FEDERAL UNIVERSITY OF PARÁ
INSTITUTE OF TECHNOLOGY
POSTGRADUATE PROGRAM IN ELECTRICAL ENGINEERING

JOHN LUCAS RODRIGUES PORTILHO DE SOUSA

ENTROPY-BASED CLIENT SELECTION STRATEGY FOR FEDERATED LEARNING OVER VEHICULAR NETWORK ENVIRONMENTS

UFPA / ITEC / PPGEE

Belém-Pará-Brazil

2024

FEDERAL UNIVERSITY OF PARÁ
INSTITUTE OF TECHNOLOGY
POSTGRADUATE PROGRAM IN ELECTRICAL ENGINEERING

JOHN LUCAS RODRIGUES PORTILHO DE SOUSA

ENTROPY-BASED CLIENT SELECTION STRATEGY FOR FEDERATED LEARNING OVER VEHICULAR NETWORK ENVIRONMENTS

Master thesis submitted to the judging panel at the Federal University of Pará as part of the requirements for obtaining a Master's Degree in Electric Engineering.

Advisor: Dr. Eduardo Coelho Cerqueira
Co-advisor: Dr. Denis Lima do Rosario

UFPA / ITEC / PPGEE
Belém-Pará-Brazil

2024

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD
Sistema de Bibliotecas da Universidade Federal do Pará
Gerada automaticamente pelo módulo Ficat, mediante os dados fornecidos pelo(a) autor(a)

R696e Rodrigues Portilho de Sousa, John Lucas.
Entropy-based Client Selection Strategy for Federated Learning over Vehicular Network Environments / John Lucas Rodrigues Portilho de Sousa. — 2024.
56 f. : il. color.

Orientador(a): Prof. Dr. Denis Lima do Rosário
Coorientador(a): Prof. Dr. Eduardo Coelho Cerqueira
Dissertação (Mestrado) - Universidade Federal do Pará, Instituto de Tecnologia, Programa de Pós-Graduação em Engenharia Elétrica, Belém, 2024.

1. Federated Learning. 2. Machine Learning. 3. Connected and Autonomous Vehicles. I. Título.

CDD 006.3

UNIVERSIDADE FEDERAL DO PARÁ
INSTITUTO DE TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

JOHN LUCAS RODRIGUES PORTILHO DE SOUSA

ENTROPY-BASED CLIENT SELECTION MECHANISM FOR VEHICULAR FEDERATED LEARNING ENVIRONMENT

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal do Pará como requisito para obtenção do título de Mestre em Engenharia Elétrica, defendida e aprovada em 13/08/2024, pela banca examinadora constituída pelos seguintes membros:

PROF. DR. DENIS LIMA DO ROSÁRIO
(UFPA - Presidente)

PROF. DR. EDUARDO COELHO CERQUEIRA
(UFPA - Coorientador - UFPA)

PROF. DR. DIEGO LISBOA CARDOSO
(PPGEE - Examinador Interno)

PROF. DR. IAGO LINS DE MEDEIROS
(UFPA - Membro Externo À Instituição)

Abstract

Entropy-based Client Selection Strategy for Federated Learning over Vehicular Network Environments

Advisor: Eduardo Coelho Cerqueira
Co-advisor: Denis Lima do Rosario
Key words: Federated Learning; Vehicular Networks; Connected and Autonomous Vehicles; Client Selection; Entropy; Client Failures;

Federated Learning (FL) emerges as a promising solution to enable collaborative model training for autonomous vehicles while preserving privacy and addressing communication overhead issues. Efficient client selection for participation in the training process remains challenging, especially in scenarios with statistical heterogeneity of data distribution and client failure events. Client failure, an uncontrollable event during training, reduces accuracy, convergence, and speed. This master thesis introduces an entropy-based client selection mechanisms for FL over Vehicular Network environments with client failure and non-IID data distributions. The proposed method is compared to a random selection mechanism in both IID and non-IID scenarios, as well as scenarios with random client drops. The results demonstrate that entropy-based selection outperforms other methods regarding training loss, accuracy, and Area Under the Curve (AUC), particularly in high client dropout and non-IID scenarios. These findings highlight the importance of considering entropy data for client selection to address the challenges posed by client failure and statistical heterogeneity in FL over Vehicular Network.

