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

Postprint

This is the accepted version of a paper presented at *IEEE International Conference on Communications (ICC) Workshop, Sydney, Australia, Jun. 10-14, 2014*.

Citation for the original published paper:

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

Parallel Distributed Neyman-Pearson Detection with Privacy Constraints

In: *Proceedings of the IEEE International Conference on Communications (ICC) 2014 Workshop* (pp. 765-770).

<https://doi.org/10.1109/ICCW.2014.6881292>

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-142040>

Parallel Distributed Neyman-Pearson Detection with Privacy Constraints

Zuxing Li, Tobias J. Oechtering, and Joakim Jaldén
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 parallel distributed detection system vulnerable to an eavesdropper is proposed and studied in the Neyman-Pearson formulation. The privacy leakage is evaluated by a metric related to the Neyman-Pearson criterion. We will show that it is sufficient to consider a deterministic likelihood-ratio test for the optimal detection strategy at the eavesdropped sensor. This fundamental insight helps to simplify the problem to find the optimal privacy-constrained distributed detection system design. The trade-off between the detection performance and privacy leakage is illustrated in a numerical example.

I. INTRODUCTION

Internet of things (IoT) has attracted much attention recently as a revolutionary idea which envisions smart environments where things (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., protecting the confidential data by cryptography [2], attack detection approaches in the centralized and neighbors' cooperative ways [3], [4], and routing security based on the 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. The countermeasure to Byzantines 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. However, an eavesdropper in practice can be more aggressive. In [9], the privacy leakage was assessed by an entropy-based metric to measure the difference between Kullback-Leibler distances of the fusion node and eavesdropper. In [10], [11], it has been proved that likelihood-ratio tests (LRT) are sufficient to be considered in the optimal privacy-constrained distributed Bayesian detection designs with different topologies.

In this work, we propose a novel privacy metric and study the parallel distributed Neyman-Pearson detection problem with a physical-layer privacy constraint. The remaining of this paper is organized as follows: An introduction to the studied system model and a review of the distributed Neyman-Pearson detection problem are provided in Section II; the privacy-constrained distributed Neyman-Pearson detection problem is formulated and discussed in Section III; numerical results of an

Fig. 1. The studied system model which consists of a binary hypothesis H , two sensors S_1 and S_2 which make local binary decisions U_1 and U_2 based on their observations Y_1 and Y_2 independently, the fusion node F which makes the final binary detection decision U_F , and the eavesdropper E which intercepts the decision U_1 and makes its binary decision U_E .

additive white Gaussian noise (AWGN) example are discussed in Section IV; and conclusions are given in Section V.

II. BACKGROUND

A. Parallel Distributed Detection with an Eavesdropper

As shown in Figure 1, the detection system consists of a binary-hypothesis phenomenon H , two remote sensors S_1 and S_2 whose random observations Y_1 and Y_2 are conditionally independent given the hypothesis and have continuous distributions $f_{Y_1|H}(y_1|h)$ and $f_{Y_2|H}(y_2|h)$ such that the likelihood ratios contain no point masses of probability, and a fusion center F which receives the binary detection decisions U_1 and U_2 of the two sensors through error-free rate-limited links and produces the final fusion decision U_F . An eavesdropper E is assumed to attach the detection system and to make its own decision U_E based on the observation of the sensor decision U_1 only. The detection and fusion tests of the sensors, fusion node, and eavesdropper are functions of their own observations and are denoted by Φ_1 , Φ_2 , Φ_F , and Φ_E as follows

$$\begin{aligned} u_i &= \Phi_i(y_i), i \in \{1, 2\}, \\ u_F &= \Phi_F(u_1, u_2), \\ u_E &= \Phi_E(u_1). \end{aligned} \tag{1}$$

Since all inputs and outputs are binary variables, functions Φ_F and Φ_E have limited numbers of candidates. There are sixteen and four possible detection tests for the fusion node and eavesdropper as listed in Tables I and II respectively. A

TABLE I
FUSION TEST CANDIDATES

		u_F							
u_1	u_2	Φ_F^1	Φ_F^2	Φ_F^3	Φ_F^4	Φ_F^5	Φ_F^6	Φ_F^7	Φ_F^8
0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	1	1	1	1
0	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1
u_1	u_2	Φ_F^9	Φ_F^{10}	Φ_F^{11}	Φ_F^{12}	Φ_F^{13}	Φ_F^{14}	Φ_F^{15}	Φ_F^{16}
0	0	1	1	1	1	1	1	1	1
1	0	0	0	0	0	1	1	1	1
0	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1

TABLE II
DETECTION TEST CANDIDATES OF THE EAVESDROPPER

		u_E			
u_1		Φ_E^1	Φ_E^2	Φ_E^3	Φ_E^4
0		0	1	0	1
1		0	1	1	0

detection system design can be a set of deterministic detection and fusion tests or a randomization of detection and fusion tests, i.e., different sets of deterministic detection and fusion tests are used with certain probabilities [12]. 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 strategy, a deterministic detection test or a randomization of different detection tests, which causes the worst privacy problem. In addition, the distributed detection system is assumed to be aware of the eavesdropper and to try to adapt to the attack. We will show that detection strategies with randomizations of local detection tests at the eavesdropped sensor are not helpful in the privacy-constrained distributed Neyman-Pearson detection problem.

