

ESTIMATION OF MICROPHONE CLUSTERS IN ACOUSTIC SENSOR NETWORKS USING UNSUPERVISED FEDERATED LEARNING

Alexandru Nelus, Rene Glitza, and Rainer Martin

Institute of Communication Acoustics, Ruhr-Universität Bochum, Bochum, Germany

email: {firstname.lastname}@rub.de

ABSTRACT

In this paper we present a privacy-aware method for estimating source-dominated microphone clusters in the context of acoustic sensor networks (ASNs). The approach is based on clustered federated learning which we adapt to unsupervised scenarios by employing a light-weight autoencoder model. The model is further optimized for training on very scarce data. In order to best harness the benefits of clustered microphone nodes in ASN applications, a method for the computation of cluster membership values is introduced. We validate the performance of the proposed approach using clustering-based measures and a network-wide classification task.

Index Terms— federated learning, clustering, privacy, acoustic sensor networks, autoencoder, unsupervised

1. INTRODUCTION

The continuously decreasing cost of acoustic sensors and the rise in popularity of wireless networks and mobile devices have helped to establish the technological infrastructure needed by (wireless) acoustic sensor networks (ASNs). These are useful in a larger number of applications, ranging from smart-homes and ambient-assisted living [1] to machine fault diagnosis [2] and surveillance [3].

Typically, ASN applications have to deal with multiple audio sources being active at the same time. In many such scenarios, the benefits provided by ASNs can be enhanced by having access to information regarding microphone nodes and their relation to the active acoustic sources. An example is provided in [4, 5] where the estimation of source-dominated microphone clusters based on hand-engineered spectral feature representations helps improve the ASN's overall signal classification and source separation performance.

While clustering and processing of multiple microphones will provide additional benefits to the aforementioned applications, the transmission of data-rich signal representations in a potentially unsafe (wireless) communication environment also poses serious privacy risks. Even in a small-scale scenario such as a smart-home, there are privacy hazards posed by eavesdroppers connecting to the network and intercepting data [6]. Moreover, in a world where privacy concerns have taken center-stage [7] and privacy policies like the European Union General Data Protection Regulation (EU GDPR) [8] aim to enforce principles such as "privacy-by-design", a more privacy-sensible solution is recommended. Therefore, this work steers away from using feature representations derived directly from the raw audio data in favor of a more privacy-aware solution based on clustered federated learning (CFL) [9]. In this way, ASN nodes (clients) need only share locally learned neural network

parameter updates with a central node (server). Furthermore, by exploiting the cosine-similarity measure between parameter update vectors, a hierarchical clustering of clients can be achieved.

Federated learning (FL) [10, 11] and inherently CFL have been designed for massively distributed systems that handle large amounts of data and have been so far only used in (semi-) supervised learning applications where (weak) classification labels were available. However, in our ASN scenarios, e.g., a smart-home, clustering has to be performed on relatively short audio segments and, most importantly, without access to training labels. Thus, the adaptation of CFL to this unsupervised scenario and its implementation in the context of ASNs becomes a challenging task. To approach this topic, we like to extend and study CFL in the context of ASNs with two simultaneously active acoustic sources in a shoebox room.

The remainder of this paper is structured as follows: we first discuss the relation to prior work, followed by a description of the proposed methods. We then continue by detailing the experimental scenarios and the results and finalize with conclusions and outlook.

2. RELATION TO PRIOR WORK

The estimation of source-dominated microphone clusters in ASN-related scenarios has been previously explored using various approaches and with different target applications. These have ranged from using coherence models [12] and energy decay information to eigenvectors [13] and spectral features [2, 4, 5, 14]. In conjunction with unsupervised fuzzy clustering, the latter works obtain robust clustering and subsequently improved signal classification results. Despite the mentioned advantages, no privacy-preserving component is included, thus falling short of modern privacy requirements [8, 15]. Moreover, supervised fuzzy clustering requires prior knowledge about the number of sources [16].

