MULTILAYER SENSOR NETWORK FOR INFORMATION PRIVACY

Xin He and Wee Peng Tay

Department of Electrical and Electronic Engineering,
Nanyang Technological University, Singapore.

ABSTRACT

A sensor network wishes to transmit information to a fusion center to allow it to detect a public hypothesis, but at the same time prevent it from inferring a private hypothesis. We propose a multilayer sensor network structure, where each sensor first applies a nonlinear fusion function on the information it receives from sensors in a previous layer, and then a linear weighting matrix to distort the information it sends to sensors in the next layer. We adopt a nonparametric approach and develop an algorithm to optimize the weighting matrices so as to ensure that the regularized empirical risk of detecting the private hypothesis is above a given privacy threshold, while minimizing the regularized empirical risk of detecting the public hypothesis. Simulations on a synthetic dataset and an empirical experiment demonstrate that our approach is able to achieve a better trade-off between the error rates of the public and private hypothesis than using only linear precoding to achieve information privacy.

***Index Terms*—** Information privacy, Internet of Things, nonparametric detection, sensor network.

1. INTRODUCTION

With the popularity of Internet of Things (IoT) devices like on-body sensors, smart home appliances, and smart phones [1–4], massive amounts of data about users' habits, routines and preferences are being collected by service providers. Sensors make observations, and sends their data to a fusion center [5–9] to allow service providers to perform inferences that can potentially improve the quality of life. However, the same data can also be exploited to learn users' private behaviors, habits and lifestyle choices. As the number of IoT devices is increasing, ensuring users' privacy has gained traction in both the IoT industry and research community. For instance, Apple has recently announced that it will incorporate differential privacy mechanisms into its data collection process [10].

Most privacy preserving mechanisms proposed in the literature concerns data privacy, i.e., the prevention of any statistical algorithms operating on the data from inferring much about each individual datum. This is the original premise of differential privacy [11]. For example, privacy preserving support vector machine (SVM) has been proposed to transform the support vectors to hide individual datum from the fusion center, while still allowing it to make inferences using all the data [12]. Privacy preserving mechanisms have also been proposed for neural networks [13]. However, in the case where multiple sensors are used to monitor a target of interest (an example is the use of on-body sensors), then preserving the privacy of each sensor's data does not preserve the privacy of the target of interest. Statistical inferences can still be made regarding certain private aspects of the target, even though the sensor data is supposedly to be used to monitor a public aspect of the target. A specific example is the use of on-body sensors in elderlies to detect falls. Data privacy mechanisms can protect the privacy of the data collected by each sensor, but do not prevent the same data from being used to infer if the person is performing other actions. We call the prevention of statistical information leakage from a database *information privacy*. A technical criterion for information privacy was first proposed by [14], while practical nonparametric approaches to achieving information privacy in distributed sensor networks were developed in [15, 16]. In [15], a nonlinear probabilistic mapping is used to distort each sensor's local observations before being sent to the fusion center. This mapping is designed to prevent the fusion center from inferring about a private hypothesis, while still allowing it to detect a public hypothesis. However, finding the optimal mappings becomes computationally complex when the range of the mapping is large. In [16], a low complexity linear precoder at each sensor is used instead. By tuning the linear precoder, the fusion center is again prevented from inferring a private hypothesis. However, in some cases, the error detection rate of the public hypothesis may deteriorate significantly.

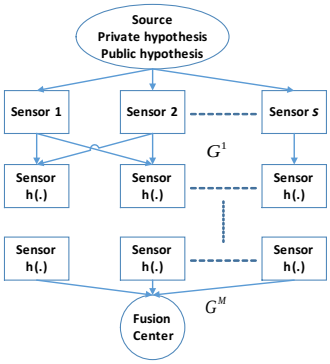

Fig. 1. Information privacy using a multilayer network.

In this paper, we propose a multilayer sensor network architecture (see Fig. 1) to achieve a better trade-off between information privacy and inference of the public hypothesis. Our inspiration comes from neural networks, a multilayer nonlinear structure that has been validated in various applications to be a flexible representation system for feature extraction and learning [17, 18]. Our experiments suggest that using a multilayer nonlinear structure in a sensor network has the potential to balance the distortion in information related to the private hypothesis and the representation of the public hypothesis. In particular, information from one layer of sensors is first linearly weighted with a weighting matrix before sending to all

This research is supported in part by the Singapore Ministry of Education Academic Research Fund Tier 2 grants MOE2013-T2-2-006 and MOE2014-T2-1-028.

sensors in the next layer. Each sensor in the next layer then uses a nonlinear function to fuse the information it has received, before repeating the procedure. The nonlinear fusion function is fixed, but the weighting matrices are optimized so that detecting the private hypothesis at the final fusion center is difficult, while keeping the accuracy of detecting the public hypothesis reasonable. The proposed method is tested with a synthetic dataset and an experiment using real images. Both tests demonstrate that our proposed method achieves high error detection rate for the private hypothesis, and low error detection rate for the public hypothesis.