Resumo

Estratégia de Seleção de Clientes Baseada em Entropia para Aprendizado Federado em Ambientes de Redes Veiculares

Orientador: Eduardo Coelho Cerqueira
Co-orientador: Denis Lima do Rosario
Palavras-chave: Aprendizado Federado; Redes Veiculares; Veículos Conectados e Autônomos; Seleção de Clientes; Entropia; Falhas de Clientes.

Aprendizado Federado (FL) surge como uma solução promissora para possibilitar o treinamento colaborativo de modelos para veículos autônomos, preservando a privacidade e abordando questões de sobrecarga de comunicação. A seleção eficiente de clientes para participar do processo de treinamento permanece desafiadora, especialmente em cenários com heterogeneidade estatística da distribuição de dados e eventos de falha de clientes. A falha de clientes, um evento incontrolável durante o treinamento, reduz a precisão, a convergência e a velocidade. Esta dissertação de mestrado introduz mecanismos de seleção de clientes baseados em entropia para FL em ambientes de Redes Veiculares com falha de clientes e distribuições de dados não-IID. O método proposto é comparado a um mecanismo de seleção aleatória em cenários tanto IID quanto não-IID, bem como em cenários com quedas aleatórias de clientes. Os resultados demonstram que a seleção baseada em entropia supera outros métodos em relação à perda de treinamento, precisão e Área Sob a Curva ROC, especialmente em cenários com alta taxa de desistência de clientes e dados não-IID. Esses achados destacam a importância de considerar dados de entropia para a seleção de clientes para abordar os desafios impostos pela falha de clientes e pela heterogeneidade estatística no FL sobre Redes Veiculares.

Acknowledgement

I dedicate my sincere thanks to:

– To Professor Denis Rosário for the guidance, support, and patience he offered me to achieve academic maturity.

– To Professor Eduardo Cerqueira, for the precious methodology knowledge and pieces of advice in the research field and life.

– To all my LACIS colleagues, especially Eduardo, Rafael, Lucas and Matheus who helped me with reviews and tips.

– To my friends, who gave me hope and joy to face life's challenges.

– To the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Finance Code 001.

– This work was partially supported by the Ministry of Science, Technology and Innovation (MCTI) (Brazil), with resources from Law No. 8,248, of October 23, 1991, within the scope of PPI-Softex, coordinated by Softex and published as Agentes inteligentes para plataformas móveis baseados em tecnologia de Arquitetura Cognitiva (processo 01245.013778/2020-21).

"Assim como no futebol, na vida acadêmica, o trabalho em equipe, a estratégia e a dedicação são fundamentais para alcançar a vitória."
John Lucas

Contents

List of Abbreviations

AUC	Area Under the Curve
CAVs	Connected and Autonomous Vehicles
CKA	Centroid-Based Kernel Alignment
DL	Deep Learning
DSRC	Dedicated Short Range Communication
FedAvg	Federated Averaging
FL	Federated Learning
FPR	False Positive Rate
ITS	Intelligent Transportation Systems
LiDAR	Light Detection and Ranging
LuST	Luxembourg SUMO Traffic
ML	Machine Learning
MLP	Multi-Layer Perceptron
NN	Neural Network
Non-IID	Non-Independent and identically distributed
RiCA	Resilience-aware Client Selection Mechanism
ROC	Receiver Operating Characteristic
RSU	Roadside Unit

SGD	Stochastic Gradient Descent
TPR	True Positive Rate

List of Figures

List of Tables

CHAPTER 1

Introduction

This dissertation proposes a novel client selection for Federated Learning (FL) environments using the entropy of the labels of data. This chapter introduces some of the main ideas regarding the application of the entropy method to assess the quality of the client data, vehicular environment challenges, non-iid data. Additionally, it motivates this research work and establishes the research questions, objectives, contributions and thesis structure.

1.1 Overview

The preservation of data privacy emerges as a paramount concern in smart cities, especially in sensitive domains, such as Connected and Autonomous Vehicles (CAVs). Autonomous driving require sophisticated learning functions related to driving, which requires a vast volumes of data [1]. In this sense, these vehicles are equipped with a comprehensive set of onboard sensors, including cameras, radar, Light Detection and Ranging(LiDAR), proximity sensors, and temperature sensors, to collect multi-modal data essential for navigation, perception, obstacle detection, and vehicle control [2]. CAVs rely on vehicular network technology to enable data sharing with neighbors and edge servers, providing data processing for a cooperative understanding of the environment among vehicles and infrastructure entities [3]. Vision-related tasks, such as steering wheel angle prediction [4], traffic sign recognition [5], semantic segmentation [6], object detection [7], and driver monitoring [8] typically use images captured by the camera as the data source. In this context, Deep Learning (DL) plays a pivotal role with its ability to extract meaningful patterns and insights from large datasets. By leveraging these datasets, services such as route-optimization, predictive maintenance, real-time decision-making, and personalized in-vehicle experiences can be enhanced [9].