Our proposed approach builds upon the concepts introduced by the aforementioned works and focuses on adding a privacy-preserving layer using a variation of FL [10, 11], namely CFL [9]. Spectral features which, although aggregated still retain privacy-sensitive information [17], are replaced with more privacy-aware, locally learned, neural network parameter updates. This approach reduces privacy risks considerably on its own and even more in conjunction with additional encryption, differential privacy [18], or encoding schemes [19]. To solve the unsupervised clustering tasks using CFL's privacy advantages, we propose using a light-weight autoencoder in each sensor node that permits unsupervised training. CFL will then compare and cluster the local updates of these distributed autoencoders in a central server and assign nodes to acoustic sources. To handle training with scarce data and to further reduce the communication overhead that arises from transmitting deep neural network (DNN) model updates [20, 21], we limit the number of transmitted parameters and update only a part of the autoencoder.

This work has been supported by the German Research Foundation (DFG) - Project Number 282835863.

Algorithm 1: Unsupervised CFL for the estimation of source-dominated microphone clusters in ASNs

Input: Pre-trained autoencoder h , thresholds ϵ_1 , ϵ_2 and ϵ_3 , maximum no. of rounds max_τ

freeze all parameters of h except θ

while $audio\ buffer \neq empty$ **do**

 read audio D of M clients

 initialize cluster list $C = \{\{1, ..M\}\}$ with a single cluster element that contains all M clients

$C' = \{\}$

$\theta_c \leftarrow$ random initialization

for $\tau = 1$ **to** max_τ **do**

for $c \in C$ **do**

for $i \in c$ **do**

$\Delta\theta_i^\tau \leftarrow SGD(h_{\theta_c}(D_i))$

end

$\Delta\bar{\theta}_c = \left\| \frac{1}{|c|} \sum_{i \in c} \Delta\theta_i \right\|$

$\Delta\hat{\theta}_c = \max_{i \in c} (\|\Delta\theta_i\|)$

if $\Delta\bar{\theta}_c \leq \epsilon_1$ & $\Delta\hat{\theta}_c \geq \epsilon_2$ & $|\nabla\Delta\bar{\theta}_c| \leq \epsilon_3$ **then**

$a_{i,j} = \frac{\langle \Delta\theta_i, \Delta\theta_j \rangle}{\|\Delta\theta_i\| \|\Delta\theta_j\|}, \forall i, j \in c$

$c_1, c_2 \leftarrow \text{bi-partition}(A)$

$\theta_{c_1}^{\tau+1} = \theta_c^\tau + \sum_{i \in c_1} \frac{|D_i|}{|D_{c_1}|} \Delta\theta_i^\tau$

$\theta_{c_2}^{\tau+1} = \theta_c^\tau + \sum_{j \in c_2} \frac{|D_j|}{|D_{c_2}|} \Delta\theta_j^\tau$

$C' = C' + \{c_1, c_2\}$

$\tau = max_\tau + 1$

else

$\theta_c^{\tau+1} = \theta_c^\tau + \sum_{i \in c} \frac{|D_i|}{|D_c|} \Delta\theta_i^\tau$

$C' = C' + \{c\}$

end

end

$C = C'$

end

3. UNSUPERVISED CLUSTERING USING CFL

3.1. Federated learning

Federated learning was introduced in [10, 11] as a method for large-scale privacy-preserving distributed learning of neural network parameters. It works using a three-step iterative process over a given number of communication rounds τ . In the first step, the clients synchronize with the server by downloading the latest model parameters represented by column vector θ^τ . In the second step each client i independently improves its own model parameters θ_i^τ by performing stochastic gradient descent (SGD) [22] on their respective data D_i . In the third step, the clients upload their model parameters updates $\Delta\theta_i^\tau$ to the server for aggregation following

$$\theta^{\tau+1} = \theta^\tau + \sum_{i=1}^M \frac{|D_i|}{|D|} \Delta\theta_i^\tau, \quad (1)$$

where M is the total number of clients, D their total dataset, and $|\cdot|$ denotes the cardinality of a dataset.