The rest of this paper is organized as follows. In Section 2, we present a multilayer sensor network structure to protect information privacy. We then develop an algorithm to design the multilayer weighting matrices in Section 3. Simulation results are presented in Section 4, and Section 5 concludes the paper.

2. MULTILAYER NETWORK FOR INFORMATION PRIVACY

Consider the multilayer sensor network shown in Fig. 1. Each sensor $t = 1, 2, \ldots, s$ in the first layer makes a local observation $\mathbf{X}^t \in \mathbb{R}^{r\times k}$, which is distributed according to an unknown distribution depending on a pair of hypotheses $(p, q) \in \{-1, 1\}^2$. The hypothesis p is the public binary hypothesis that the sensor network wants the fusion center to detect, while q is a private binary hypothesis whose true state the sensor network wishes to protect from the fusion center. In order to protect the private hypothesis, each sensor applies a linear weight to its observation before sending to all the sensors in the second layer of the network. Let $\mathbf{X} = [(\mathbf{X}^1)^T, \ldots, (\mathbf{X}^s)^T]^T \in \mathbb{R}^{rs\times k}$ be the collection of all sensor observations, and let the received information at each sensor in the second layer be $\mathbf{G}^1\mathbf{X}$, where $\mathbf{G}^1 \in \mathbb{R}^{d\times rs}$ is the weighting matrix or linear precoder used by the sensors in the first layer. Each sensor in the second layer then applies a nonlinear fusion function $h(\cdot)$ to $\mathbf{G}^1\mathbf{X}$ and weigh it with $\mathbf{G}^2$ before sending $\mathbf{G}^2h(\mathbf{G}^1\mathbf{X})$ to sensors in the third layer. This process is repeated until the fusion center receives

$$\mathbf{Z}(\mathbf{X}) = \mathbf{G}^M h(\mathbf{G}^{M-1}h(\cdots h(\mathbf{G}^1\mathbf{X}))), \tag{1}$$

where M is the number of layers in the network. The nonlinear function $h(\cdot)$ is fixed, but we tune $\mathbf{G} = \{\mathbf{G}^m\}_{m=1}^M$ in order to make it difficult for the fusion center to detect the private hypothesis q. In this paper, we assume that we do not know the underlying distributions relating the sensor observations and the hypotheses. Instead, we are given a training set consisting of independent and identically distributed (i.i.d.) samples $(\mathbf{X}_i, p_i, q_i)_{i=1}^l$. Let $\mathbf{Z}_i = \mathbf{Z}(\mathbf{X}_i)$. We assume that the fusion center has access to the training samples $(\mathbf{Z}_i, p_i, q_i)_{i=1}^l$, and trains a Tikhonov regularized empirical risk function [19] as a classifier for both p and q.

Our goal is to find $\mathbf{G}$ so as to minimize the regularized empirical risk of detecting p at the fusion center, while keeping the regularized empirical risk of detecting q above a given privacy threshold θ, i.e., we solve the following optimization problem:

$$\begin{aligned}\min_{\mathbf{G}\in\mathcal{G},\mathbf{w}_\alpha} &\sum_{i=1}^{l}\phi(p_i\langle\mathbf{w}_\alpha,\Phi(\mathbf{Z}_i)\rangle_{\mathcal{H}}) + \frac{\lambda_\alpha}{2}\|\mathbf{w}_\alpha\|_2^2,\\ \text{s.t. } \min_{\mathbf{w}_\beta} &\sum_{i=1}^{l}\phi(q_i\langle\mathbf{w}_\beta,\Phi(\mathbf{Z}_i)\rangle_{\mathcal{H}}) + \frac{\lambda_\beta}{2}\|\mathbf{w}_\beta\|_2^2 \geq \theta,\end{aligned} \tag{2}$$