Traditional Machine Learning (ML) algorithms are predominantly cloud-centric, where data is stored and processed centrally on cloud servers [10]. However, the widespread data sharing between CAVs and servers poses significant privacy risks, as well as demand substantial network bandwidth. In response to these challenges, there is an urgent need for a privacy-preserving distributed ML solution for CAV environments. In addition, it is believed that the future of ML and cloud computing schemes will be distributed at the network edges [11].

In recent years, FL, driven by ML, has garnered significant attention in this area due to its decentralized nature, which allows data training locally on devices. FL enables multiple clients (*e.g.*, CAVs) to collaboratively train a shared model without sharing individual data [12, 13, 14]. Specifically, FL considers the distributed ML process by allowing mobile devices (*i.e.*, clients) to train models locally. The locally trained models send their ML parameters (*i.e.*, Neural Network Weight) to a central server, which aggregates the parameters of different clients under a specified aggregation policy (*e.g.*, averaging). Afterward, the server returns a consolidated model to the clients, and the clients participating in the federation retrain it with local data. In this context, clients do not share their private raw data with a centralized server, reducing data transmission between the client and a server and mitigating user privacy issues [15]. User data remains private while it indirectly contributes to building improved models.

FL relies on a robust and always connected client selection mechanism deployed at the edge server to choose a group of clients with valuable samples for the model training at each communication round [16]. These selected clients receive the global model, conduct training based on their local data, and then share their model parameters instead of transmitting their raw sensing data, as described in [17]. Afterwards, the shared local models are aggregated at the cloud or edge servers by a given aggregation policy to produce an accurate global model. Finally, the updated global model is distributed to the clients. In this way, FL allows ongoing learning by adapting the ML model without sharing raw data, provides privacy preservation by keeping the collected data stored on the CAVs, and also avoids the potential communication overhead that can be caused by the intense data traffic of CAV information. Hence, integrating FL in CAV systems opens up a variety of possibilities for enhancing vehicular intelligence while addressing privacy, security, and communication challenges [3].

Vehicular FL presents a compelling solution for enhancing model performance in Intelligent Transportation Systems (ITS) by leveraging data from vehicles without compromising privacy or requiring large-scale data transfers to a centralized server. The primary motivation for this research is to improve the efficiency and effectiveness of the method through the use of entropy-based client selection mechanisms. By selecting clients with relevant and diverse data, indicated by clients which have a higher entropy in their data, these mechanisms have the potential to enhance model generalization and convergence speed, ultimately improving the overall performance of ITS applications.

Entropy-based client selection appears as a promising approach for a FL over CAV scenario with client failure, since entropy enables to identify the most relevant client with more diverse data for learning models, capturing the heterogeneity of FL over CAV scenario. In this sense, clients with high entropy ensure that the learned models represent the entire network and capture the scenario variations to improve the accuracy of round training more robustly. However, it is important to understand the impact of arbitrary client failure, and how it affect the performance of a entropy-based client selection mechanism, which are the central questions of this master thesis.

In this context, entropy enables the identification of the most relevant clients by measuring how diverse the client data is, the more variety, the higher the client entropy will be, in that way capturing the heterogeneity of the data presented in CAV scenarios. Clients with high entropy ensure that the learned models represent the entire network and capture scenario variations, thereby improving the accuracy of round training in a more robust manner. However, understanding the impact of arbitrary client failures and how they affect the performance of an entropy-based client selection mechanism are central questions of this thesis.

