Federated Domain Adaptation for ASR with Full Self-Supervision

Junteng Jia, Jay Mahadeokar, Weiyi Zheng, Yuan Shangguan, Ozlem Kalinli, Frank Seide

Meta AI

{juntengjia,jaym,wyz,yuansg,okalinli,seide}@fb.com

Abstract

Cross-device federated learning (FL) protects user privacy by collaboratively training a model on user devices, therefore eliminating the need for collecting, storing, and manually labeling user data. While important topics such as the FL training algorithm, non-IID-ness, and Differential Privacy have been well studied in the literature, this paper focuses on two challenges of practical importance for improving on-device ASR: the lack of ground-truth transcriptions and the scarcity of compute resource and network bandwidth on edge devices. First, we propose a FL system for on-device ASR domain adaptation with full self-supervision, which uses self-labeling together with data augmentation and filtering techniques. The system can improve a strong Emformer-Transducer based ASR model pretrained on out-of-domain data, using in-domain audio without any ground-truth transcriptions. Second, to reduce the training cost, we propose a self-restricted RNN Transducer (SR-RNN-T) loss, a variant of alignment-restricted RNN-T that uses Viterbi alignments from self-supervision. To further reduce the compute and network cost, we systematically explore adapting only a subset of weights in the Emformer-Transducer. Our best training recipe achieves a 12.9% relative WER reduction over the strong out-of-domain baseline, which equals 70% of the reduction achievable with full human supervision and centralized training.

Index Terms: ASR, Adaptation, Federated Learning

1. Introduction

With the increasing adoption of deep learning in artificial intelligence applications, data privacy is of growing concern [1, 2]. Automatic speech recognition (ASR) is a particularly sensitive use case due to the personalized nature of speech [3, 4]. Aiming to protect user privacy, cross-device federated learning (FL) has been proposed and applied to a variety of tasks [5, 6, 7, 8]. FL is a distributed training paradigm that allows a loose federation of trainers to collectively improve a shared model [9, 10, 11, 12]. Cross-device FL for ASR faces several unique challenges. These include the lack of ground truth transcriptions; the high costs of computation and network communication; the non-independent and identical distribution of training data (non-IID-ness); and the difficulty of providing privacy guarantees. Several recent works have considered cross-device FL for ASR applications [13, 14, 15, 16, 17, 18]. In particular, weighted model averaging [13, 14] and federated variation noise [16] have been proposed to address the challenge of training on non-IID data, while differential privacy has been proposed to provide formal privacy guarantees [19, 20]. In this paper, however, we address the other two practical challenges for on-device FL: the lack of ground truth transcriptions, and the scarcity of compute resources and network bandwidth.

A common assumption in existing literature on FL for ASR is the availability of ground-truth transcriptions [13, 14, 15, 16, 17, 18]. However, this assumption is not practical. Users of on-device ASR have neither the incentive to manually transcribe their audio, nor the desire to frequently edit inaccurate automatic transcriptions. Assuming no labeled audio data, [11] proposes to use a large pretrained teacher model to label target domain audio on cloud servers; other works, not focused on ASR, have studied semi-supervised FL for keyword spotting, audio classification [21], and image classification [22, 23]. However, to the best of our knowledge, there has been limited literature that explored on-device adaptation for ASR with self-supervision. To this end, we propose an FL system for on-device model domain adaptation with self-supervision that runs alongside an ASR application.

On a high level, user audio and respective automatic transcriptions (pseudo labels) from an on-device ASR model are stored temporarily on the device in an encrypted queue. Then, a trainer that runs alongside the ASR process consumes minibatches of examples from the queue and performs local model updates. Model updates are periodically sent to a central FL server for aggregation. We develop data augmentation and filtering techniques to improve robustness of the self-supervised learning. Our offline experiments on two diverse FL adaptation scenarios confirm the effectiveness of the proposed system.

