operation points of inner minimizations.

As shown in Remark 1, each inner optimization in (11) is a convex optimization problem where a linear function has to be minimized over a convex sub-region. Thus, the optimum will be found on the boundary of a sub-region $\mathcal{R}_{itk|u_1^{t-1}, u_2^{t-1}}$ [20].

Further, the boundary of a sub-region $\mathcal{R}_{itk|u_1^{t-1}, u_2^{t-1}}$ consists possibly of boundary segments of $\mathcal{R}_{it|u_1^{t-1}, u_2^{t-1}}$ and other line segments. For a linear objective function, it is sufficient to consider only the end points of a line segment as the optimal point candidates [21]. For the k th inner minimization, it is therefore sufficient to consider only points on the boundary segments of $\mathcal{R}_{it|u_1^{t-1}, u_2^{t-1}}$ and vertices of $\mathcal{R}_{itk|u_1^{t-1}, u_2^{t-1}}$ (end points of line segments on the boundary of $\mathcal{R}_{itk|u_1^{t-1}, u_2^{t-1}}$) as optimal point candidates of $(p_{it|u_1^{t-1}, u_2^{t-1}}^F, p_{it|u_1^{t-1}, u_2^{t-1}}^D)^\Delta$. ■

Based on the person-by-person optimality argument, we can obtain the following result about $\Phi_{it|u_1^{t-1}, u_2^{t-1}}^*$ and its

operation point $(p_{it|u_1^{t-1}, u_2^{t-1}}^F, p_{it|u_1^{t-1}, u_2^{t-1}}^D)^*$.

Corollary 1. *Different from the result of the problem without privacy concerns [17], $(p_{it|u_1^{t-1}, u_2^{t-1}}^F, p_{it|u_1^{t-1}, u_2^{t-1}}^D)^*$ may not be on the boundary of $\mathcal{R}_{it|u_1^{t-1}, u_2^{t-1}}$, i.e., $\Phi_{it|u_1^{t-1}, u_2^{t-1}}^*$ of the optimal privacy-concerned distributed sequential detection design may not be achieved by a deterministic LRT. In this case, $(p_{it|u_1^{t-1}, u_2^{t-1}}^F, p_{it|u_1^{t-1}, u_2^{t-1}}^D)^*$ is constrained by the greedy eavesdropping behaviors and the optimal strategy $\Phi_{it|u_1^{t-1}, u_2^{t-1}}^*$ can be realized by a randomized strategy of two LRTs.*

C. Optimal Strategy of the Fusion Node

Given decision strategies of remote decision makers during the whole time-horizon, the person-by-person optimality argument is used to determine Φ_F^Δ . In addition, the information structure of this problem setting has been shown to be *quasi-classical* [17]. Therefore, dynamic programming arguments can be employed here [22], [23].

The minimal conditional expected privacy-concerned risk-to-go at an active time index t , r_{Pt} , is a function of the information available to the fusion node and eavesdropper, i.e., $\{u_1^t, u_2^t\}$. As analyzed before, the greedy and informed eavesdropper is supposed to utilize all available data and will not make its decision U_E until the fusion node makes the decision U_F .

Define functions of $\{u_1^t, u_2^t\}$ as

$$\begin{aligned} r_{Ft}^1 &= \sum_h p_{H|U_1^t, U_2^t}(h|u_1^t, u_2^t) c_{U_F, H}(1, h), \\ r_{Ft}^0 &= \sum_h p_{H|U_1^t, U_2^t}(h|u_1^t, u_2^t) c_{U_F, H}(0, h), \\ r_{Et}^{\min} &= \min \left\{ \begin{aligned} &\sum_h p_{H|U_1^t, U_2^t}(h|u_1^t, u_2^t) c_{U_E, H}(1, h) \\ &\sum_h p_{H|U_1^t, U_2^t}(h|u_1^t, u_2^t) c_{U_E, H}(0, h) \end{aligned} \right\}. \end{aligned} \quad (12)$$

At time T ,

$$r_{PT} = \min\{\alpha r_{FT}^1 - (1 - \alpha)r_{ET}^{\min}, \alpha r_{FT}^0 - (1 - \alpha)r_{ET}^{\min}\}, \quad (13)$$

where the first (second) term denotes the conditional expected privacy-concerned risk of making a decision $u_F = 1$ ($u_F = 0$) given $\{u_1^T, u_2^T\}$.

At time $t < T$, we have the backward recursion

$$r_{Pt} = \min \left\{ \begin{aligned} &\alpha r_{Ft}^1 - (1 - \alpha)r_{Et}^{\min} \\ &\alpha r_{Ft}^0 - (1 - \alpha)r_{Et}^{\min} \\ &E_{U_1^{t+1}, U_2^{t+1}} \{r_{Pt+1}|u_1^t, u_2^t\} \end{aligned} \right\}, \quad (14)$$

where the third term represents the conditional expected privacy-concerned risk of continuing given $\{u_1^t, u_2^t\}$.