where $\phi(\cdot)$ is a convex loss function, $\mathbf{w}$ belongs to a reproducing kernel Hilbert space $\mathcal{H}$ with kernel $\kappa(\cdot,\cdot)$ and feature map $\Phi(\cdot)$, and $\langle\cdot,\cdot\rangle_{\mathcal{H}}$ is the inner product of $\mathcal{H}$. The constants λ_α and λ_β are positive regularization constants. The weighting matrices $\mathbf{G}$ are chosen to be within a constraint set $\mathcal{G} \subset \mathbb{R}^{d\times rs}$ of matrices. The set $\mathcal{G}$ is defined in practice to have certain desirable properties in order to facilitate implementation. In this paper, we consider two cases for $\mathcal{G}$: (i) $\mathbf{G}$ can take any value in $\mathbb{R}^{d\times rs}$, and (ii) the matrices $\mathbf{G}$ are positive semi-definite (PSD) matrices with small trace. Since the rectifier linear unit $h(x) = \max(0, x)$ induces sparsity and facilitates training and implementation [20], we adopt this as $h(\cdot)$ in the rest of this paper. In addition, for illustrative purposes, we will adopt the Gaussian kernel, i.e., $\kappa(\mathbf{Z}_i, \mathbf{Z}_j) = \exp(-\gamma\|\mathbf{Z}_i - \mathbf{Z}_j\|_F^2)$, in our presentation. We derive algorithms to first find an appropriate privacy threshold θ and then to solve (2) for the optimal $\mathbf{G}$.

3. ALGORITHM DESIGN

Given the weighting matrices $\mathbf{G}$, both public and private classifiers can be obtained from their dual problems. Therefore, the optimization problem (2) can be written as

$$\begin{aligned}\min_{\mathbf{G}\in\mathcal{G},\mathbf{w}_\alpha} &\sum_{i=1}^{l}\phi(p_i\langle\mathbf{w}_\alpha,\Phi(\mathbf{Z}_i)\rangle) + \frac{\lambda_\alpha}{2}\|\mathbf{w}_\alpha\|_2^2,\\ \text{s.t. } \max_{\boldsymbol{\beta}} &-\sum_{1=1}^{l}\phi^*(-\beta_i) - \frac{1}{2\lambda_\beta}(\mathbf{q}\circ\boldsymbol{\beta})^T\mathbf{K}(\mathbf{G},\overline{\mathbf{X}})(\mathbf{q}\circ\boldsymbol{\beta}) \geq \theta,\end{aligned} \tag{3}$$

where $\mathbf{q} = (q_i)_{i=1}^l$, $\overline{\mathbf{X}} = \{\mathbf{X}_i\}_{i=1}^l$, the (i,j)-th element of $\mathbf{K}(\mathbf{G},\overline{\mathbf{X}})$ is $\kappa(\mathbf{Z}_i,\mathbf{Z}_j)$. The function $\phi^*(\cdot)$ is the conjugate function of $\phi(\cdot)$. For example, if the logistic loss function is adopted, then $\phi^*(-\beta_i) = \beta_i\ln\beta_i + (1-\beta_i)\ln(1-\beta_i)$ with domain $\beta_i \in [0,1]$. If the hinge loss function is adopted, then $\phi^*(-\beta_i) = -\beta_i$ with domain $\beta_i \in [0,1]$.

The optimization problem (3) is nonconvex. Therefore, using a gradient based method to solve it is preferred [19]. Depending on the specific constraint set $\mathcal{G}$, we derive the gradients of the objective functions in (3) as follows. We also show how to choose the privacy threshold θ using an iterative procedure.

3.1. General Weighting Matrices

If the weighting matrix $\mathbf{G}^m$ is allowed to take any value in $\mathbb{R}^{d\times rS}$, the gradient of the empirical error of the private hypothesis in (3) with respect to (w.r.t.) $\mathbf{G}^m$ is

$$\mathbf{g}_\beta(\mathbf{G},\boldsymbol{\beta}_k) = \frac{\gamma}{\lambda_\beta}\sum_{i=1}^{l}\sum_{j=1}^{l}\exp(-\gamma\|\mathbf{Z}_i - \mathbf{Z}_j\|_F^2)\beta_i\beta_j q_i q_j \mathbf{D}^m, \tag{4}$$

where for $2 \leq m \leq M-1$,

$$\mathbf{D}^m = \mathbf{B}^m(i,j)\mathbf{F}^{m-1}(\mathbf{X}_i) + \mathbf{B}^m(j,i)\mathbf{F}^{m-1}(\mathbf{X}_j), \tag{5}$$

$$\mathbf{D}^1 = \mathbf{B}^1(i,j)\mathbf{X}_i^T + \mathbf{B}^1(j,i)\mathbf{X}_j^T, \tag{6}$$

$$\mathbf{D}^M = (\mathbf{Z}_i - \mathbf{Z}_j)[\mathbf{F}^{M-1}(\mathbf{X}_i) - \mathbf{F}^{M-1}(\mathbf{X}_j)], \tag{7}$$

with

$$\mathbf{F}^m(\mathbf{X}_i) = [h(\mathbf{G}^m\cdots h(\mathbf{G}^1\mathbf{X}_i))]^T, \tag{8}$$

$$\mathbf{I}_i^m = \mathbf{1}\{h(\mathbf{G}^m\cdots h(\mathbf{G}^1\mathbf{X}_i)) > 0\}, \tag{9}$$

$$\mathbf{B}^m(i,j) = \left[\mathbf{I}_i^m \circ ((\mathbf{G}^{m+1})^T\cdots[\mathbf{I}_i^{M-1}\circ((\mathbf{G}^M)^T(\mathbf{Z}_i - \mathbf{Z}_j)))]\right], \tag{10}$$

