# Privacy-Preserving Nonparametric Decentralized Detection

Meng Sun[1] Wee Peng Tay[2]

[1]School of Electrical and Electronic Engineering
Nanyang Technological University

[2]School of Electrical and Electronic Engineering
Nanyang Technological University

ICASSP, 2016

# Background

- Internet of Things has attracted much attention recently where machines are connected via a sensor network. And this can be modeled using a decentralized detection framework.
- In this framework, a curious fusion center can use the received sensor information to infer a correlated private hypothesis.

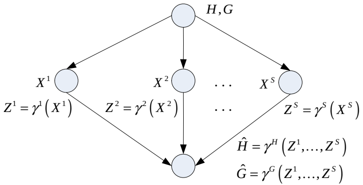
### Example

The deployment of home-monitoring video cameras in old folks' home for fall detection. In order to make fall detection, without exposing too much privacy of the old people to the fusion center, what information should the video cameras send to fusion center?

# Related Work

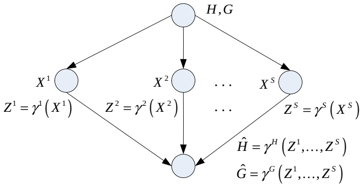
- [Nadendla and Varshney, 2014] considers decentralized detection in the presence of an eavesdropper.
- In [Li and Oechtering, 2014] and [du Pin Calmon and Fawaz, 2012], preserving the privacy of a correlated hypothesis was studied in the decentralized detection framework. The distribution of the hypothesis have to be known to use the method provided in both papers.
- A nonparametric approach to decentralized detection was introduced by [Nguyen et al., 2005], which proposes the use of kernel-based method to learn the optimal sensor decision rules from a given set of labeled training data.

# Problem Formulation



- Public hypothesis $H$, and private hypothesis $G$ take values $\{-1, +1\}$.
- Each sensor $t$ makes a noisy observation $X^t \in \mathcal{X}$ of $(H, G)$, summarizes its observation using a local decision rule $\gamma^t : \mathcal{X} \mapsto \mathcal{Z}$, and transmits $Z^t = \gamma^t(X^t)$ to a fusion center. Here, $\mathcal{X} = \{1, 2, \ldots, M\}$, and $\mathcal{Z} = \{1, 2, \ldots, L\}$, where $M \gg L$.
- Let $\underline{X} = \{X^1, X^2, \ldots, X^S\}$ and $\underline{Z} = \{Z^1, Z^2, \ldots, Z^S\}$. And the fusion center makes a decision $\hat{H} = \gamma^H(\underline{Z}) \in \{-1, +1\}$ and $\hat{G} = \gamma^G(\underline{Z}) \in \{-1, +1\}$.

# Problem Formulation



Following [Nguyen et al., 2005], our problem is

$$\min_{\gamma^H \in \mathcal{H}, Q \in \mathcal{Q}} \sum_{\underline{z} \in \mathcal{Z}^S} \sum_{i=1}^{n} \phi(h_i \gamma^H(\underline{z})) Q(\underline{z} \mid \underline{x}_i) + \frac{\lambda}{2} \|w^H\|^2,$$

$$\text{s.t.} \quad \sum_{\underline{z} \in \mathcal{Z}^S} \sum_{i=1}^{n} \phi(g_i \gamma_*^G(\underline{z})) Q(\underline{z} \mid \underline{x}_i) + \frac{\lambda}{2} \|w^G\|^2 \geq T,$$

$$\gamma_*^G = \arg\min_{\gamma^G \in \mathcal{H}} \sum_{\underline{z} \in \mathcal{Z}^S} \sum_{i=1}^{n} \phi(g_i \gamma^G(\underline{z})) Q(\underline{z} \mid \underline{x}_i) + \frac{\lambda}{2} \|w^G\|^2$$

# Algorithm Design

$$\begin{aligned} \min_{\underline{\alpha}^H \in \mathbb{R}^n, Q \in \mathcal{Q}} \; & F^H(\underline{\alpha}^H, Q), \\ \text{s.t. } \; & F^G(\underline{\alpha}^G, Q) \geq T, \\ & \underline{\alpha}^G = \arg\min_{\underline{\alpha} \in \mathbb{R}^n} F^G(\underline{\alpha}, Q) \end{aligned}$$

where

$$\begin{aligned} F^H(\underline{\alpha}^H, Q) = & \sum_{i=1}^{n} \phi \left( h_i \sum_{j=1}^{n} \alpha_j^H h_j K_Q(\underline{x}_i, \underline{x}_j) \right) \\ & + \frac{\lambda}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_i^H \alpha_j^H h_i hj K_Q(\underline{x}_i, \underline{x}_j), \end{aligned}$$

$$\begin{aligned} F^G(\underline{\alpha}^G, Q) = & \sum_{i=1}^{n} \phi \left( g_i \sum_{j=1}^{n} \alpha_j^G g_j K_Q(\underline{x}_i, \underline{x}_j) \right) \\ & + \frac{\lambda}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_i^G \alpha_j^G g_i g_j K_Q(\underline{x}_i, \underline{x}_j). \end{aligned}$$