Another important challenge in cross-device FL is the cost of training and synchronization with the central FL server [10], since edge devices typically have limited compute, battery, and network resources [9]. In this work, we present a combination of techniques to improve an Emformer-Transducer based ASR model [24, 25], which is trained with the RNN-T loss [26]. First, to reduce the compute cost during on-device adaptation,
we propose a self-restricted (SR)-RNN-T loss, which extends the alignment-restricted (AR)-RNN-T [27] by replacing the external alignment with a Viterbi alignment (similar to [28]) from the model itself. Secondly, to further reduce the network cost during synchronization, we consider only adapting a subset of model weights. Inspired by a recent work on speaker adaptation [29], we study which subset of weights in the ASR model would give the best domain-adaptation performance. We find that it is important for adaptation performance to use confidence filtering and data augmentation. Finally, after K updates, the difference $\Delta^{(i)}$ is sent back to the central FL server for aggregation.

### 2.2. Efficient RNN-T Adaptation with Self-Alignment

We use an Enformer-Transducer [26, 33] as our ASR model, pretrained with AR-RNN-T loss and centralized distributed data-parallel (DDP) training. Let $x$ denote the audio features over $T$ time steps and $y$ denote the reference text over $U$ target tokens. First, the encoder maps the audio features $x$ to input embeddings $h$, and the predictor maps the reference tokens $y$ into output embeddings $g$. Then, a joiner network combines every pair of $h, g_u \in h, g$ to compute the probability distribution $Pr(\hat{h}, g_u)$ over all possible output tokens including blank. During training, the RNN-T loss optimizes the sum of the probabilities over all possible audio-text alignments. During inference, a beam search algorithm is used to output the most probable sequence, which we refer to as $\hat{y}$.

In FL scenario, $y$ is not available. Instead, we use the most probable sequence $\hat{y}$ from inference as target labels. A straightforward implementation of the RNN-T loss would directly use $x$ and $\hat{y}$ and optimize over all possible alignments. However, this approach is computationally intensive. As a potential alternative, [27] showed that the AR-RNN-T loss can greatly reduce memory and compute by restricting the forward-backward algorithm to a band around a ground truth alignment. However, AR-RNN-T relies on external ground-truth alignments generated offline with a separate hybrid model. Motivated by recent studies [28], we propose to use Viterbi forced-alignment from the model itself in place of an external alignment. Particularly, the forced-alignments are computed on the fly over the RNN-T grid using the backtracing (see Fig. 2). We refer
the resulting loss function as self-restricted (SR)-RNN-T loss. In our design of the FL system, the Viterbi forced-alignment is further approximated with the most probable alignment encountered during beam search decoding after pruning.

2.3. Data Filtering and Augmentation

One main concern with self-supervision is the quality of the pseudo labels \( \hat{y} \). Incorrect pseudo labels carry the risk of reinforcing errors. We find an effective mitigation to be data filtering, where all utterances with \( \log P(\hat{y}) < \theta \) are discarded. The threshold \( \theta \) is a tunable hyper-parameter, which is empirically determined on a small development dataset. We find that data filtering is especially important if adaptation domain data is noisy (see section 3.4).

On the other hand, when the target domain audios are clean, we find the semi-supervised self-training can be further boosted with data augmentation (speed perturbation and additive noise) while keeping the pseudo labels unchanged (see section 3.3).

2.4. Finetuning Only a Subset of Model Weights

To reduce the cost of computation, memory, and communication, we consider adapting and synchronizing only a subset of model weights. Inspired by a recent study [29], we systematically studied which subset of weights in the Emformer-Transducer model provides the best trade-off between domain-adaptation performance vs. communication cost. We explore adaptation of encoder, predictor and joiner separately. Within the encoder, we carefully analyze adapting only attention or attention key/value matrices. We find adapting the key/value matrices is very effective for the target domain, and freezing the rest of weights serves as a regularization technique, which prevents catastrophic forgetting on the source domain.