B. Review of Distributed Neyman-Pearson Detection

A comprehensive discussion of the distributed Neyman-Pearson detection problem is provided in [13]. Here, we briefly review some important relevant concepts and results.

Denote Sensor S_i 's detection probability $p_i^D = p_{U_i|H}(1|1)$ and false alarm probability $p_i^F = p_{U_i|H}(1|0)$ for $i \in \{1, 2\}$. In S_i 's operation region $\mathcal{R}_i$, a detection test Φ_i is represented as an operation point (p_i^F, p_i^D) . Any LRT is mapped to a point on one of the upper and lower boundaries of $\mathcal{R}_i$ which are point symmetric with respect to $(0.5, 0.5)$. The upper boundary of $\mathcal{R}_i$, known as the receiver operating characteristics (ROC) curve, satisfies the properties [14]:

- 1) The ROC curve is increasing and strictly concave.
- 2) The ROC curve is above the line $p_i^D = p_i^F$.
- 3) End points of the ROC curve are $(0, 0)$ and $(1, 1)$.

Figure 2 illustrates a typical sensor operation region. Notice that $\mathcal{R}_i$ can be separated into upper and lower parts by the line $p_i^D = p_i^F$. The two parts are equivalent since two detection tests corresponding to operation points which are point symmetric with respect to $(0.5, 0.5)$ in the upper and lower operation region parts have inversely-allocated decision regions and are equivalent in combination with inverse fusion strategies.

Fig. 2. A typical operation region of a sensor which makes a binary decision based on its random observation of the binary hypothesis. The observation has a continuous distribution such that the local likelihood ratios contain no point masses of probability.

The distributed Neyman-Pearson detection problem aims to design the optimal parallel system which maximizes the detection probability of the fusion decision $p_F^D = p_{U_F|H}(1|1)$ subject to an upper bound constraint of its false alarm probability $p_F^F = p_{U_F|H}(1|0)$:

$$\begin{aligned} \max_{\Phi_1, \Phi_2, \Phi_F} p_F^D, \\ \text{s.t. } p_F^F \leq \lambda. \end{aligned} \quad (2)$$

We assume w.l.o.g. that $p_i^D \geq p_i^F$ for $i \in \{1, 2\}$. As proved in [15] and [13, Remark 5.2.2], it is sufficient to consider deterministic LRTs for detection and fusion strategies in the optimal design.

III. PRIVACY IN DISTRIBUTED NEYMAN-PEARSON DETECTION

In [9], an entropy-based privacy metric is considered so that the privacy leakage is studied in an information-theoretic perspective. Here, we propose a novel detection operational privacy metric related to the Neyman-Pearson criterion.

A. Privacy Metric Related to Neyman-Pearson Criterion

We assume that the eavesdropper is informed of the distributed detection system and curious about the hypothesis. In this work, a Neyman-Pearson privacy scenario is considered that the eavesdropper maximizes its detection probability subject to an acceptable false alarm probability upper bound by employing the optimal detection test or randomization of detection tests. Therefore, our choice of the privacy metric in the distributed Neyman-Pearson detection problem is the maximum detection probability of the eavesdropper which has an acceptable false alarm probability upper bound,

$$\begin{aligned} \hat{p}_E^{D,\gamma} = \max_{\Phi_E} p_E^D, \\ \text{s.t. } p_E^F \leq \gamma. \end{aligned} \quad (3)$$

Obviously, $\hat{p}_E^{D,\gamma}$ is decided by the operation region of the eavesdropper $\mathcal{R}_E$. Since U_E is made based on U_1 , $\mathcal{R}_E$ is closely related to the detection test Φ_1 and $\mathcal{R}_1$ as shown in Figure 3. $\mathcal{R}_E$ has similar properties as $\mathcal{R}_1$. The lower bound of $\hat{p}_E^{D,\gamma}$ that $\hat{p}_E^{D,\gamma} \geq \gamma$ can be derived by the property that the upper boundary of $\mathcal{R}_E$ is always above the line $p_E^D = p_E^F$.

Fig. 3. The operation region $\mathcal{R}_E$ (gray) of the eavesdropper whose observation is the binary decision U_1 . In the operation region $\mathcal{R}_1$, the black circle represents Φ_1 employed by S_1 . In $\mathcal{R}_E$, the circles and squares represent four detection test candidates of the eavesdropper listed in Table II: the black circle (Φ_E^3), the white circle (Φ_E^4), and white squares (Φ_E^1 and Φ_E^2). All other points within $\mathcal{R}_E$ are achieved by randomization of the four detection tests. The same as $\mathcal{R}_1$, upper and lower boundaries of $\mathcal{R}_E$ are point symmetric with respect to $(0.5, 0.5)$ and the upper boundary is increasing, concave, and above the line $p_E^D = p_E^F$.