3.2. Clustered federated learning

It is shown in [9, 19] that for the cases where clients' data comes from different (*incongruent*) distributions, there is no single θ^* that can optimally minimize the loss of all clients at the same time. For

this reason, the authors suggest clustering the clients that have similar (*congruent*) distributions and training separate server models for each resulting cluster. The clustering criterion proposed uses the cosine similarity measure $a_{i,j}$ between the nodes' weight update vectors following

$$a_{i,j} = \frac{\langle \Delta\theta_i, \Delta\theta_j \rangle}{\|\Delta\theta_i\| \|\Delta\theta_j\|}, \quad (2)$$

where $\langle \cdot, \cdot \rangle$ denotes the inner product and $\|\cdot\|$ the L_2 norm. The cosine similarities $a_{i,j}$ of all clients are collected in the symmetric matrix A .

Hierarchical clustering using bi-partitioning can be recursively applied using A . The resulting two clusters c_1 and c_2 of each bi-partitioning step are derived such that the maximum cross-cluster cosine similarity is always smaller than the minimum of either intra-cluster cosine similarities [9]:

$$\max_{\forall i \in c_1, k \in c_2} (a_{i,k}) < \min(\min_{\forall i, j \in c_1} (a_{i,j}), \min_{\forall k, l \in c_2} (a_{k,l})). \quad (3)$$

The process is recursively repeated, and new sub-clusters are obtained, until the data distributions' congruence condition is no longer violated. The latter can be verified for each cluster c by analyzing the mean and the maximum Euclidean norms of the weight update vectors $\Delta\theta_c$, defined as

$$\Delta\bar{\theta}_c = \left\| \frac{1}{|c|} \sum_{i \in c} \Delta\theta_i \right\| \quad \text{and} \quad \Delta\hat{\theta}_c = \max_{i \in c} (\|\Delta\theta_i\|). \quad (4)$$

Whenever the server has reached a stationary solution but some clients are still converging towards a locally stationary point, a low value of $\Delta\bar{\theta}_c$ in conjunction with a higher value of $\Delta\hat{\theta}_c$ is observed. This indicates incongruent data distributions and prompts bi-partitioning.

3.3. Unsupervised clustered federated learning

In other works, FL and CFL have been used for improving a server-based classification model with the goal of high classification accuracy. Our work, however, is only concerned with obtaining good clustering results which can be further used to enhance subsequent ASN-based applications. Moreover, we aim for a more general solution that does not rely on the availability of labeled data, thus requiring an unsupervised approach in the clustering process. As such, we propose to use a light-weight autoencoder with a low number of trainable parameters that are periodically re-initialized.

The proposed adaptation, along with the standard CFL algorithm [9], are schematically described in Algorithm 1. Prior to performing FL, the light-weight autoencoder h is pre-trained, after which all layers except the bottleneck layer are frozen. The latter is always re-initialized with random parameters before applying CFL. The reduction of trainable network parameters is necessary in order to avoid overfitting [23] caused by the large discrepancy between the very small number of training samples and the large number of parameters of a complete model. Moreover, processing fewer parameters reduces computational and bandwidth costs [20].

Additional to the incongruity verification based on $\Delta\bar{\theta}_c \leq \epsilon_1$ and $\Delta\hat{\theta}_c \geq \epsilon_2$ introduced in [9], we propose a supplementary verification as to fit the high $\Delta\bar{\theta}_c$ and $\Delta\hat{\theta}_c$ variation generated by handling a small number of training samples. This consists in thresholding the gradient $|\nabla\Delta\bar{\theta}_c| \leq \epsilon_3$, based on the intuition that a small $\Delta\bar{\theta}_c$ slope indicates the system reaching a stationary solution regardless of the absolute values of $\Delta\theta_c$.