3. Experiments

Table 1: Different experiment setups for simulating diverse set of FL experiments. The 1st row in each setup denotes the source domain data used for model pretraining, and 2nd row denotes the target domain data used for FL adaptation.

<table>
<thead>
<tr>
<th>Setup</th>
<th>Dataset</th>
<th>Train (hours)</th>
<th>Eval (utterances)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Mixture</td>
<td>1.5M</td>
<td>3.6K</td>
</tr>
<tr>
<td></td>
<td>Edge</td>
<td>9.7K</td>
<td>28.6K</td>
</tr>
<tr>
<td>Video</td>
<td>Clean</td>
<td>17.4K</td>
<td>1.2K</td>
</tr>
<tr>
<td></td>
<td>Noisy</td>
<td>1.2K</td>
<td>1.5K</td>
</tr>
</tbody>
</table>

3.1. Data Setup

To simulate realistic federated learning in practical scenarios, we consider two different experiment setups. Each setup takes a converged model pretrained on a source domain and performs FL adaptation to a target domain. The adapted model is tested on the evaluation data from both the source and target domains. Table 1 gives more information on the data used in each setup.

Device: This setup closely resembles a cross-device FL use case. For pretraining, we use a mixture of data sources, including public videos, audios collected by paid third-party vendors on portal, and synthetic audios generated by text-to-speech. This dataset contains 1.5 Million hours of audios, which are transcribed either through human annotators or a large teacher model (see [34] for details). For adaptation, we use assistant and dictation audios recorded on edge devices, which are collected by external vendors under clean acoustic conditions. The source domain evaluation data is a separably prepared conversation dataset, while the target domain evaluation data is held out subset of the on-device recordings.

Video: For pretraining, we use 17.4K hours of long form videos (averaged 45 sec) with relative clean audios. For adaptation, we use short form videos (averaged 12 sec) that might be recorded in noisy environments. A subset of the audios from both the clean and noisy videos are held out for evaluation.

3.2. Modeling

Our ASR model is an Emformer-Transducer [33]. Features are 80 mel-spaced log filter-bank channels with a sliding window of 25ms at 10ms frame shift, regularized with SpecAugment [35]. A time reduction layer stacks features with a stride of 6, and the resulting 480-dimensional vectors form the input to the encoder. The predictor is a 2-layer LSTM model with a hidden dimension of 256. Both the encoder and the predictor outputs are projected to 768-dimension tensors and combined in the RNN-T joiner, which consists of a ReLU followed by a softmax layer with a sentence-piece vocabulary size of 4096.

For each task, we first pretrain the ASR model on the source domain until convergence, using an AR-RNN-T loss with buffer size \( b_l = 5 \), \( b_r = 25 \) and an Adam optimizer with learning rate \( 10^{-3} \) and tri-stage learning rate scheduling. We then finetune the ASR model to the target domain using 32 parallel workers. Each worker uses an Adam optimizer with a fixed learning rate of \( 10^{-4} \) for local model updates. The local models on different workers are synchronized every 20 local updates using FedAvgBMUF with a block momentum of 0.8.

3.3. Device Adaptation

The Device adaptation setup adapts from the source domain “Mixture” to the target domain “Edge”. The baseline pretrained model achieves a lower WER on the target domain (4.96) than on the source domain (6.07), since the latter captures diverse acoustic conditions while the former is a commissioned data collection that is mostly clean.

Lower bound: We first consider supervised adaptation with centralized DDP training, using the ground-truth labels and the AR-RNN-T loss. The adapted model’s WER on the source and target domains across different checkpoints are plotted in figure 3 ①. In particular, the best checkpoint (see table 2 ②) reduces the WER 4.96 \( \rightarrow 4.05 \) on the target domain, which serves as a lower bound for semi-supervised FL adaptations. We also observe a slight WER increase 6.07 \( \rightarrow 6.12 \) on the
source domain.