B. General Privacy-Constrained Distributed Neyman-Pearson Detection Problem

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

$$\begin{aligned} \max_{\Phi_1, \Phi_2, \Phi_F} \quad & p_F^D, \\ \text{s.t.} \quad & p_F^F \leq \lambda, \\ & \hat{p}_E^{D,\gamma} \leq \delta. \end{aligned} \quad (4)$$

Similar to the unconstrained Neyman-Pearson problem, the general privacy-constrained optimization problem aims to maximize p_F^D subject to an upper bound of acceptable p_F^F , but now with an additional condition $\hat{p}_E^{D,\gamma} \leq \delta$ which guarantees the privacy of the eavesdropped system. The additional condition results in a privacy-constrained operation region $\mathcal{R}_1^P$ as depicted in Figure 4. In addition, the general privacy-constrained optimization problem is feasible if and only if $\delta \geq \gamma$ since the condition $\hat{p}_E^{D,\gamma} \geq \gamma$ needs to be satisfied.

If the operation point of the deterministic LRT Φ_1 in the optimal design for the unconstrained distributed Neyman-Pearson detection problem is in $\mathcal{R}_1^P$, the optimal deterministic detection and fusion tests for the unconstrained problem are also optimal for the privacy-constrained distributed detection problem. This always holds if $\mathcal{R}_1 = \mathcal{R}_1^P$, i.e., the point (γ, δ) is on or above the ROC curve of $\mathcal{R}_1$. Otherwise, according to [15], the optimal solution of the general privacy-constrained distributed Neyman-Pearson detection problem may be a randomization among sets of detection and fusion tests rather than a set of deterministic detection and fusion tests.

Theorem 1. *By employing randomization for the fusion strategy, it is sufficient to consider a deterministic LRT whose operation point is in $\mathcal{R}_1^P$ for S_1 's optimal detection strategy of the general privacy-constrained distributed Neyman-Pearson detection problem.*

Fig. 4. A privacy-constrained operation region $\mathcal{R}_1^P$ which satisfies the condition $\hat{p}_E^{D,\gamma} \leq \delta$. If the point $A = (\gamma, \delta)$ is on or above the ROC curve, $\mathcal{R}_1 = \mathcal{R}_1^P$. Otherwise, four segments can be identified on the upper boundary of $\mathcal{R}_1^P$: the ROC segment between points $(0, 0)$ and C, line segment between points C and A, line segment between points A and B, and ROC segment between points B and $(1, 1)$, where points C, A, and $(1, 1)$ are on a line and points $(0, 0)$, A, and B are on the other line.

Proof: Any point in $\mathcal{R}_1^P$ can be achieved by a randomization of a point on the boundaries of $\mathcal{R}_1$ in $\mathcal{R}_1^P$ and one of the points $(0, 0)$ and $(1, 1)$ which correspond to trivial detection tests. Such a randomization does not violate the privacy constraint and can always be realized at the fusion node while S_1 employs the deterministic non-trivial LRT. Therefore, it is sufficient to consider a deterministic LRT for S_1 's optimal detection strategy of the general privacy-constrained distributed Neyman-Pearson problem. ■

The algorithm to find the optimal detection system design of the general privacy-constrained problem can be simplified since only a deterministic LRT needs to be considered for the detection strategy of the eavesdropped sensor. However, randomization may still be needed for the fusion strategy.

C. Privacy-Constrained Distributed Neyman-Pearson Detection Problem with Deterministic Strategies

We now focus on a particular privacy-constrained distributed Neyman-Pearson detection problem which only considers deterministic detection and fusion tests and additionally assumes $\lambda = \gamma$. Results of the particular problem are summarized in the following theorem.

Theorem 2. *It is sufficient to consider a LRT whose corresponding operation point is on the ROC curve of $\mathcal{R}_1$ in $\mathcal{R}_1^P$ for S_1 's optimal detection strategy of the privacy-constrained distributed Neyman-Pearson detection problem with deterministic detection and fusion strategies and $\lambda = \gamma$.*

D. Proof of Theorem 2

According to the review in Section II, it is sufficient to consider the upper parts of the operation regions $\mathcal{R}_1$ ($\mathcal{R}_1^P$) and $\mathcal{R}_2$, i.e., $p_1^D \geq p_1^F$ and $p_2^D \geq p_2^F$. In addition, the upper bounds of p_E^F and p_F^F are set to be $0 \leq \lambda = \gamma \leq 0.5$ (or equivalently $0 \leq \lambda = \gamma \leq 1 - \lambda \leq 1$). Similar results can be obtained when $0 \leq 1 - \lambda \leq \lambda = \gamma \leq 1$.