Table 1. Algorithm to find θ^*

With a random initialization $\mathbf{G}[0]$ and $n = 0$, iterate the following two steps until convergence.
Step 1. Solve the following convex problem,

$$\max_{\boldsymbol{\beta}} -\sum\nolimits_{i=1}^{l} \phi^*(-\beta_i) - \frac{1}{2\lambda_\beta}(\mathbf{q}\circ\boldsymbol{\beta})^T\mathbf{K}(\mathbf{G}[n],\overline{\mathbf{X}})(\mathbf{q}\circ\boldsymbol{\beta}) \quad (13)$$

Denote the optimum solution as $\boldsymbol{\beta}[n]$ and the optimal value as $L[n]$.
Step 2. Sequentially update $\{\mathbf{G}^m[n+1] = \mathbf{G}^m[n] + \Delta t_m \mathbf{g}_\beta(\mathbf{G}^m[n], \boldsymbol{\beta}[n])\}_{m=1}^M$ from the M-th layer to the first layer, Δt_m is obtained by backtracking line search.
If $(L[n+1] - L[n])/L[n] \leq \epsilon$, the iteration between the two steps is terminated and $\theta^* = L[n+1]$. Increment n by one.

Table 2. Algorithm to solve problem (3)

With the final solution $\mathbf{G}[n]$ in Table 1, iterate the following two steps until convergence.
Step 1. Solve the convex problem (11), and let the optimal solution and optimal value be denoted as $\boldsymbol{\alpha}[n]$ and $L[n]$, respectively.
Step 2. Sequentially update $\{\mathbf{G}^m[n+1] = \mathbf{G}^m[n] - \Delta t_m \mathbf{g}_\alpha(\mathbf{G}^m[n], \boldsymbol{\alpha}[n])\}_{m=1}^M$ from the M-th layer to the first layer, where Δt_m is obtained by backtracking line search, which is restricted such that the objective function (3) is decreased and the privacy restriction in (3) is satisfied (with undated $\boldsymbol{\beta}$).
The termination criterion is $(L[n] - L[n+1])/L[n] \leq \epsilon$. Finally, increment n by one.

and $\mathbf{1}\{\cdot\}$ being a pointwise indicator function.

With the gradients derived in (4), we can now use an iterative gradient-based method to solve

$$\max_{\mathbf{G},\boldsymbol{\beta}} -\sum_{1=1}^{l} \phi^*(-\beta_i) - \frac{1}{2\lambda_\beta}(\mathbf{q}\circ\boldsymbol{\beta})^T\mathbf{K}(\mathbf{G},\overline{\mathbf{X}})(\mathbf{q}\circ\boldsymbol{\beta}),$$

which gives us the best empirical risk of detecting the private hypothesis q under the worst case $\mathbf{G}$. Let this be θ^*. We then choose $\theta = p\theta^*$, where $p \in (0,1)$. The algorithm to find θ^* is listed in Table 1.

Similarly, the problem (3) can be solved by an alternative minimization between $\mathbf{w}_\alpha$ and $\mathbf{G}$. With a fixed feasible $\mathbf{G}$, the optimal $\mathbf{w}_\alpha = \sum_{j=1}^l \alpha_j p_j \Phi(\mathbf{Z}_j)$, and the optimal dual variable $\boldsymbol{\alpha}$ is obtained from the convex problem

$$\max_{\boldsymbol{\alpha}} -\sum\nolimits_{1=1}^{l} \phi^*(-\alpha_i) - \frac{1}{2\lambda_\alpha}(\mathbf{p}\circ\boldsymbol{\alpha})^T\mathbf{K}(\mathbf{G},\overline{\mathbf{X}})(\mathbf{p}\circ\boldsymbol{\alpha}). \quad (11)$$

Furthermore, owing to the strong duality between the dual (11) and its primal problem, the gradient of the empirical error for the public hypothesis in (3) w.r.t. $\mathbf{G}^m$ can be derived from (11), and is given by,

$$\mathbf{g}_\alpha(\mathbf{G},\boldsymbol{\alpha}_k) = \frac{\gamma}{\lambda_\alpha}\sum_{i=1}^{l}\sum_{j=1}^{l}\exp(-\gamma\|\mathbf{Z}_i - \mathbf{Z}_j\|_F^2)\alpha_i\alpha_j p_i p_j \mathbf{D}^m. \quad (12)$$

The algorithm to solve (3) is listed in Table 2.

