Towards Federated Unsupervised Representation Learning

BRAM VAN BERLO, AAQIB SAEED AND TANIR OZCELEBI
Current Situation

Labeled data for model training
• Extensive number centrally aggregated

Ever-increasing number of IoT devices
• Data hard to aggregate
• Active learning is undesirable

Privacy concerns
• GDPR

Supervised architecture # of labeled training data used
ResNet 1.28M images
Deep Speech 2 English: 12K hours
VGG 1.3M images
Unsupervised Representation Learning

Methodology
• Pre-train with unlabeled data
• Extract high-level features from labeled data
• Train down-stream task with labeled data

Existing literature
• Limited to centralized context
Federated Machine Learning

Communication round overview

Step 1: distribute
- 1 server
- Global model parameters $\theta$
- $K$ clients

Step 2: local updates
- Local model parameters $\theta_k$
- Local dataset

Step 3: aggregate
- Local model parameter update $H_k$

Step 4: global update
- $\theta = f(\theta, H_1 \ldots H_k)$

Towards Federated Unsupervised Representation Learning
Federated Machine Learning

Existing implementations
• Implicitly labeled data from user interaction

Next word prediction

Bookmark suggestion optimization
Federated and Self-supervised Learning

Auxiliary task data generation
- Automated pre-processing step on devices

Compared to active learning
- No human involvement
Contributions

Pre-training models with unlabeled data at IoT devices

Introduction of FURL

Effectiveness demonstration against supervised learning
Effectiveness Demonstration Methodology

Supervised, autoencoder, and self-supervised network

- Encoder-decoder TCN
- Common trunk

Three human activity detection datasets

- HHAR, MobiAct and HAPT

Performance assessment (test data)

- 5-fold user-split cross validation
- Metrics: F1 and Kappa score
Preliminary findings – baseline comparison

(Un)labeled data share
- Classes
- Generative distribution

Compared to supervised learning: mixed results
- MobiAct, HHAR: on par
- HAPT: worse

Baseline comparison - federated setting

<table>
<thead>
<tr>
<th>Score</th>
<th>Supervised</th>
<th>Autoencoder</th>
<th>Self-supervised</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>F1</td>
<td>Kappa</td>
<td>HHAR</td>
</tr>
<tr>
<td></td>
<td>MobiAct</td>
<td>Kappa</td>
<td>MobiAct</td>
</tr>
<tr>
<td></td>
<td>HAPT</td>
<td>Kappa</td>
<td>HAPT</td>
</tr>
</tbody>
</table>
Preliminary findings – feature transferability

Down-stream end-to-end training on HHAR, HAPT

Pre-training with MobiAct
• More classes
• Bigger generative distribution

Compared to supervised learning
• On average slightly outperforming
Future Work

Experiment extensions
• Non-IID data
• Other application domains

Privacy and security attack handling

Compound model scaling

New modalities and frameworks

Want to collaborate?

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bram van Berlo*</td>
<td><a href="mailto:b.r.d.v.berlo@tue.nl">b.r.d.v.berlo@tue.nl</a></td>
</tr>
<tr>
<td>Aaqib Saeed</td>
<td><a href="mailto:a.saeed@tue.nl">a.saeed@tue.nl</a></td>
</tr>
<tr>
<td>Tanir Ozcelebi</td>
<td><a href="mailto:t.ozcelebi@tue.nl">t.ozcelebi@tue.nl</a></td>
</tr>
</tbody>
</table>

* Corresponding author