Denote an operation point (p_i^F, p_i^D) on the ROC curve of $\mathcal{R}_i$ by $(p_i^F, ROC_i(p_i^F))$ where $i \in \{1, 2\}$. Then, properties of

the ROC curve, concavity, $ROC_i(0) = 0$, and $ROC_i(1) = 1$, imply the following inequalities:

$$ROC_i\left(\frac{a}{b}\right) \leq \frac{ROC_i(a)}{b}, \quad (0 \leq a \leq \frac{a}{b} \leq 1), \quad (5)$$

$$ROC_i\left(\frac{a}{b}\right) \geq \frac{ROC_i(a)}{\frac{1-a}{1-\frac{a}{b}}} + 1 - \frac{1-\frac{a}{b}}{1-a}, \quad (0 \leq a \leq \frac{a}{b} \leq 1). \quad (6)$$

Let us divide the upper part of the operation region $\mathcal{R}_1$ further into two parts:

$$\begin{aligned} \mathcal{R}_1^1 &= \{(p_1^F, p_1^D) : (p_1^F, p_1^D) \in \mathcal{R}_1, p_1^D \geq p_1^F, 0 < p_1^F < \lambda\}, \\ \mathcal{R}_1^2 &= \{(p_1^F, p_1^D) : (p_1^F, p_1^D) \in \mathcal{R}_1, p_1^D \geq p_1^F, \lambda \leq p_1^F \leq 1\}. \end{aligned} \quad (7)$$

Lemmas 1 and 2 show how to optimize the distributed detection system when Φ_1 is fixed to be in $\mathcal{R}_1^1$ or $\mathcal{R}_1^2$.

Lemma 1. Given an operation point $(p_1^F, p_1^D) \in \mathcal{R}_1^1$, the maximum p_F^D subject to $p_F^F \leq \lambda$ is

$$\max \left\{ ROC_2(\lambda), p_1^D + (1 - p_1^D) ROC_2\left(\frac{\lambda - p_1^F}{1 - p_1^F}\right) \right\}. \quad (8)$$

The result $ROC_2(\lambda)$ is achieved when $(\Phi_2, \Phi_F) = ((\lambda, ROC_2(\lambda)), \Phi_F^4)$. The other result is achieved when $(\Phi_2, \Phi_F) = ((\frac{\lambda - p_1^F}{1 - p_1^F}, ROC_2(\frac{\lambda - p_1^F}{1 - p_1^F})), \Phi_F^8)$.

Lemma 2. Given an operation point $(p_1^F, p_1^D) \in \mathcal{R}_1^2$, the maximum p_F^D subject to $p_F^F \leq \lambda$ is

$$\max \left\{ ROC_2(\lambda), p_1^D ROC_2\left(\frac{\lambda}{p_1^F}\right) \right\}. \quad (9)$$

The result $ROC_2(\lambda)$ is achieved when $(\Phi_2, \Phi_F) = ((\lambda, ROC_2(\lambda)), \Phi_F^4)$. The other result is achieved when $(\Phi_2, \Phi_F) = ((\frac{\lambda}{p_1^F}, ROC_2(\frac{\lambda}{p_1^F})), \Phi_F^2)$.

Proofs of Lemmas 1 and 2 are similar. In Appendix, only the proof of Lemma 1 is given due to the space limitation. Lemma 3 shows how to optimize the distributed detection system when p_1^F is fixed.

Lemma 3. When p_1^F is fixed, it is sufficient to consider the point on the upper boundary, with the largest p_1^D , for the optimal operation point in the upper part of $\mathcal{R}_1$ to maximize p_F^D subject to $p_F^F \leq \lambda$.

Lemma 3 is a straightforward extension of Lemmas 1 and 2 since $p_1^D + (1 - p_1^D) ROC_2(\frac{\lambda - p_1^F}{1 - p_1^F})$ in (8) and $p_1^D ROC_2(\frac{\lambda}{p_1^F})$ in (9) both are increasing functions of p_1^D while $ROC_2(\lambda)$ is a constant coefficient. According to Lemma 3, it is sufficient to consider a point on the upper boundary of the privacy-constrained operation region $\mathcal{R}_1^P$ for the optimal operation point (p_1^F, p_1^D) of the particular privacy-constrained distributed Neyman-Pearson detection problem with deterministic strategies and $\lambda = \gamma$.

Besides the increasing property with respect to p_1^D for fixed p_1^F , functions $p_1^D + (1 - p_1^D) ROC_2(\frac{\lambda - p_1^F}{1 - p_1^F})$ and $p_1^D ROC_2(\frac{\lambda}{p_1^F})$ satisfy the following two properties:

Fig. 5. The detection performance parameter p_F^D of the optimal privacy-constrained distributed Neyman-Pearson detection designs with deterministic strategies and $\lambda = \gamma$ against the privacy leakage constraint parameter δ when $\lambda \in \{0.2, 0.3, 0.4\}$.