1.2 Motivations and Challenges

To fully harness the potential of this paradigm, several challenges must be addressed, particularly in the context of entropy-based client selection. First, the mobility of CAVs and the unpredictability of wireless channels can cause fluctuations in vehicle participation in the FL process, making it difficult to maintain consistent training performance. Second, the local data across CAVs is often unbalanced and non-IID, leading to variations in data quality, which can negatively impact model convergence [18]

These challenges can be categorized into three primary areas: data diversity and distribution, representativeness and client connectivity. In the context of client connectivity, ensuring robust model performance despite the variability in CAV participation and data quality is critical. Maintaining efficient data transfer and processing amidst the dynamic network conditions is essential for the practical implementation of vehicular FL. Addressing these issues is important to realize the full potential of entropy-based client selection in enhancing the performance and scalability of ITS applications.

1.2.1 Representativeness in Client Selection

Client selection in FL is essential for optimizing model training efficiency and reducing network load. One of the primary challenges in client selection is ensuring representativeness, especially in scenarios with non-IID. Statistical heterogeneity results in lower classification accuracy because it introduces representativeness issues, potentially decreasing model accuracy and fairness among the participating entities. In this way, it is important to develop a client selection mechanism that can handle non-IID data in dynamic and mobile environments without compromising classification accuracy in FL over CAV scenarios [19].

This method also helps the network avoid overloading. Transmission overhead is a critical factor impacting the FL environment, ensuring that only the most informative updates are transmitted. As the size of the learning model and the number of participating clients increase, so does the size of the model update parameter set and the number of updates, potentially leading to transmission bottlenecks. This approach not only reduces network load but also maintains model performance by leveraging data diversity and minimizing the impact of non-IID data

Fairness in client selection is essential to prevent biases in the model. Ensuring representativeness in client selection directly contributes to this fairness by incorporating a wide range of data sources, which helps in building robust and generalized models. This is particularly important in FL over CAV scenarios where data diversity can significantly impact the performance and accuracy of the model. By selecting a representative subset of clients, the FL process can better capture the underlying data distribution, leading to improved model performance.

1.2.2 Data Distribution

Data diversity arises from the non-uniform distribution of datasets among edge devices, where training data is stored locally. In FL, this non-IID data is common because each device collects data from its specific local environment, leading to significant variations. For instance, in autonomous driving, vehicles in different regions gather image data with distinct features based on their geographic contexts, such as varying lighting conditions or types of traffic signs. These differences result in unique data characteristics across clients, causing significant variances in averaged gradient data and slowing the convergence rate of learning models, particularly neural networks (NNs). The diverse data limits the NN's ability to extract and generalize features effectively, further complicating training.

This imbalance is compounded by system heterogeneity, where edge devices differ in computational power, storage, and network capacity, impacting the volume and type of data they handle. Non-IID data can be classified into two main types: attribute skew and label skew. Attribute skew occurs when feature distributions vary across clients, such as when some vehicles collect daytime data while others gather nighttime data. Label skew refers to differences in label distributions across clients, such as certain road signs being more prevalent in certain regions. Both types of skew hinder the performance of NNs and cause gradient divergence, further slowing down model convergence. The consequences of non-IID data are significant. The biased local datasets lead to inconsistent model updates, which fluctuates the performance of the global model. Models trained under these conditions struggle to generalize across all clients, performing well for some but poorly for others. Additionally, federated averaging, which aggregates updates from all clients, becomes biased due to the uneven data distribution, diminishing the effectiveness of the global model.

1.2.3 Performance under Client Failure Scenarios

In the context of FL for CAVs, client failures pose significant challenges to the learning process. Clients might fail to provide their local model updates due to various reasons, such as insufficient computing resources, client aborts, network failures, and other factors related to their heterogeneous composition [20]. These failures interfere with FL's ability to learn effectively, as only a subset of clients can complete local training and transmit their model updates in each round. This limitation reduces the accuracy, convergence, and training speed of the global model [10]. When clients fail to contribute their local model updates, the overall training data available for the global model update is reduced, and it obtain a biased update that deviates from the desired global model [21]. This reduction in training data lead to slower convergence of the global model and decreased model accuracy. In this context, it is important to design a robust and reliable client selection mechanism for FL over CAV systems, which can be based on random, clustering, entropy, and others approaches [22].

Despite the FL strengths, the system's performance can be significantly impacted by client failure scenarios, where participating clients drop out or fail to complete their local training tasks. Such failures can occur due to various factors, including network instability, limited battery life, or hardware malfunctions. These disruptions can introduce several challenges that affect the overall efficacy of the FL process.