By using the interior-point method with the logistic barrier, we obtain the following optimization problem

$$\min_{\underline{\alpha}^H \in \mathbb{R}^n, Q \in \mathcal{Q}} F^H(\underline{\alpha}^H, Q) - \frac{1}{\mu} \log \left( F^G(\underline{\alpha}^G, Q) - T \right),$$
$$\text{s.t. } \underline{\alpha}^G = \arg\min_{\underline{\alpha} \in \mathbb{R}^n} F^G(\underline{\alpha}, Q),$$

where $\mu > 0$ is the barrier parameter. From Proposition 2 in [Nguyen et al., 2005], for a fixed $Q$ we have

$$\min_{\underline{\alpha} \in \mathbb{R}^n} F^G(\underline{\alpha}^G, Q)$$
$$= \sup_{\underline{\alpha}^G \in \mathbb{R}^n} \left\{ -\sum_{i=1}^n \phi^*(-\alpha_i) - \frac{1}{2\lambda} \sum_{i=1}^n \sum_{j=1}^n \alpha_i^G \alpha_j^G g_i g_j K_Q(\underline{x}_i, \underline{x}_j) \right\},$$

where $\phi^*$ is the conjugate dual of $\phi$ [Rockafellar, 1972].

$$\min_{\underline{\alpha}^H \in \mathbb{R}^n, \underline{\alpha}^G \in \mathbb{R}^n, Q \in \mathcal{Q}} F_0(\underline{\alpha}^H, \underline{\alpha}^G, Q),$$

where

$$\begin{aligned} & F_0(\underline{\alpha}^H, \underline{\alpha}^G, Q) \\ & = F^H(\underline{\alpha}^H, Q) \\ & - \frac{1}{\mu} \log \Big( - \sum_{i=1}^{n} \phi^*(-\alpha_i^G) \\ & - \frac{1}{2\lambda} \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_i^G \alpha_j^G g_i g_j K_Q(\underline{x}_i, \underline{x}_j) - T \Big). \end{aligned}$$

# Algorithm

- **input:**$\{h_i, g_i, x_i^1, \ldots, x_i^S\}_{i=1}^n$
- **Step 0:** Initialize $\underline{\alpha}^H[0] \in \mathbb{R}^n, \underline{\alpha}^G[0] \in \mathbb{R}^n, Q[0] \in \mathcal{Q}$,
- **Step** $k \geq 1$**:**
  - Fix $\underline{\alpha}^G[k-1]$ and $Q[k-1]$, update

$$\underline{\alpha}^H[k] = \underline{\alpha}^H[k-1] - t_\alpha \nabla_{\underline{\alpha}^H} F_0(\underline{\alpha}^H[k-1], \underline{\alpha}^G[k-1], Q[k-1]),$$

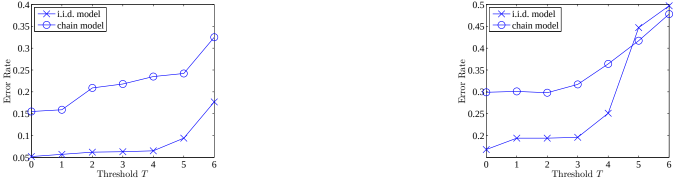
    where $t_\alpha \leq 2/L_0$, and $L_0$ is the Lipschitz constant of $F_0$.
  - Fix $\underline{\alpha}^H[k]$ and $Q[k-1]$, update

$$\underline{\alpha}^G[k] = \underline{\alpha}^G[k-1] - t_\alpha \nabla_{\underline{\alpha}^G} F_0(\underline{\alpha}^H[k], \underline{\alpha}^G[k-1], Q[k-1]),$$

    where $t_\alpha \leq 2/L_0$.
  - Fix $\underline{\alpha}^H[k]$ and $\underline{\alpha}^G[k]$, with $t_Q \leq 1/L_0$, update

$$Q[k] = \arg\min_{Q \in \mathcal{Q}} \left\| Q - Q[k-1] + t_Q \nabla_Q F_0(\underline{\alpha}^H[k], \underline{\alpha}^G[k], Q[k-1]) \right\|_{\ell_2},$$

# Simulation Results



(a) For hypothesis $H$

(b) For hypothesis $G$

Figure: Error rate of deciding hypothesis as $T$ varies

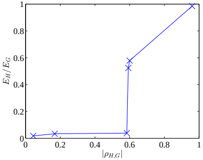


Figure: The ratio between the error rates of $H$ and $G$, as the correlation coefficient varies

| $(H, G)$ | $x$ |
|---|---|
| $(-1, -1)$ | $-3$ |
| $(-1, 1)$ | $-1$ |
| $(1, -1)$ | $1$ |
| $(1, 1)$ | $3$ |

Table: Sensor observations for different realizations of $(H, G)$.

# Summary

- In decentralized detection network, we studied the way to protect the private signal of correlated source from the curious fusion center.
- We proposed an algorithm to design the local decision rule and fusion center rule.
- We ran several simulations and find that:
  - Our algorithm can yield a high error rate for the private hypothesis $G$, while keeping the error rate of deciding the public hypothesis $H$ relatively low.
  - The error rates for deciding $H$ and $G$ increase with increasing threshold $T$ in both models.
  - The detection ability become more similar if $H$ and $G$ are more correlated.

THANKS

du Pin Calmon, F. and Fawaz, N. (2012).
Privacy against statistical inference.
In *Proc. Allerton Conf. on Commun., Control and Computing*, pages 1401–1408. IEEE.

Li, Z. and Oechtering, T. J. (2014).
Differential privacy in parallel distributed bayesian detections.
*Proc. Int. Conf. on Information Fusion*, pages 1–7.

Nadendla, V. and Varshney, P. K. (2014).
Design of binary quantizers for distributed detection under secrecy constraints.
*arXiv preprint arXiv:1410.8100*.

Nguyen, X., Wainwright, M. J., Jordan, M., et al. (2005).
Nonparametric decentralized detection using kernel methods.
*IEEE Trans. Signal Process.*, 53(11):4053–4066.

Rockafellar, R. T. (1972).
*Convex analysis*.
Princeton University Press, Princeton, New Jersey.