Property 1.

$$p_1^D ROC_2\left(\frac{\lambda}{p_1^F}\right) \leq \frac{p_1^D}{g} ROC_2\left(\frac{g\lambda}{p_1^F}\right), \quad (10)$$

where $0 < g \leq 1$ and $(p_1^F, p_1^D), (\frac{p_1^F}{g}, \frac{p_1^D}{g}) \in \mathcal{R}_1^2$.

Property 2.

$$\begin{aligned} & p_1^D + (1 - p_1^D) ROC_2\left(\frac{\lambda - p_1^F}{1 - p_1^F}\right) \\ & \geq 1 - g(1 - p_1^D) + g(1 - p_1^D) ROC_2\left(\frac{\lambda - (1 - g(1 - p_1^F))}{g(1 - p_1^F)}\right), \end{aligned} \quad (11)$$

where $0 < g \leq 1$ and $(p_1^F, p_1^D), (1 - g(1 - p_1^F), 1 - g(1 - p_1^D)) \in \mathcal{R}_1^1$.

Properties 1 and 2 can be proved by (5) and (6) respectively. Recall that $\lambda = \gamma$ in the particular problem. According to Property 1, the function $p_1^D ROC_2(\frac{\lambda}{p_1^F})$ (or the maximum achievable p_F^D , $\max \left\{ ROC_2(\lambda), p_1^D ROC_2(\frac{\lambda}{p_1^F}) \right\}$, when $(p_1^F, p_1^D) \in \mathcal{R}_1^2$) is increasing (or non-decreasing) when the operation point (p_1^F, p_1^D) changes along the line from A to B in Figure 4. Property 2 indicates that the function $p_1^D + (1 - p_1^D) ROC_2(\frac{\lambda - p_1^F}{1 - p_1^F})$ (or the maximum achievable p_F^D , $\max \left\{ ROC_2(\lambda), p_1^D + (1 - p_1^D) ROC_2(\frac{\lambda - p_1^F}{1 - p_1^F}) \right\}$, when $(p_1^F, p_1^D) \in \mathcal{R}_1^1$) is increasing (or non-decreasing) when the operation point (p_1^F, p_1^D) changes along the line from A to C in Figure 4. Since points C and B are on the ROC curve in $\mathcal{R}_1^P$, we can choose all candidates of the optimal operation point (p_1^F, p_1^D) to be LRTs on the ROC curve in $\mathcal{R}_1^P$, which proves Theorem 2. ■

IV. AWGN EXAMPLE

Here, we suppose that the observation of S_i is corrupted by an additive noise as $Y_i = H + N_i$ where $N_i \sim \mathcal{N}(0, 1)$ and $i \in \{1, 2\}$. In addition, N_1 and N_2 are independent. The optimal privacy-constrained distributed Neyman-Pearson detection designs with deterministic strategies and $\lambda = \gamma$ are obtained when the coefficients are set as $\lambda \in \{0.2, 0.3, 0.4\}$

and $\lambda \leq \delta \leq 1$. The trade-off between the optimal detection performance and privacy leakage upper constraint can be observed in Figure 5 that privacy-constrained distributed detection designs become more secure at the cost of worse detection performance. In each curve, p_F^D of the optimal privacy-constrained distributed Neyman-Pearson detection design does not increase when δ surpasses the threshold that the operation point of the optimal Φ_1 for the unconstrained distributed Neyman-Pearson detection problem is in $\mathcal{R}_1^P$. When $\lambda = 0.3$ and 0.4 , the corresponding curves are not smooth. That is because the point of the optimal Φ_1 changes from $\mathcal{R}_1^2 \cap \mathcal{R}_1^P$ to $\mathcal{R}_1^1 \cap \mathcal{R}_1^P$ when δ increases.

V. CONCLUSION

In this work, we propose a novel privacy metric related to the Neyman-Pearson criterion and formulate the general privacy-constrained distributed Neyman-Pearson detection problem. We also discuss a particular privacy-constrained problem in which only deterministic detection and fusion tests are considered and false alarm probability upper bounds of the fusion node and eavesdropper are the same. As proved in this paper, it is sufficient to consider a deterministic LRT for the detection strategy of the eavesdropped sensor in the optimal privacy-constrained distributed detection design. This conclusion is quite helpful to simplify privacy-constrained optimization problems. From results of an AWGN example, we can observe the trade-off between the detection performance and privacy leakage.

APPENDIX PROOF OF LEMMA 1

Given an operation point $(p_1^F, p_1^D) \in \mathcal{R}_1^1$ such that $p_1^D \geq p_1^F$ and $p_1^F \leq \lambda \leq 1 - \lambda$, the problem studied in Lemma 1 can be formulated as

$$\begin{aligned} \max_{\Phi_2, \Phi_F} p_F^D, \\ \text{s.t. } p_F^F \leq \lambda, p_2^D \geq p_2^F, \end{aligned} \quad (12)$$

where Φ_2 and Φ_F are deterministic strategies.