Client failures can lead to inconsistent model updates, as the central server may not receive the expected local model parameters from all participating clients. This inconsistency can slow down the convergence rate of the global model and degrade its overall performance. In addition, since each client in an FL system typically holds a unique subset of the data, the loss of any client results in a reduction of the available training data. This reduction can be particularly problematic in scenarios involving non-IID data distributions, where each client's data is essential for capturing the overall variability in the dataset. [23, 24]

Additionally, frequent client failures can create an imbalance in contributions from different clients. Inconsistent participation means that the model may become skewed towards the data of the more reliable clients, thus reducing the generalization capability of the model. This imbalance can lead to a global model that does not accurately represent the entire data distribution, especially if the data from failed clients contains unique or critical information.

1.3 Research Questions

Based on the above motivation, we considered the following research question for this master thesis: How effective are entropy-based client selection mechanisms in improving model performance in vehicular FL environments compared to other client selection strategies?

1.4 Objectives and Contributions

By addressing this research questions, this master thesis seeks to contribute to the advancement of FL in vehicular environments and provide insights into the effective implementation of entropy-based client selection mechanism for improving FL over vehicular network environments. This work has the following main contributions:

- Introduces an entropy-based client selection strategy for FL over vehicular network environments [17].
- Provides a comprehensive analysis of the reliability and robustness of an entropy-based client selection mechanism in FL environments subject to client failures [25]. It highlights how this mechanism can maintain superior performance regarding training loss, accuracy, and AUC metrics, even in high client failure scenarios.
- Introduces simulation results to compare the entropy-based selection mechanism with other client selection methods, demonstrating its effectiveness in ensuring faster convergence, reduced training loss instability, and higher accuracy across various client failure rates.

1.5 Text Organization

This text presents the fundamentals of this research based on related works, the main milestones already achieved with the prior published papers, and the planned advances for future research works. The remaining of this document is structured as follows:

- Chapter 2: Presents basic concepts regarding the area, such as information about FL, ML, aggregation methods, information of what is entropy and how to use it in CAV. This chapter also presents some of the main challenges of vehicular FL.
- Chapter 3: This chapter reviews the current state-of-the-art in FL, particularly focusing on client selection mechanisms in vehicular networks. It examines various approaches to handle data heterogeneity and connectivity issues in dynamic and distributed environments. The chapter also evaluates different methods for assessing the efficiency and effectiveness of these techniques.
- Chapter 4: This chapter details the proposed entropy-based client selection mechanism, discussing its implementation and the underlying principles. It also analyzes the impact of client failures on the FL process, providing a comprehensive evaluation of the mechanism's performance in such scenarios.
- Chapter 5: This chapter presents the experimental setup, including the environment parameters and the methodology used for the evaluation. It compares the proposed

entropy-based client selection mechanism with other existing methods, highlighting its advantages and effectiveness in various client failure scenarios.

- Chapter 6: This chapter summarizes the key findings of the research, discusses the implications of the results, and suggests directions for future work. It also lists the published works associated with this project.

CHAPTER 2

Basic Concepts

This chapter presents some of the main concepts about FL, what ML techniques are needed, aggregation methods, what the bases for information theory are, and what metrics are used. The main techniques and methodologies are analyzed for user classification.

2.1 Vehicular Federated Learning Environments

CAVs refer to vehicles that integrate two key technologies: automation of driving functions and connectivity with other devices and infrastructure [2]. These vehicles are equipped with advanced sensor technologies, such as LiDAR, radar, and cameras, along with sophisticated algorithms, enabling them to drive and navigate without human intervention. The level of autonomy can vary, typically defined by the levels of driving automation, ranging from Level 0 (no automation) to Level 5 (full automation), where the vehicle performs all driving tasks under all conditions. CAVs not only operate autonomously but also have the capability to communicate with other vehicles, infrastructure, pedestrians, and the network using wireless communication technologies. This connectivity enables a wide range of functions, such as real-time traffic updates, safety warnings, and remote diagnostics. It also allows CAVs to respond to dynamic road conditions, enhancing their ability to operate safely and efficiently.

The integration of connectivity and automation provides CAVs with situational awareness beyond their direct line of sight and sensor range. For instance, vehicles can receive information about upcoming traffic jams, road hazards, or accidents, allowing them to take preemptive actions to avoid potential issues. This capability is crucial for improving traffic flow and safety, reducing the likelihood of accidents, and optimizing travel times. Also, the data collected and shared by CAVs can be utilized for various

ITS applications. These applications include adaptive traffic signal control, dynamic route planning, and cooperative driving, where vehicles work together to optimize traffic conditions that can leverage the vast amount of data generated by CAVs, making informed decisions that enhance overall traffic management and safety [26, 27].