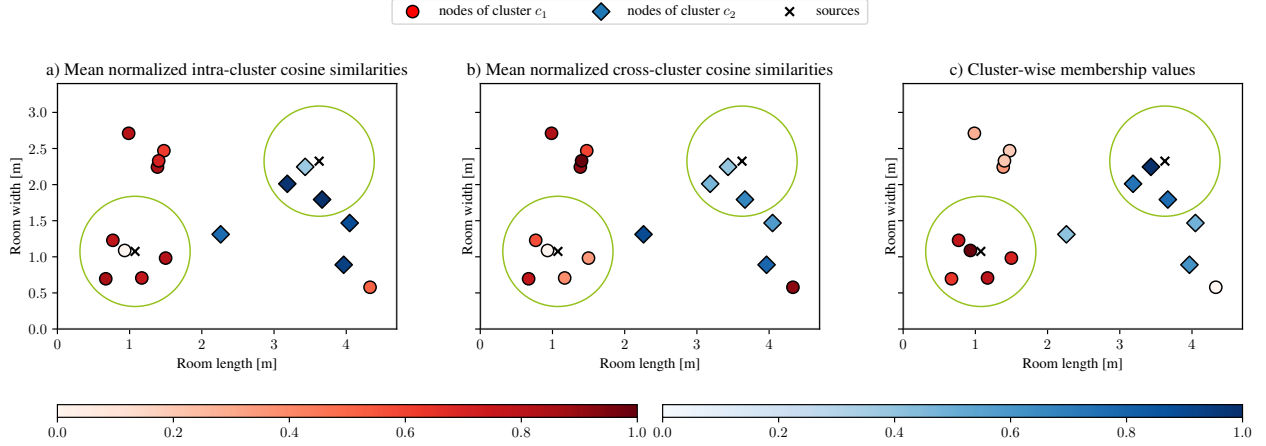


Fig. 1. Cluster membership values (MVs) for unsupervised CFL where mean normalized intra- (a) and cross-cluster cosine similarities (b) are aggregated in order to determine cluster reference nodes which in turn are used to compute MVs (c). Outliers are occasionally observed due to specific acoustic constellations which include wall reflections and reverberation. Illustration regards a single simulation scenario.

3.4. Membership values

To assess the contribution of each node to its respective cluster we propose the computation of cluster membership values (MVs) after each bi-partitioning of clients into clusters c_1 and c_2 . We first compute the mean intra- and cross-cluster similarities for each client i and stack them in vectors \mathbf{q} and \mathbf{r} , respectively, with

$$q_i = \frac{1}{|c_x| - 1} \sum_{j \in c_x \setminus \{i\}} a_{i,j} \text{ and } r_i = \frac{1}{|c_y|} \sum_{k \in c_y} a_{i,k} \quad (5)$$

for $\forall i \in c_x$ and $(c_x, c_y) \in \{(c_1, c_2), (c_2, c_1)\}$, where $|\cdot|$ denotes the cardinality of a set. We further apply min-max normalization to \mathbf{q} and \mathbf{r} after which we compute vector \mathbf{p} that contains the aggregated mean cosine similarity values for each client using a weighted sum,

$$p_i = \lambda \frac{q_i - \min(\mathbf{q})}{\max(\mathbf{q}) - \min(\mathbf{q})} + (1 - \lambda) \frac{r_i - \min(\mathbf{r})}{\max(\mathbf{r}) - \min(\mathbf{r})}. \quad (6)$$

Since the acoustic sources are modeled as spherical point sources, nodes very close to a source pick up quite different signals from other nodes which are dominated by a reverberant mixture of both sources. This results in small mean intra-cluster similarity values for nodes positioned close to the cluster source and those positioned at extremities, thus requiring additional cross-cluster information in order to distinguish them. After applying (6), only the nodes closest to a cluster source will display small p_i values. We further select the node with the smallest p_i value in each cluster as a reference node and compute the MVs vector $\boldsymbol{\mu}$ as the cosine similarities between the cluster nodes and their respective reference node:

$$\mu_i = a_{i, \arg \min(p_j)}, \forall i, j \in c_x \text{ and } c_x \in \{c_1, c_2\}. \quad (7)$$

Min-max normalization is again applied to vector $\boldsymbol{\mu}$. An example of a single simulation scenario is provided in Figure 1. Additionally, thresholding with $\mu_i = 0, \forall \mu_i \leq v$ is also considered in order to disregard nodes with low MVs.