Remark 2. *Since decision strategies $\{\Phi_1^T, \Phi_2^T\}$ have been fixed here, we can determine any $p_{H|U_1^t, U_2^t}(h|u_1^t, u_2^t)$ and $p_{U_1^{t+1}, U_2^{t+1}|U_1^t, U_2^t}(u_1^{t+1}, u_2^{t+1}|u_1^t, u_2^t)$ with $h \in \{0, 1\}$, $t \in \{1, \dots, T\}$, and $\{u_1^t, u_2^t\} \in \{\{0, 1\}^t, \{0, 1\}^t\}$. Then, by solving r_{Pt} given $\{u_1^t, u_2^t\}$ in a backward way, we can decide for the person-by-person optimal fusion strategy Φ_F^Δ .*

Fig. 3. Detection performance c_F and privacy risk $c_E^{\min}$ of the optimal privacy-concerned design against weight parameter α .

D. Extended Person-by-Person Optimization

The method of person-by-person optimization (PBPO) [24] is proposed to approach the globally optimal design by iteratively refining the local person-by-person optimal decision strategies. To solve our proposed privacy-concerned Bayesian detection problem, the standard algorithm of PBPO can be extended following Theorem 1, Corollary 1, and Remark 2.

IV. NUMERICAL EXAMPLE

Here, we consider a simplified numerical example where $T = 1$ such that the model in Figure 1 reduces to be a one-shot system; $p_H(0) = p_H(1) = 0.5$; $c_{U_F, H}(1, 0) = c_{U_F, H}(0, 1) = 1$, $c_{U_F, H}(0, 0) = c_{U_F, H}(1, 1) = 0$ such that the Bayesian risk c_F reduces to the average error probability of the fusion decision; and $c_{U_E, H}(1, 0) = 1$, $c_{U_E, H}(0, 1) = 2$, $c_{U_E, H}(0, 0) = c_{U_E, H}(1, 1) = 0$ such that the eavesdropper is assumed to be more concerned about its probability of miss $p_{U_E|H}(0|1)$.

In Figure 3, we can observe the trade-off between the detection performance and privacy risk. It can be also verified that the optimal design concerns more about improving the detection performance when α increases and more about suppressing the privacy risk when α decreases.

V. CONCLUSION

In this paper, the eavesdropping privacy problem in the parallel distributed sequential detection is considered. We propose a novel detection operational metric, the privacy-concerned Bayesian risk, which takes both the detection performance and privacy risk into account. Therewith, we state the privacy-per-design optimization problem to find the optimal detection strategies which optimally trade-off the privacy concern and detection performance. Arguments of the person-by-person optimality and dynamic programming are employed to study the privacy-concerned distributed Bayesian sequential detection problem. The result shows that the optimal strategy of a remote decision maker at an active time index may not be a deterministic LRT. In this case, it can be realized by a randomized strategy of two LRTs. The standard algorithm of PBPO can be extended to solve the proposed problem and to obtain the optimal privacy-concerned design.

REFERENCES

- [1] L. Tan and N. Wang, "Future Internet: the Internet of things," in *Proceedings of ICACTE 2010*, vol. 5, 2010, pp. 376–380.
- [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 and T. J. Oechtering, "Tandem distributed Bayesian detection with privacy constraints," in *Proceedings of ICASSP 2014*, 2014, pp. 8168–8172.
- [11] Z. Li, T. J. Oechtering, and K. Kittichokechai, "Parallel distributed Bayesian detection with privacy constraints," in *Proceedings of ICC 2014*, 2014, pp. 2178–2183.
- [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] D. Teneketzis, "The decentralized Wald problem," *Information and Computation*, vol. 73, no. 1, pp. 23–44, 1987.
- [17] V. V. Veeravalli, T. Basar, and H. V. Poor, "Decentralized sequential detection with a fusion center performing the sequential test," *Information Theory, IEEE Transactions on*, vol. 39, no. 2, pp. 433–442, 1993.
- [18] J. N. Tsitsiklis, "Decentralized detection," in *Advances in Statistical Signal Processing*. JAI Press, 1993, pp. 297–344.
- [19] H. L. V. Trees, *Detection, Estimation, and Modulation Theory, Part I*. Wiley-Interscience, 2001.
- [20] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.
- [21] D. Bertsimas and J. N. Tsitsiklis, *Introduction to Linear Optimization*. Athena Scientific, 1997.
- [22] T. Basar and J. B. Cruz, "Concepts and methods in multi-person coordination and control," Decision and Control Lab., Illinois University at Urbana-Champaign, Tech. Rep., 1981.
- [23] H. S. Witsenhausen, "Separation of estimation and control for discrete time systems," *Proceedings of the IEEE*, vol. 59, no. 11, pp. 1557–1566, 1971.
- [24] I. Y. Hoballah and P. K. Varshney, "Distributed Bayesian signal detection," *Information Theory, IEEE Transactions on*, vol. 35, no. 5, pp. 995–1000, 1989.