This massive amount of data generated by CAVs by its sensors create a challenging task, where this volume of data needs advanced algorithms and methods to process it in real-time while considering current traffic conditions, road works and other dynamic factors. With the emergence of ML as a tool capable of handling and processing vast amounts of data, it becomes a viable tool for CAVs to fully reach their potential.

Vehicular FL environments represent a unique application of FL in the context of ITS [28]. This section provides an overview of vehicular federated environments, focusing on their characteristics, challenges, and potential applications. FL is a type of distributed ML that allows multiple devices to collaboratively learn a shared model without requiring data to be transferred to a central server [29, 30]. Deep learning, a popular form of ML that uses neural networks with multiple layers has been shown to benefit from FL due to its ability to handle large and complex datasets [31, 32]. The general idea of FL is depicted in Figure 1, which consists of a central server and a set of N clients, each having its local dataset. At the beginning of each training iteration, the N clients will receive the current global state of the shared model in terms of model weights. This model is broadcasted to clients (step 1). Each client uses its CPU and energy resources to carry out local computations on its dataset based on the shared parameters (step 2). Clients then send the model updates (step 3) to the central server that applies them a given aggregation policy to generate a new one (step 4).

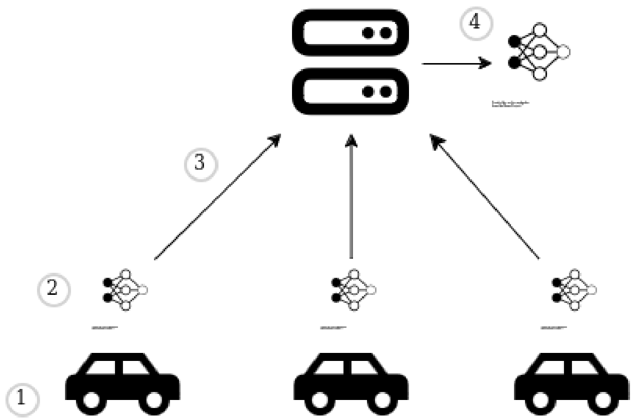


Figure 1: Overview of four main steps of FL training process

This process is repeated over several iterations (sometimes referred to as epochs) until the global model reaches a certain accuracy level determined by the central server. In summary, an FL scenario consists of two main phases, *i.e.*, local update and global aggregation. The local update phase refers to the process of computing the gradient descents by the client devices to minimize the underlying loss function for their local data. Global aggregation includes the steps of collecting the updated model parameters by the server from the different client devices, aggregating these parameters, and then sending back the aggregate parameters to the clients to be used in their next training iteration.

For the local model aggregation phase, FedAvg is a aggregation algorithm mostly used in FL environments. The FedAVG algorithms works by minimizing the global loss function by averaging the received gradients calculated by all participant clients via Stochastic Gradient Descent(SGD). SGD is the backbone of ML and for large datasets, it is implemented distributed where the dataset is shuffled and split equally across worker nodes. Ideally, if we have more nodes, we are processing more data per iteration and we expect to increase the speed to get a target accuracy. Still, in reality, it is not so easy to achieve such speed due to issues related to synchronization and communication delays that increase with the number of clients.

In terms of optimization research, there are opportunities in client and server optimization. The former is related to the process of local updates/training while the later is related to the process aggregating the model parameters sent by clients to produce an enhanced model. FL needs some orchestration back and forth between the server and the devices to train and evaluate a model, there are many architecture and strategies related to this orchestration. The initial model can be either initialized randomly or can be pre-trained. This process happens hundreds or even thousands of times in model training. The service provider is interested in the data that the device has. The initial model can be initialized randomly or we can pre-trained it. This process is going to happen hundreds or maybe thousands of times. Both the initial model and how the model evolves are important and must get attention from the management entity that controls all this process. To determine the optimal set of parameters that fits the training data, the training model has to optimize a loss (objective) function, which penalizes the model when it produces an inaccurate label on a data point.