4. EXPERIMENTS AND RESULTS

4.1. Database and simulation scenarios

For this work, we employ a subset of the LibriSpeech corpus [24], namely *train-clean-100*, which consists of 251 speakers (125 female,

126 male) from audiobook recordings sampled at 16 kHz. We further apply voice activity detection (VAD) and restructure the data into 25006 utterances of length 10 s each. Next, the dataset is split into *Libri-server* with 157 speakers (79 female, 78 male) used to train the autoencoder and gender recognizer and *Libri-clients* containing 94 speakers used to perform clustering and infer speaker genders.

The current work only considers two simultaneously active sources randomly positioned in opposing quadrants of a shoe-box room of size $4.7 \times 3.4 \times 2.4$ m with the reverberation time $T_{60} = 0.34$ s. The ASN deployed in the room consists of $M = 16$ microphone nodes, which are, as well, randomly spread under the constraint that for every source, a minimum of three nodes is positioned within critical distance, thus having higher direct component energy than reverberation energy. The random spread of sources and microphones is performed ten times. For each constellation created, 20 gender-balanced speaker pairs are randomly selected from Libri-clients resulting in 200 simulation scenarios. For each scenario, we randomly select 16 utterances/speaker to perform CFL followed by gender recognition using the estimated cluster configuration.

Each ASN node i is exposed to a mix of signals from both sources s_1 and s_2 , expressed as

$$x_i(t) = s_1(t) * g_i^{s_1}(t) + s_2(t) * g_i^{s_2}(t), \quad (8)$$

where $g_i^{s_j}$ is the impulse response from source j to node i and is simulated with CATT Acoustic using cone-tracing [25].

4.2. Server pre-training

The architecture of the proposed autoencoder h is detailed in Table 1. This is trained to reconstruct the Log-Mel Band Energy (LMBE) input feature representation \mathbf{Y} . The latter is extracted for each 10 s utterance as detailed in [26] using a short-time discrete Fourier transform (STFT) with window length $L_1 = 0.064$ s and step size $R_1 = 0.032$ s along with $K = 128$ Mel filters. Training is performed on the Libri-server set for 300 epochs using an SGD optimizer with a learning rate of $l_r = 0.1$. The loss function that is minimized over the entire model parameters set $\boldsymbol{\theta}$ is the mean squared error (MSE) between the input and reconstructed feature vectors:

$$\min_{\boldsymbol{\theta}} L_{\text{mse}}(\mathbf{Y}, \hat{\mathbf{Y}}) = \min_{\boldsymbol{\theta}} \frac{1}{N} \sum_{n=1}^N (y_n - \hat{y}_n)^2. \quad (9)$$

After the model is trained, the $\boldsymbol{\theta}$ parameters, except for subset $\boldsymbol{\theta}_1$, are frozen. The initial number of $O_1 = 5999$ trainable parameters

Table 1. Neural network architecture of autoencoder h .

Layer	Input	Operator	Out ch.	Stride	Kernel/Nodes	Activation
1	128 x 128	Conv2d	6	1	5 x 5	ReLU
2	6 x 124 x 124	MaxPool	-	2	2 x 2	-
3	6 x 62 x 62	Conv2d	16	1	5 x 5	ReLU
4	16 x 58 x 58	MaxPool	-	2	2 x 2	-
5	16 x 29 x 29	Dense	-	-	29	ReLU
6	16 x 29 x 29	Unpool	-	2	2 x 2	-
7	16 x 58 x 58	ConvTrans2d	6	1	5 x 5	ReLU
8	6 x 62 x 62	Unpool	-	2	2 x 2	-
9	6 x 124 x 124	ConvTrans2d	1	1	5 x 5	Sigmoid

Table 2. Normalized cluster-to-source distance $\tilde{d}_{c_x}^{s_z}$ from cluster c_x to source s_z , averaged over 200 scenarios.

	c_1	c_2
s_1	0.15	0.91
s_2	0.87	0.14

is thus reduced to $O_2 = 841$. This subset corresponds to the parameters of Layer 5 from Table 1. These are further re-initialized and trained as described in the next subsection.