To satisfy the Neyman-Pearson criterion $p_F^F \leq \lambda$ by deterministic Φ_2 and Φ_F for the given Φ_1 , not all Φ_F strategy candidates listed in Table I are feasible. The idea of the proof is firstly to search for all the feasible fusion tests, then to optimize Φ_2 which maximizes p_F^D for a feasible fusion test and the given Φ_1 , and finally to find the optimal deterministic tests (Φ_2, Φ_F) by comparing the obtained designs in the second step.

Proof: p_F^F can be expressed in terms of p_1^F, p_2^F , and Φ_F as

$$\begin{aligned} p_F^F = & \Phi_F(0, 0)(1 - p_1^F)(1 - p_2^F) + \Phi_F(1, 1)p_1^F p_2^F \\ & + \Phi_F(0, 1)(1 - p_1^F)p_2^F + \Phi_F(1, 0)p_1^F(1 - p_2^F). \end{aligned} \quad (13)$$

Similarly, p_F^D can be expressed in terms of p_1^D, p_2^D , and Φ_F as

$$\begin{aligned} p_F^D = & \Phi_F(0, 0)(1 - p_1^D)(1 - p_2^D) + \Phi_F(1, 1)p_1^D p_2^D \\ & + \Phi_F(0, 1)(1 - p_1^D)p_2^D + \Phi_F(1, 0)p_1^D(1 - p_2^D). \end{aligned} \quad (14)$$

The problem in (12) is discussed in two cases.

- 1) Suppose that $p_1^F \leq p_F^F \leq \lambda$. Substituting p_F^F by the right hand side of (13) into $p_1^F \leq p_F^F \leq \lambda \leq 1 - \lambda \leq 1 - p_1^F \leq 1 - p_1^D$, feasible fusion strategy candidates are $\Phi_F^3, \Phi_F^4, \Phi_F^7, \Phi_F^8, \Phi_F^9, \Phi_F^{10}, \Phi_F^{13}$, and Φ_F^{14} .

- a) If Φ_F^4 is employed, $p_1^F \leq p_2^F = p_F^F \leq \lambda$ and $p_F^D = p_2^D$. The maximum p_F^D subject to $p_F^F \leq \lambda$ is achieved when $\Phi_2 = (\lambda, ROC_2(\lambda))$ as

$$ROC_2(\lambda). \quad (15)$$

- b) If Φ_F^8 is employed, $0 \leq p_2^F = \frac{p_F^F - p_1^F}{1 - p_1^F} \leq \frac{\lambda - p_1^F}{1 - p_1^F}$ and $p_F^D = p_1^D + (1 - p_1^D)p_2^D$. The maximum p_F^D subject to $p_F^F \leq \lambda$ is achieved when $\Phi_2 = (\frac{\lambda - p_1^F}{1 - p_1^F}, ROC_2(\frac{\lambda - p_1^F}{1 - p_1^F}))$ as

$$p_1^D + (1 - p_1^D)ROC_2(\frac{\lambda - p_1^F}{1 - p_1^F}). \quad (16)$$

- c) If Φ_F^3 is employed, $\frac{p_1^F}{1 - p_1^F} \leq p_2^F = \frac{p_F^F}{1 - p_1^F} \leq \frac{\lambda}{1 - p_1^F}$ and $p_F^D = (1 - p_1^D)p_2^D$. The maximum p_F^D subject to $p_F^F \leq \lambda$ is achieved when $\Phi_2 = (\frac{\lambda}{1 - p_1^F}, ROC_2(\frac{\lambda}{1 - p_1^F}))$ as

$$(1 - p_1^D)ROC_2(\frac{\lambda}{1 - p_1^F}). \quad (17)$$

Compared with (15), $(1 - p_1^D)ROC_2(\frac{\lambda}{1 - p_1^F}) \leq \frac{1 - p_1^D}{1 - p_1^F}ROC_2(\lambda) \leq ROC_2(\lambda)$.

- d) If Φ_F^{14} is employed, $\frac{1 - \lambda}{1 - p_1^F} \leq p_2^F = \frac{1 - p_F^F}{1 - p_1^F} \leq 1$ and $p_F^D = 1 - (1 - p_1^D)p_2^D$. The maximum p_F^D subject to $p_F^F \leq \lambda$ is achieved when $\Phi_2 = (\frac{1 - \lambda}{1 - p_1^F}, \frac{1 - \lambda}{1 - p_1^F})$ as

$$1 - (1 - p_1^D)(1 - \frac{\lambda - p_1^F}{1 - p_1^F}). \quad (18)$$

Compared with (16), $1 - (1 - p_1^D)(1 - \frac{\lambda - p_1^F}{1 - p_1^F}) \leq 1 - (1 - p_1^D)(1 - ROC_2(\frac{\lambda - p_1^F}{1 - p_1^F})) = p_1^D + (1 - p_1^D)ROC_2(\frac{\lambda - p_1^F}{1 - p_1^F})$.