3.2. PSD Weighting Matrices With Small Trace

In order to reduce the model complexity of the sensor network, we now restrict for all $m \geq 1$, $\mathbf{G}^m$ to belong to the set $\mathcal{G}^m$ of PSD matrices with trace $\mathrm{Tr}(\mathbf{G}^m) = r_m$. To reflect the geometry of the given constraint set, a common nonlinear projection method to modify the gradient update is to utilize the Bergman divergence as a distance measure [21]. In each iteration of algorithms in Tables 1 and 2, with gradient $\mathbf{g}(\mathbf{G}^m[n], \boldsymbol{\alpha}[n])$ and stepsize Δt_m, the modified $\mathbf{G}^m[n+1]$ is obtained from

$$\min_{\mathbf{H}\in\mathcal{G}^m} \langle \mathbf{g}(\mathbf{G}^m[n], \boldsymbol{\alpha}[n]), \mathbf{H} - \mathbf{G}^m[n]\rangle + \Delta t_m B(\mathbf{H}, \mathbf{G}^m[n]) \quad (14)$$

where the Bergman divergence $B(\mathbf{H}, \mathbf{G}^m[n]) = \psi(\mathbf{H}) - \psi(\mathbf{G}^m[n]) - \langle \psi'(\mathbf{G}^m[n]), \mathbf{H} - \mathbf{G}^m[n]\rangle$, $\psi(\mathbf{H}) = \sum_{i=1}^{rs} \lambda_i(\mathbf{H})\ln(\lambda_i(\mathbf{H}))$, and $\langle \mathbf{A}, \mathbf{B}\rangle = \mathrm{Tr}(\mathbf{A}\mathbf{B}^T)$.

However, when the gradient is not symmetric, its complex eigenvalue leads to an invalid objective function in (14). Therefore, we use a two-step projection method instead:

$$\min_{\mathbf{H}\in\mathcal{G}_m} \quad \langle \mathcal{P}\left(\mathbf{g}(\mathbf{G}^m[n], \boldsymbol{\alpha}[n])\right), \mathbf{H} - \mathbf{G}^m[n]\rangle + \Delta t_m B(\mathbf{H}, \mathbf{G}^m[n]) \quad (15)$$

where $\mathcal{P}\left(\mathbf{g}(\mathbf{G}^m[n], \boldsymbol{\alpha}[n])\right) = (\mathbf{g}(\mathbf{G}^m[n], \boldsymbol{\alpha}[n]) + \mathbf{g}(\mathbf{G}^m[n], \boldsymbol{\alpha}[n])^T)/2$, is optimal solution of $\min_{\mathbf{Y}=\mathbf{Y}^T} \|\mathbf{Y} - \mathbf{g}(\mathbf{G}^m[n], \boldsymbol{\alpha}[n])\|_F^2$. Therefore, (15) is simplified as

$$\min_{\mathbf{H}\in\mathcal{G}_m} \langle \mathcal{P}\left(\mathbf{g}(\mathbf{G}^m[n], \boldsymbol{\alpha}[n])\right) - \Delta t_m \psi'(\mathbf{G}^m[n]), \mathbf{H}\rangle + \Delta t_m \sum\nolimits_{j=1}^{rs} \lambda_j(\mathbf{H})\ln(\lambda_j(\mathbf{H})) \quad (16)$$

where $\psi'(\mathbf{G}^m[n]) = \sum_{j=1}^{rs}(\ln(\lambda_j(\mathbf{G}^m[n])) + 1)\mathbf{u}_j\mathbf{u}_j^T$,[1], and $\mathbf{u}_j$ is the j-th eigenvector of the matrix $\mathbf{G}^m[n]$. The closed form solution of (16) is described as follows.

Proposition 1. *The optimal solution of* (16) *is* $\mathbf{H} = \mathbf{U}\mathrm{Diag}(\lambda(\mathbf{H}))\mathbf{U}^T$, *where* $\mathbf{U}$ *comes from the eigendecomposition* $\mathcal{P}\left(\mathbf{g}(\mathbf{G}^m[n], \boldsymbol{\alpha}[n])\right) - \Delta t_m \psi'(\mathbf{G}^m[n]) = \mathbf{U}\mathrm{Diag}(\mathbf{h})\mathbf{U}^T$, *and* $\lambda_j(\mathbf{H}) = r_m \exp(-h_j/\Delta t_m - 1)/\sum_{j=1}^{rs}\exp(-h_j/\Delta t_m - 1)$