4.3. Clustering

The pre-trained autoencoder h detailed in Subsection 4.2 is employed for unsupervised CFL as indicated in Algorithm 1. The MSE loss function introduced in (9) acts only on parameters subset θ , as the rest of the parameters are frozen. We empirically set $\epsilon_1 = 0.0134$, $\epsilon_2 = 0.005$, $\epsilon_3 = 0.0007$, and $max_\tau = 25$ communication rounds. Each of the total $M = 16$ clients trains for one epoch in every round τ , with $l_r = 0.1$. The clients' input feature representation \mathbf{Y}_i is computed based on the 10 s time-domain signal $x_i(t)$ as detailed in (8), where s_1 and s_2 are selected from the Libri-clients dataset. The MVs defined in (6) are computed using $\lambda = 0.5$.

To evaluate and compare the clustering performance to state-of-the-art solutions [4], we employ from the latter the normalized cluster-to-source distance from cluster c_x to source s_z as

$$\tilde{d}_{c_x}^{s_z} = \frac{\|\rho_{s_z} - \bar{\rho}_{c_x}\|}{\|\rho_{s_1} - \rho_{s_2}\|}, \forall c_x \in \{c_1, c_2\} \text{ and } s_z \in \{s_1, s_2\}, \quad (10)$$

where ρ_{s_z} is the geometric position of source s_z and $\bar{\rho}_{c_x}$ is the average of geometric positions of nodes i assigned to cluster c_x which are weighted by their respective MVs. Table 2 shows $\tilde{d}_{c_x}^{s_z}$ averaged over all 200 simulation scenarios.

It can be observed that low values of $\tilde{d}_{c_1}^{s_1}$ and $\tilde{d}_{c_2}^{s_2}$ are obtained, indicating that the MV-weighted cluster centers are each situated in close proximity to their dominant source. The high $\tilde{d}_{c_1}^{s_2}$ and $\tilde{d}_{c_2}^{s_1}$ values validate that the MV-weighted cluster centers are, concurrently, situated away from their opposing sources. The obtained metrics point towards good cluster predictions, comparable to results in [4].

4.4. Gender recognition

In order to assess the clustering performance from a utility standpoint, we further implement a gender recognition task. To this end, we first train a gender recognition model e on the Libri-server dataset, where a part of the clean signals is randomly augmented with male-female reverberant signal mixtures. The model architecture is described in Table 3, where the input feature representation \mathbf{Y} is extracted for $L_1 = 0.064$, $R_1 = 0.02$, and $K = 40$. Training is performed for 13 epochs using a cross-entropy loss function and an SGD optimizer with $l_r = 0.01$. Testing is performed for all 200

Table 3. Neural network architecture of gender recognizer e .

Input	Operator	Out ch.	Stride	Kernel/Nodes	Batch norm.	Activation	Dropout
501 x 40	Conv2d	32	1	5 x 40	Yes	ReLU	-
497 x 32	MaxPool	-	1	5 x 1	-	-	-
99 x 32	Conv2d	64	1	3 x 32	Yes	ReLU	-
92 x 64	MaxPool	-	1	92 x 1	-	-	-
1 x 64	Dense	-	-	64	-	ReLU	50%
1 x 64	Dense	-	-	2	-	Softmax	-

Table 4. Aggregated gender recognition Accuracy (A_{cc}) and F_1 -score (F_1) of estimated clusters, without and with membership value (MV) weighting using threshold v . Results reflect 200 scenarios.

	no MV	MV $v=0$	MV $v=0.5$	MV $v=0.9$
$A_{cc}(\%)$	90	96	97	99
$F_1(\%)$	89	96	97	98

simulation scenarios indicated above, utilizing the utterances from Libri-clients used to generate clustering estimations.

The proposed evaluation metrics are Accuracy (A_{cc}) and F_1 -score (F_1), where the ground truth gender label of a node is given by the gender of the source with the shortest first peak delay of the impulse response. The ground truth gender label of a cluster is given by the mode of the ground truth gender labels of its constituting nodes. The predicted gender label of a cluster is the mode of predicted gender labels of its nodes. Since each node processes 16 utterances/scenario, its gender label is given by the mode of gender predictions across the utterances. The evaluation metrics are averaged across all 200 simulation scenarios. Results are shown in the first column of Table 4.