- e) If Φ_F^{13} is employed, $1 - \lambda \leq p_2^F = 1 - p_F^F \leq 1 - p_1^F$ and $p_F^D = 1 - p_2^D$. The maximum p_F^D subject to $p_F^F \leq \lambda$ is achieved when $\Phi_2 = (1 - \lambda, 1 - \lambda)$ as

$$\lambda. \quad (19)$$

Compared with (15), $\lambda \leq ROC_2(\lambda)$.

- f) If Φ_F^9 is employed, $\frac{1 - p_1^F - \lambda}{1 - p_1^F} \leq p_2^F = \frac{1 - p_1^F - p_F^F}{1 - p_1^F} \leq \frac{1 - 2p_1^F}{1 - p_1^F}$ and $p_F^D = (1 - p_1^D)(1 - p_2^D)$. The maximum p_F^D subject to $p_F^F \leq \lambda$ is achieved when $\Phi_2 = (\frac{1 - p_1^F - \lambda}{1 - p_1^F}, \frac{1 - p_1^F - \lambda}{1 - p_1^F})$ as

$$\frac{1 - p_1^D}{1 - p_1^F}\lambda. \quad (20)$$

Compared with (15), $\frac{1 - p_1^D}{1 - p_1^F}\lambda \leq \lambda \leq ROC_2(\lambda)$.

- g) If Φ_F^7 is employed, $0 \leq p_2^F = \frac{p_F^F - p_1^F}{1 - 2p_1^F} \leq \frac{\lambda - p_1^F}{1 - 2p_1^F}$ and $p_F^D = (1 - 2p_1^D)(p_2^D - \frac{1}{2}) + \frac{1}{2}$. If $0 \leq p_1^D \leq 0.5$, the maximum p_F^D subject to $p_F^F \leq \lambda$ is achieved when $\Phi_2 = (\frac{\lambda - p_1^F}{1 - 2p_1^F}, ROC_2(\frac{\lambda - p_1^F}{1 - 2p_1^F}))$ as

$$(1 - 2p_1^D)(ROC_2(\frac{\lambda - p_1^F}{1 - 2p_1^F}) - \frac{1}{2}) + \frac{1}{2}. \quad (21)$$

Compared with (16),

$$\begin{aligned}
& (1 - 2p_1^D)(ROC_2(\frac{\lambda - p_1^F}{1 - 2p_1^F}) - \frac{1}{2}) + \frac{1}{2} \\
& = (1 - 2p_1^D)ROC_2(\frac{\lambda - p_1^F}{1 - 2p_1^F}) + p_1^D \\
& = (1 - 2p_1^D)ROC_2\left(\frac{\frac{\lambda - p_1^F}{1 - p_1^F}}{\frac{1 - 2p_1^F}{1 - p_1^F}}\right) + p_1^D \quad (22) \\
& \leq \frac{(1 - 2p_1^D)(1 - p_1^F)}{1 - 2p_1^F}ROC_2(\frac{\lambda - p_1^F}{1 - p_1^F}) + p_1^D \\
& \leq (1 - p_1^D)ROC_2(\frac{\lambda - p_1^F}{1 - p_1^F}) + p_1^D.
\end{aligned}$$

If $0.5 \leq p_1^D \leq 1$, the maximum p_F^D subject to $p_F^F \leq \lambda$ is achieved when $\Phi_2 = (0, 0)$ as

$$p_1^D. \quad (23)$$

Compared with (16), $p_1^D \leq p_1^D + (1 - p_1^D)ROC_2(\frac{\lambda - p_1^F}{1 - p_1^F})$.

- h) If Φ_F^{10} is employed, $\frac{1 - p_1^F - \lambda}{1 - 2p_1^F} \leq p_2^F = \frac{1 - p_1^F - p_F^F}{1 - 2p_1^F} \leq 1$ and $p_F^D = (1 - 2p_1^D)(\frac{1}{2} - p_2^D) + \frac{1}{2}$. If $0 \leq p_1^D \leq 0.5$, the maximum p_F^D subject to $p_F^F \leq \lambda$ is achieved when $\Phi_2 = (\frac{1 - p_1^F - \lambda}{1 - 2p_1^F}, \frac{1 - p_1^F - \lambda}{1 - 2p_1^F})$ as

$$(1 - 2p_1^D)(\frac{\lambda - p_1^F}{1 - 2p_1^F} - \frac{1}{2}) + \frac{1}{2}. \quad (24)$$

Compared with (16), $(1 - 2p_1^D)(\frac{\lambda - p_1^F}{1 - 2p_1^F} - \frac{1}{2}) + \frac{1}{2} \leq (1 - 2p_1^D)(ROC_2(\frac{\lambda - p_1^F}{1 - 2p_1^F}) - \frac{1}{2}) + \frac{1}{2} \leq p_1^D + (1 - p_1^D)ROC_2(\frac{\lambda - p_1^F}{1 - p_1^F})$.

