Analysis 1: A Survey of Federated Learning for Connected and Automated Vehicles

Objective:

This Research paper dives into methodologies that can be used to circumvent data and privacy issues when it comes to Connected and Automated Vehicles (CAVs), while training models using data from these vehicles.

Method:

The Paper suggests Federated Learning, a method where the central server sends a generic model to each car, and the car trains this model using its own data (Cameras, LiDAR, GPS). The car then only sends back the mathematical aspect of this model (weights), and the central server receives these weights and can combine it with other weights it receives using a Federated Average algorithm. The combined model can now be sent back to the car, which will now be trained on a variety of data. This process can be repeated to make the central model smarter without exposing and personably identifiable information. This central system is implemented using blockchain or encryption to maintain security.

Results:

Federated Learning complies with privacy laws since the raw data will never leave the car. The overall quality of the model will be fairly high since its trained-on data from countless cars and can easily handle unseen circumstances if even one other car experienced it first. The overall accuracy goes up as the model iterates through multiple levels of training using these cars, getting smarter each time.

Future Directions:

There are certain caveats to this type of learning. The most prominent issues that need to be addressed are:

- The model may forget old lessons as it learns new ones.
- Validation against any data that is compromised, as it will infect the rest of the cars as well.
- Hardware optimizations might be needed so the process does not unnecessarily tax the computing or battery

Analysis 2: Explainable Traffic Flow Prediction with Large Language Models

Objective:

This Research paper aims to solve the interpretability issue of traditional deep learning models, where the predictions are often correct but very difficult for humans to understand. The objective is to develop framework that not only predicts traffic volume but also explains why it predicated as such.

Method:

The methodology provided starts with annotating the multi-modal data (traffic, weather, landmarks, dates) and convert these into textual prompts. This data is now sent as an input to an LLM, armed with Chain of Thought prompting, so the LLM can be guided through the data thoroughly. The model used is the Llama2-7B-chat, fine-tuned using LoRA, which allows for adaptation to local data without retraining the whole model. Using the LLM's ability to predict tokens, the model outputs a consistent object that contains the forecast and an explanation.

Results:

This methodology outperformed many deep learning models (GWNET, STGCN) beating the next best model by 18.37% in MAE, and 34.00% in MAPE. The zero-shot capability was also remarkable, with the model predicting accurate on cities it was not trained on, outperforming even GPT-4. The explanations provided were also highly logical and well-constructed, often taking into account real scenarios.

Future work:

The framework was a success, but there are a few improvements that can be made.

- The framework can be improved at understanding the relation between multiple sensors to predict more accurately.
- The framework can be adjusted to allow for real-time data, so it can account for unexpected events and predict accordingly.
- This framework can be used as a proof of concept to build a much larger "City wide" LLM that can be used for other tasks like Urban planning.