The aforementioned results are further improved by taking into account the nodes' dominant-source proximity indicated by the MVs. In this case, the predicted gender label of a cluster is given by the sum of MV-weighted node predictions normalized by the sum of MVs. In the second column of Table 4, it is observed how the MV-weighting has a positive effect on gender recognition performance as smaller/larger distances between sources and nodes imply less/more reverberation and signal interference, thus leading to more/less accurate node-wise gender predictions.

Moreover, in an additional experiment, the MVs smaller than a threshold v are set to 0 to exclude poorly performing nodes. The threshold is systematically varied and results are shown in the second to last columns of Table 4. The results from the previous experiment where no thresholding was used correspond to $v = 0$. It is observed that for an increasing v , gender recognition scores gradually improve. This, in conjunction with the previous results, indicates that the proposed clustering approach has a significant performance-enhancing effect on a network-wide task.

5. CONCLUSIONS AND OUTLOOK

We have proposed an unsupervised adaptation of CFL to ASN scenarios by using a light-weight autoencoder as server and isolating a subset of its parameters for re-initialization and re-training in FL rounds. An additional bi-partitioning indicator was introduced along with a novel method for generating cluster membership values. It has been empirically demonstrated that the presented privacy-aware approach offers good clustering performance by means of cluster-to-source distance measures and the performance of a multi-sensor gender recognition task. A more comprehensive investigation using a larger variety of acoustic conditions along with a more detailed assessment of privacy risks is planned for future works.