Proof. Since the symmetric matrix can be factorized as $\mathbf{H} = \mathbf{U}\mathrm{Diag}(\lambda(\mathbf{H}))\mathbf{U}^T$, it is obvious that the eigenvectors of the optimal solution in $\min_{\mathbf{H}}\langle \mathcal{P}\left(\mathbf{g}(\mathbf{G}^m[n], \boldsymbol{\alpha}[n])\right) - \Delta t_m \psi'(\mathbf{G}^m[n]), \mathbf{H}\rangle$ are the eigenvectors of $\mathcal{P}\left(\mathbf{g}(\mathbf{G}^m[n], \boldsymbol{\alpha}[n])\right) - \Delta t_m \psi'(\mathbf{G}^m[n]) = \mathbf{U}\mathrm{Diag}(\mathbf{h})\mathbf{U}^T$. Therefore, the problem (16) is simplified as,

$$\begin{aligned} \min_{\{\lambda_j(\mathbf{H})\}_{j=1}^{rs}} \ & \textstyle\sum_{j=1}^{rs}\lambda_j(\mathbf{H})h_j + \Delta t_m \sum_{j=1}^{rs}\lambda_j(\mathbf{H})\ln(\lambda_j(\mathbf{H})) \\ \text{s.t.} \ & \textstyle\sum_{j=1}^{rs}\lambda_j(\mathbf{H}) = r_m \\ & \{\lambda_j(\mathbf{H}) \geq 0\}_{j=1}^{rs} \end{aligned} \quad (17)$$

The Lagrange of (17) is

$$\begin{aligned} \mathcal{L} = & \textstyle\sum_{j=1}^{rs}\lambda_j(\mathbf{H})h_j + \Delta t_m \sum_{j=1}^{rs}\lambda_j(\mathbf{H})\ln(\lambda_j(\mathbf{H})) \\ & + \mu(\textstyle\sum_{j=1}^{rs}\lambda_j(\mathbf{H}) - r_m) - \sum_{j=1}^{rs}\nu_j\lambda_j(\mathbf{H}), \end{aligned} \quad (18)$$

then $\frac{\partial\mathcal{L}}{\partial\lambda_j(\mathbf{H})} = 0$ leads to the condition $\lambda_j(\mathbf{H}) = \exp((\nu_j - \mu)/\Delta t_m)\exp(-h_j/\Delta t_m - 1)$. Since the problem (17) is a convex problem, the optimal solution comes from the K.K.T. condition.

$$\{\lambda_j(\mathbf{H}) = \exp((\nu_j - \mu)/\Delta t_m)\exp(-h_j/\Delta t_m - 1)\}_{j=1}^{rs}$$
$$\textstyle\sum_{j=1}^{rs}\lambda_j(\mathbf{H}) = r_m, \mu \in \mathbb{R}, \{\nu_j \geq 0\}_{j=1}^{rs}, \{\nu_j\lambda_j(\mathbf{H}) = 0\}_{j=1}^{rs}.$$

Then the solution is $r_m \exp(-h_j/\Delta t_m - 1)/\sum_{j=1}^{rs}\exp(-h_j/\Delta t_m - 1)$. □

[1] When $\lambda_j(\mathbf{G}^m[n])$ is close to zero, computing $\ln(\lambda_j(\mathbf{G}^m[n]))$ may result in numerical instability. This problem can be alleviated by letting $\lambda_j(\mathbf{G}^m[n]) = \varepsilon$ whenever $\lambda_j(\mathbf{G}^m[n]) \leq \varepsilon$, where ε is the numeric accuracy level.

Table 3. Adaptation of algorithms in Table 1 and Table 2

Initialization: The start point $\{\mathbf{G}^m[0] \in \mathcal{G}_i\}_{m=1}^M$.
Step 1. Same as Step 1 in Table 1 and Table 2, respectively.
Step 2. In Table 1, update $\mathbf{G}^m[n+1]$ as the result in Proposition 1 with $\mathbf{g}(\mathbf{G}^m[n], \boldsymbol{\alpha}[n]) = -\mathbf{g}_\beta(\mathbf{G}^m[n], \boldsymbol{\beta}[n])$. In Table 2, update $\mathbf{G}^m[n+1]$ as the result in Proposition 1 with $\mathbf{g}(\mathbf{G}^m[n], \boldsymbol{\alpha}[n]) = \mathbf{g}_\alpha(\mathbf{G}^m[n], \alpha[n])$.

The softmax expression of the closed form solution exaggerates the differences between $\{h_j\}_{j=1}^{rs}$, which induces low rank weighting matrices $\mathbf{G}$. The algorithms in Table 1 and 2 are updated as Table 3.

