WASP Project Course 2021

Federated Learning for Safety Assurance of ADSs

Background

This project aims at investigating and implementing Federated Learning (FL) of traffic behavioural models used for safety analysis, assurance, design-decisions and run-time decision-making in automated driving systems (ADS). In a production setting, the behavioural models should be updated using local data experienced by each vehicle and these local model parameters, which are shared with a central entity, are aggregated to form an updated global model. Compared to common models used for FL we proposed to use Gaussian Mixture Models (GMMs), which are adequate to capture traffic behaviours and also has the property of reliable statistical confidence intervals required for safety assurance. The proposed key question of this project is: What are suitable aggregation functions for GMMs to conduct FL? There are several challenges in answering this question (1) what KPIs help in judging the suitability of an aggregation function? (2) How to ensure that rare cases of traffic behaviour is adequately captured in the aggregation? and (3) What are the implications to the global GMM from not having independent and identically distributed samples at the clients? It is the task of this project to investigate potential solutions to challenges 1-3 as well as to provide a first implementation (POC) of such a FL scheme using real traffic data. The identified solutions should be compared and evaluated using the implemented POC and the identified KPIs.

Please refer to the extended project description for more information.

Constraints: None identified. We will be able to run the project "working on distance".

Participants

Industrial partner: Zenseact AB

Industrial supervisor: Majid Khorsand Vakilzadeh, majid.vakilzadeh@zenseact.com, and Mina Alibeigi Nabi, mina.alibeigi@zenseact.com

Academic supervisor: Andreas Hellander, andreas.hellander@it.uu.se, Uppsala University

Coordinating WARA representative: ?, WARA-Common

Suggested WASP PhD students: Magnus Gyllenhammar (Zenseact/KTH) (magnus.gyllenhammar@zenseact.com), and Muhammad Rusyadi Ramli (KTH)

Challenges to investigate

With the proposed research question for the project: **What are suitable aggregation functions for GMMs to conduct FL?** we have identified three main challenges:

1. What KPIs help in judging the suitability of an aggregation function?
2. How to ensure that rare cases of traffic behaviour is adequately captured in the aggregation? and
3. What are the implications to the global GMM from not having independent and identically distributed samples at the clients?

Resources

Data set in terms of HighD-dataset (German highways) and a dataset shared by Viscando. We will also consider using Zenseact's internal data as an additional dataset.
Potentially, use computational resources provided by WARA-Common, but might not be necessary considering the computational requirements of the proposed models (GMMs). As this project is relevant to the scope of EdgeLab an additional alternative is to use those resourses.

Deliverables

- Compare state of the art methods for aggregation of model parameters in FL (Examples include: Fedavg, IterativeAvg, Gradient Average, PFNM, Krum, Coordinated median, Zeno, SPAHM. Note that a reasoable scope for the project would be to select a few for evaluation and comparison.) for the application of GMMs,
- Identify useful KPIs to assess the effectiveness of the aggregation,
- Implement a proof of concept (in FEDn[1]) of this idea using (at least) one aggregation method across (at least) one of data set with traffic behaviour on highway (out of the ones discussed in Resources), and
- Evaluate and compare the selected aggregation methods with respect to the identified KPIs.

References

Please refer to the extended project description for a complete list of references and more elaborate description.

Keywords

Safety, Automated driving, ADS, Federated learning, statistical modelling, GMM, traffic behaviour, FEDn

[1] https://github.com/scaleoutsystems/fedn