If $0.5 \leq p_1^D \leq 1$, the maximum p_F^D subject to $p_F^F \leq \lambda$ is achieved when $\Phi_2 = (1, 1)$ as

$$p_1^D. \quad (25)$$

Compared with (16), $p_1^D \leq p_1^D + (1 - p_1^D)ROC_2(\frac{\lambda - p_1^F}{1 - p_1^F})$.

- 2) Suppose that $p_F^F \leq p_1^F \leq \lambda$. Substituting p_F^F by the right hand side of (13) into $p_F^F \leq p_1^F \leq \lambda \leq 1 - \lambda \leq 1 - p_1^F \leq 1 - p_F^F$, feasible fusion strategy candidates are Φ_F^2 , Φ_F^3 , Φ_F^4 , Φ_F^5 , Φ_F^9 , and Φ_F^{13} .

- a) If Φ_F^4 is employed, the maximum p_F^D subject to $p_F^F \leq \lambda$ is achieved when $\Phi_2 = (p_1^F, ROC_2(p_1^F))$ as

$$ROC_2(p_1^F). \quad (26)$$

Compared with (15), $ROC_2(p_1^F) \leq ROC_2(\lambda)$.

- b) If Φ_F^2 is employed, the maximum p_F^D subject to $p_F^F \leq \lambda$ is achieved when $\Phi_2 = (1, 1)$ as

$$p_1^D. \quad (27)$$

Compared with (16), $p_1^D \leq p_1^D + (1 - p_1^D)ROC_2(\frac{\lambda - p_1^F}{1 - p_1^F})$.

- c) If Φ_F^3 is employed, the maximum p_F^D subject to $p_F^F \leq \lambda$ is achieved when $\Phi_2 = (\frac{p_1^F}{1 - p_1^F}, ROC_2(\frac{p_1^F}{1 - p_1^F}))$ as

$$(1 - p_1^D)ROC_2(\frac{p_1^F}{1 - p_1^F}). \quad (28)$$

Compared with (15), $(1 - p_1^D)ROC_2(\frac{p_1^F}{1 - p_1^F}) \leq \frac{1 - p_1^D}{1 - p_1^F}ROC_2(p_1^F) \leq ROC_2(p_1^F) \leq ROC_2(\lambda)$.

- d) If Φ_F^5 is employed, the maximum p_F^D subject to $p_F^F \leq \lambda$ is achieved when $\Phi_2 = (0, 0)$ as

$$p_1^D. \quad (29)$$

Compared with (16), $p_1^D \leq p_1^D + (1 - p_1^D)ROC_2(\frac{\lambda - p_1^F}{1 - p_1^F})$.

- e) If Φ_F^9 is employed, the maximum p_F^D subject to $p_F^F \leq \lambda$ is achieved when $\Phi_2 = (\frac{1 - 2p_1^F}{1 - p_1^F}, \frac{1 - 2p_1^F}{1 - p_1^F})$ as

$$\frac{1 - p_1^D}{1 - p_1^F}p_1^F. \quad (30)$$

Compared with (15), $\frac{1 - p_1^D}{1 - p_1^F}p_1^F \leq \frac{1 - p_1^D}{1 - p_1^F}\lambda \leq ROC_2(\lambda)$.

- f) If Φ_F^{13} is employed, the maximum p_F^D subject to $p_F^F \leq \lambda$ is achieved when $\Phi_2 = (1 - p_1^F, 1 - p_1^F)$ as

$$p_1^F. \quad (31)$$

Compared with (15), $p_1^F \leq \lambda \leq ROC_2(\lambda)$.

Based on all the above analysis, we can make a conclusion as Lemma 1. ■

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. Jaikao, 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 at ICC 2014.
- [11] Z. Li and T. J. Oechtering, "Tandem distributed Bayesian detection with privacy constraints," accepted at ICASSP 2014.
- [12] J. N. Tsitsiklis, "Decentralized detection," in *Advances in Statistical Signal Processing*. JAI Press, 1993, pp. 297–344.
- [13] P. K. Varshney, *Distributed Detection and Data Fusion*. Springer-Verlag New York, Inc., 1996.
- [14] H. L. V. Trees, *Detection, Estimation, and Modulation Theory, Part I*. Wiley-Interscience, 2001.
- [15] P. Willett and D. Warren, "The suboptimality of randomized tests in distributed and quantized detection systems," *Information Theory, IEEE Transactions on*, vol. 38, no. 2, pp. 355–361, 1992.