**FedAvgM/BMUF:** Next, we look at the effect of using the FL training algorithm, by replacing DDP with FedAvgM/BMUF while keeping the labels and the loss function the same (2). We observe a marginal WER increase on both the target domain (to 4.09) and the source domain (to 6.16).

Table 3: The effect of data augmentation. When target domain is clean, adaptation is less effective without data augmentation.

<table>
<thead>
<tr>
<th>Model</th>
<th>Target</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>①</td>
<td>3.1 (4.4%) 4.68 6.19</td>
<td>②</td>
</tr>
<tr>
<td>① - Data Augment</td>
<td>4.35 6.17</td>
<td>③</td>
</tr>
<tr>
<td>① - Data/Spec Augment</td>
<td>4.48 6.44</td>
<td>⑤</td>
</tr>
</tbody>
</table>

**Pseudo labels:** Now, we introduce pseudo labels to determine the effects of self-supervision (3). Although not as effective as the true labels, self-supervision still reduces the pretrained model’s WER on the target domain 4.96 → 4.35. We note the data filtering techniques discussed in section 2.3 greatly contributes to the success of self-supervision. Without filtering, adaptation with the pseudo labels becomes much less effective, causing a WER increase on the target domain 4.35 → 4.48 (see table 3). If we also remove SpecAugment, the target domain WER further increases to 4.89. On the other hand, confidence filtering makes little difference since the target domain WER of the pretrained model is already low.

**SR-RNN-T:** To reduce on-device computation cost, the proposed SR-RNN-T loss restricts the forward/backward to a limited window of 2 frames around the most probable alignment (b = b_r = 2) according to the respective current model. The SR-RNN-T trained model is marginally more accurate than the AR-RNN-T on both target (4.32) and source domain (6.08).

**KeyValue adaptation:** Lastly, we experiment with finetuning only subsets of the model weights (see table 4). Finetuning only the key/value matrices of the self-attention module not only achieves a low target domain WER (4.32), but also prevents catastrophic forgetting on the source domain as the number of updates increases (see figure 3). Most importantly, communication is greatly reduced as key/value matrices only account for 5.7% of all weights. Similarly, finetuning only the bias also has the same benefits, however, it takes more updates to converge.

3.4. Video Adaptation

The Video adaptation setup adapts from the source domain “Clean” to the target domain “Noisy”. The adaptation results are summarized in figure 4 and table 5, and they confirms most of our conclusions in section 3.3. In particular, FL adaptation of key/value matrices with pseudo labels (5) effectively reduces the WER on the target domain (14.91 → 13.36). Moreover, we have two additional learnings.

**Filtering:** Since the audios in the target domain is noisy, the pseudo labels from the pretrained model have a significant error rate. We find it necessary to apply confidence filtering using the decoding scores to remove low-confidence examples. The optimal threshold parameter \(\theta = -0.2\) removes 77% of training examples. As shown in table 5 row 8, semi-supervised adaptation is much less effective when confidence filtering is removed, which negates most of the gains (14.91 → 14.72).

**KeyValue adaptation:** Adapting only the key/value weights outperforms full model adaptation by large margins on both target (13.36 vs. 13.74) and source domain (9.43 vs. 10.08). Moreover, the adapted model even outperforms the pretrained model on the source domain (9.43 vs. 10.30). This is likely because the target domain contains more diverse audio.

4. Conclusions

This paper addressed two practical challenges for domain adaptation of an Emformer-Transducer ASR model on edge devices using Federated Learning. First, we show that the combination of self-restricted RNN-T loss with data augmentation and filtering techniques can improve an on-device ASR model on target domain data with full self-supervision. Second, we explored techniques reducing the FL compute and network communication costs by adapting only a subset of weights in the model. We will further explore effects of non-IID-ness and differential privacy on our proposed techniques as part of future work.
5. References