6. REFERENCES

- [1] Maximo Cobos, Juan J. Perez-Solano, and Lars T. Berger, "Acoustic-based technologies for ambient assisted living," *Introduction to Smart eHealth and eCare Technologies*, pp. 159–180, 2016.
- [2] Nilesh Madhu, Sebastian Gergen, and Rainer Martin, "A robust sequential hypothesis testing method for brake squeal localisation," *The Journal of the Acoustical Society of America*, vol. 146, no. 6, pp. 4898–4912, 2019.
- [3] Jeong-Sik Park and Seok-Hoon Kim, "Sound learning-based event detection for acoustic surveillance sensors," *Multimedia Tools and Applications*, pp. 1–13, 2019.
- [4] Sebastian Gergen, Anil Nagathil, and Rainer Martin, "Classification of reverberant audio signals using clustered ad hoc distributed microphones," *Signal Process.*, vol. 107, no. C, pp. 21–32, Feb. 2015.
- [5] Sebastian Gergen, Rainer Martin, and Nilesh Madhu, "Source separation by fuzzy-membership value aware beamforming and masking in ad hoc arrays," in *Speech Communication; 13th ITG-Symposium*, 2018, pp. 1–5.
- [6] Gurjot Singh Gaba, Gulshan Kumar, Himanshu Monga, Tai-Hoon Kim, and Pardeep Kumar, "Robust and lightweight mutual authentication scheme in distributed smart environments," *IEEE Access*, vol. 8, pp. 69722–69733, 2020.
- [7] Nicolas Papernot, Patrick McDaniel, Arunesh Sinha, and Michael P. Wellman, "SoK: Security and privacy in machine learning," in *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2018, pp. 399–414.
- [8] European Parliament and Council, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," 2016.
- [9] Felix Sattler, Klaus-Robert Müller, and Wojciech Samek, "Clustered federated learning: Model-agnostic distributed multitask optimization under privacy constraints," *IEEE Transactions on Neural Networks and Learning Systems*, pp. 1–13, 2020.
- [10] Jakub Konečný, Brendan H. McMahan, Daniel Ramage, and Peter Richtárik, "Federated optimization: Distributed machine learning for on-device intelligence," *arXiv preprint arXiv:1610.02527*, 2016.
- [11] Brendan H. McMahan, Eider Moore, Daniel Ramage, and Blaise Agüera y Arcas, "Federated learning of deep networks using model averaging," *arXiv preprint arXiv:1602.05629*, 2016.
- [12] Ivan Himawan, Iain McCowan, and Sridha Sridharan, "Clustering of ad-hoc microphone arrays for robust blind beamforming," in *2010 IEEE International Conference on Acoustics, Speech and Signal Processing*. IEEE, 2010, pp. 2814–2817.
- [13] Mohamad Hasan Bahari, L. Khadidja Hamaidi, Michael Muma, Jorge Plata-Chaves, Marc Moonen, Abdelhak M. Zoubir, and Alexander Bertrand, "Distributed multi-speaker voice activity detection for wireless acoustic sensor networks," *arXiv preprint arXiv:1703.05782*, 2017.
- [14] Sebastian Gergen, Rainer Martin, and Nilesh Madhu, "Source separation by feature-based clustering of microphones in ad hoc arrays," in *16th International Workshop on Acoustic Signal Enhancement, IWAENC 2018, Tokyo, Japan, September 17-20, 2018*. 2018, pp. 530–534, IEEE.
- [15] Wenxiu Ding, Xuyang Jing, Zheng Yan, and Laurence T. Yang, "A survey on data fusion in internet of things: Towards secure and privacy-preserving fusion," *Information Fusion*, vol. 51, pp. 129–144, 2019.
- [16] Lotfi A. Zadeh, "Fuzzy sets," *Inf. Control.*, vol. 8, no. 3, pp. 338–353, 1965.
- [17] Alexandru Nelus, Sebastian Gergen, and Rainer Martin, "Analysis of temporal aggregation and dimensionality reduction on feature sets for speaker identification in wireless acoustic sensor networks," in *19th IEEE International Workshop on Multimedia Signal Processing, MMSP 2017, Luton, United Kingdom, October 16-18, 2017*. 2017, pp. 1–6, IEEE.
- [18] Qiang Yang, Yang Liu, Tianjian Chen, and Yongxin Tong, "Federated machine learning: Concept and applications," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, pp. 12:1–12:19, 2019.
- [19] Felix Sattler, Klaus-Robert Müller, Thomas Wiegand, and Wojciech Samek, "On the byzantine robustness of clustered federated learning," in *2020 IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2020, Barcelona, Spain, May 4-8, 2020*. 2020, pp. 8861–8865, IEEE.
- [20] Felix Sattler, Simon Wiedemann, Klaus-Robert Müller, and Wojciech Samek, "Robust and communication-efficient federated learning from non-i.i.d. data," *IEEE Trans. Neural Networks Learn. Syst.*, vol. 31, no. 9, pp. 3400–3413, 2020.
- [21] Felix Sattler, Simon Wiedemann, Klaus-Robert Müller, and Wojciech Samek, "Sparse binary compression: Towards distributed deep learning with minimal communication," *International Joint Conference on Neural Networks, IJCNN 2019 Budapest, Hungary, July 14-19, 2019*, pp. 1–8, 2019.
- [22] Léon Bottou, "Large-scale machine learning with stochastic gradient descent," in *Proceedings of COMPSTAT'2010*, pp. 177–186. Springer, 2010.
- [23] Chiyuan Zhang, Samy Bengio, Moritz Hardt, Benjamin Recht, and Oriol Vinyals, "Understanding deep learning requires rethinking generalization," in *5th International Conference on Learning Representations, ICLR 2017, Toulon, France, April 24-26, 2017, Conference Track Proceedings*. 2017, OpenReview.net.
- [24] Vassil Panayotov, Guoguo Chen, Daniel Povey, and Sanjeev Khudanpur, "Librispeech: An ASR corpus based on public domain audio books," in *2015 IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2015, South Brisbane, Queensland, Australia, April 19-24, 2015*. 2015, pp. 5206–5210, IEEE.
- [25] Bengt-Inge Dalenbäck, *TUCT v2.0e:1*, CATT, Mariagatan 16A, SE-41471 Gothenburg, Sweden, 2019.
- [26] Alexandru Nelus, Janek Ebberts, Reinhold Haeb-Umbach, and Rainer Martin, "Privacy-Preserving Variational Information Feature Extraction for Domestic Activity Monitoring versus Speaker Identification," in *Proc. Interspeech 2019*, 2019, pp. 3710–3714.