4. EXPERIMENTAL EVALUATION

The performance of our proposed algorithm with hinge loss function is tested under a synthetic dataset and an empirical experiment using real images. The weighting matrix $\mathbf{G}^m[0]$ at each layer is initialized as a normalized identity matrix, the kernel parameter γ is the inverse of the median of the set $\{\|\mathbf{G}^M[0]h(\mathbf{G}^{M-1}[0]h(\cdots h(\mathbf{G}^1[0]\mathbf{X}_i)))-\mathbf{G}^M[0]h(\mathbf{G}^{M-1}[0]h(\cdots h(\mathbf{G}^1[0]\mathbf{X}_j)))\|_F^2 | i,j \in [1,l], i \neq j\}$, the termination threshold $\epsilon = 10^{-3}$, and $\{r_m = 1\}_{m=1}^M$.

4.1. Synthetic Dataset

In the synthetic dataset, the data sample is generated as $\mathbf{X}_i = \mathbf{1}_{\{q_i=1\}}\mathbf{a}_i + \mathbf{1}_{\{p_i=1\}}\mathbf{b}_i + \mathbf{n}_i \in \mathbb{R}^{3\times 80}$, where $\mathbf{a}_i = R_{\varphi(i)}[\mathbf{a}, \mathbf{a}+1, 10\mathbf{a}+2]^T$, with $R_{\varphi(i,t)}$ being a rotation matrix with random rotation angle $\varphi(i)$ uniformly generated from $[0, 30^\circ]$ and $\mathbf{a} \in \mathbb{R}^{80}$ being a vector of 80 evenly spaced points in $[-1, 1]$, is a rotated line segment whose presence or absence is the private hypothesis; $\mathbf{b}_i = R_{\varphi(i)}[\cos(\mathbf{b}), \sin(\mathbf{b}), \mathbf{b}]^T$, with $\mathbf{b} \in \mathbb{R}^{80}$ being a vector of 80 evenly spaced points in $[0, 10\pi]$, is a rotated helix whose presence or absence is the public hypothesis; and $\mathbf{n}_i$ is white Gaussian noise with zero mean and standard deviation $\sigma = 15$. The training sample size is 50, and the testing sample size is 950. The regularization parameters are tuned to be $[\lambda_\alpha, \lambda_\beta] = [1, 0.01]$, and the threshold $p = 0.8, 0.9, 0.96, 0.96$ are fixed for the linear precoding [16], multilayer nonlinear (MLN) mapping with $M = 2, 3, 4$, respectively.

The upper part of Fig. 2 shows that the private hypothesis error rates are similar and close to 40% for linear precoding (M=1) and MLN methods (M=2,3,4), while the MLN method with larger layer number has lower public hypothesis error rate. The lower part of Fig. 2 compares the private hypothesis error rates of different methods under different SVM detections [19]. The private hypothesis error rates of the linear and MLN methods are all higher than the no mapping method, in which the observed data is directly sent to the fusion center. Therefore, the proposed method preserves information privacy under different SVMs, and detect the public information at the same time.

4.2. Experiment With Real Images

We use a webcam to record a image, which may depict a gun or cash. The presence or absence of a gun is the public hypothesis, and the presence or absence of cash is the private hypothesis. One image sample is shown in Fig. 3. The original image is evenly sampled from 400×400 to 40×40. The training sample size is 50, and the test sample size is 150. The regularization parameters are tuned to be $[\lambda_\alpha, \lambda_\beta] = [0.01, 0.2]$, and the threshold $p = 90\%$.

Table 4 shows that the public hypothesis error rate of the MLN approach is much smaller than that of the linear precoder method,

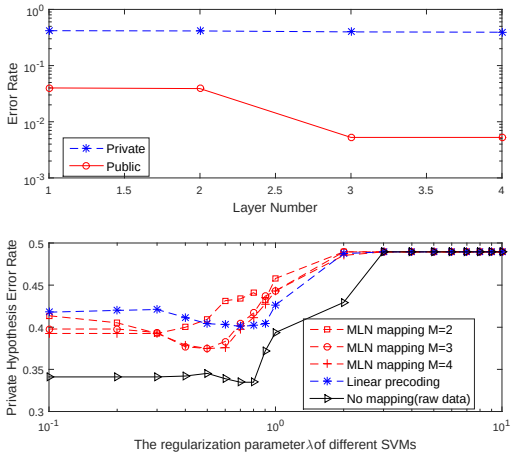

Fig. 2. Synthetic dataset. Top: Error rates for different M. Bottom: Error rates for different methods.

Fig. 3. Image experiment. The presence or absence of a gun and cash are the public and private hypothesis, respectively.

Table 4. Error rates in real image experiment.

Hypothesis error rate	Public	Private
SVM with raw data	32.67%	41.3%
Linear precoding [16]	26%	48%
MLN (M=2)	7.33%	45.33%

and the private hypothesis error rates of both methods are close to 50%. This reveals that the multilayer nonlinear structure is better at representing the public hypothesis while distorting information related to the private hypothesis. With proposed methods, the private hypothesis error rates under SVMs with different λ_β as that in Fig. 2 are larger than the private hypothesis error rates in Table 4.

5. CONCLUSION

We have proposed a multilayer network structure with nonlinear mapping at each sensor in order to distort information related to a private hypothesis. By tuning the weighting matrices at each sensor, we achieve information privacy protection up to a privacy threshold, while still allowing the fusion center to detect the public hypothesis with reasonable error rates. Simulations and empirical experiments suggest that our proposed multilayer network achieves better performance than using a single layer of sensors with linear precoding.

6. REFERENCES

[1] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE Commun. Surveys & Tutorials*, vol. 16, no. 1, pp. 266–282, 2014.

[2] J. Chen, K. Kwong, D. Chang, J. Luk, and R. Bajcsy, "Wearable sensors for reliable fall detection," in *Proc. Annual Int. Conf. of the IEEE Engineering in Medicine and Biology Society*, 2006, pp. 3551–3554.

[3] W. P. Tay, J. N. Tsitsiklis, and M. Z. Win, "On the impact of node failures and unreliable communications in dense sensor networks," *IEEE Trans. Signal Process.*, vol. 56, no. 6, pp. 2535 – 2546, Jun. 2008.

[4] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2688–2710, 2010.

[5] W. P. Tay, J. N. Tsitsiklis, and M. Z. Win, "Data fusion trees for detection: Does architecture matter?" *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4155 – 4168, Sep. 2008.

[6] W. P. Tay, "The value of feedback in decentralized detection," *IEEE Trans. Inf. Theory*, vol. 58, no. 12, pp. 7226 – 7239, Dec. 2012.

[7] H. Chen, B. Chen, and P. Varshney, "A new framework for distributed detection with conditionally dependent observations," *IEEE Trans. Signal Process.*, vol. 60, no. 3, pp. 1409 –1419, Mar. 2012.

[8] W. P. Tay, "Whose opinion to follow in multihypothesis social learning? A large deviations perspective," *IEEE J. Sel. Topics Signal Process.*, vol. 9, no. 2, pp. 344 – 359, Mar. 2015.

[9] J. Ho, W. P. Tay, T. Q. S. Quek, and E. K. P. Chong, "Robust decentralized detection and social learning in tandem networks," *IEEE Trans. Signal Process.*, vol. 63, no. 19, pp. 5019 – 5032, Oct. 2015.

[10] J. Evans, "What apple users need to know about differential privacy," www.computerworld.com, Jun. 2016.

[11] L. Wassermana and S. Zhou, "A statistical framework for differential privacy," *Journal of the American Statistical Association*, vol. 105, no. 489, 2010.

[12] J. Vaidya, H. Yu, and X. Jiang, "Privacy-preserving SVM classification," *Knowledge and Information Systems*, vol. 14, pp. 161–178, 2008.

[13] T. Chen and S. Zhong, "Privacy-preserving backpropagation neural network learning," *IEEE Trans. Neural Netw.*, vol. 20, no. 10, pp. 1554–1564, Oct 2009.

[14] F. Calmon and N. Fawaz, "Privacy against statistical inference," in *Proc. Allerton Conf. Commun., Control, Comput.*, 2012.

[15] M. Sun and W. P. Tay, "Privacy-preserving nonparametric decentralized detection," in *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing*, Shanghai, China, Mar. 2016.

[16] X. He, W. P. Tay, and M. Sun, "Privacy-aware decentralized detection using linear precoding," in *Proc. IEEE Sensor Array and Multichannel Signal Processing Workshop*, July 2016.

[17] Y. Bengio, "Learning deep architectures for ai," *Found. Trends Mach. Learn.*, vol. 2, no. 1, pp. 1–127, Jan. 2009. [Online]. Available: http://dx.doi.org/10.1561/2200000006

[18] G. Hinton, L. Deng, D. Yu, G. E. Dahl, A. r. Mohamed, N. Jaitly, A. Senior, V. Vanhoucke, P. Nguyen, T. N. Sainath, and B. Kingsbury, "Deep neural networks for acoustic modeling in speech recognition: The shared views of four research groups," *IEEE Signal Processing Magazine*, vol. 29, no. 6, pp. 82–97, Nov 2012.

[19] V. Vapnik, *The Nature of Statistical Learning Theory*. Springer-Verlag New York, 2000.

[20] X. Glorot, A. Bordes, and Y. Bengio, "Deep sparse rectifier neural networks," in *Proc. Int. Conf. on Artificial Intelligence and Statistics*, Florida, USA, 2011, pp. 315–323.

[21] A. Beck and M. Teboulle, "Mirror descent and nonlinear projected subgradient methods for convex optimization," *Oper. Res. Lett.*, vol. 31, no. 3, pp. 167–175, May 2003.