The problems related to synchronization delays are related to workers with less computing power as demonstrated in [33]. Communication delay is the time taken to aggregate the gradients, update them, and send the updated model back to the clients. One solution to overcome this communication delay is called local update SGD, where the workers perform more local updates instead of computing only one update and sending the model to the server aggregates. This reduces the frequency of communication and makes the derivation of a single model more efficient. However, clients are not homogeneous as expected and they are not available for training all the time. Then, add more clients does not bring the process to convergence. If too many clients drop off the training process can become unstable.

Considering these challenges in client homogeneity and availability, sampling the best fit clients for training becomes a viable solution, where only the most representative clients are selected to participate in FL process, This helps alleviate the impact in the network reducing the traffic while maintaining the performance of the global model generated by maintaining the representativeness of the data, often spread unevenly between the participants.

Non-IID data refers to situations where data samples are not independent and do not follow the same probability distribution, as often seen in FL environments. In vehicular networks, this is particularly evident due to the varying data generated by vehicles based on location, driving conditions, traffic patterns, and individual behaviors. The heterogeneity of data collected from CAVs makes processing a challenging task, directly impacting the performance of machine learning models. Non-IID data violates traditional ML assumptions, requiring specialized FL techniques to account for this variability while maintaining privacy and model effectiveness. Methods such as data normalization, reweighting of samples, or adjusting learning rates can mitigate these effects and improve generalization across diverse datasets.[10]

2.2 Entropy

Entropy is a fundamental concept in information theory that quantifies the uncertainty or randomness of a system [34]. In FL, entropy plays a crucial role in client selection mechanisms, particularly in determining the relevance and diversity of data clients contribute. In information theory, entropy is the average amount of information produced by a stochastic process. It measures the degree of randomness or unpredictability in a system. Mathematically, entropy is represented by the Shannon entropy formula:

$$H(X) = -\sum_{i=1}^{n} P(x_i)\log_2 P(x_i) \tag{2.1}$$

Where $H(X)$ is the entropy of a random variable X, $p(x_i)$ is the probability of the i-th outcome of X, and n is the total number of outcomes.

In FL, entropy is utilized in client selection mechanisms to prioritize clients with diverse and informative data for model training. The entropy of a client's data distribution is used as a metric to quantify the relevance of the client's data to the overall federated model. Clients with higher entropy, indicating greater diversity or unpredictability in their data, are often selected to improve the robustness and generalization of the federated model. The use of entropy-based client selection mechanisms offers several benefits, including improved model generalization, enhanced privacy, and reduced communication overhead. By selecting clients with diverse data, entropy-based mechanisms can improve federated models' robustness and mitigate data bias issues.

2.3 Convolutional Neural Networks

CNNs are a specific type of artificial neural network architecture excelling at tasks that process data with a grid-like topology, such as images, time series data, or spatial data. Unlike standard Multi-Layer Perceptrons (MLPs), CNNs exploit the inherent hierarchical nature of such data by employing specialized layers called convolutional layers.

They also leverage powerful principles to excel in image recognition and processing. Local Connectivity keeps neurons in a layer connected only to a small area of the previous layer, reducing parameters and focusing on local features. Parameter sharing strengthens this by using the same filters across the entire image, finding features regardless of location. Finally, Pooling Layers condense the data by averaging or picking the largest value. This reduces complexity, helps prevent overfitting, and allows the network to build higher-level features from the local ones. Together, these principles are the backbone of CNNs, enabling their remarkable performance in various technical domains.

CNNs autonomously extract features from data without manual feature engineering, distinguishing them from classic ML algorithms like SVMs and decision trees, which rely on manually crafted features. The convolutional layers in CNNs provide translation-invariant properties, meaning they can identify and extract patterns regardless of variations in position, orientation, scale, or translation. Several pre-trained CNN architectures (e.g., VGG-16, ResNet50, Inceptionv3, EfficientNet) achieve top-tier performance and can be fine-tuned for new tasks with relatively little data. Beyond image classification, CNNs find applications in natural language processing, time series analysis, and speech recognition.

CNNs draw inspiration from the layered architecture of the human visual cortex. Both CNNs and the visual cortex have a hierarchical structure, where simple features are extracted in early layers, and deeper layers build more complex representations. Neurons in the visual cortex connect to local regions of the input, similar to how CNN layers are locally connected through convolution operations. Visual cortex neurons detect features regardless of location, and pooling layers in CNNs provide a degree of translation invariance by summarizing local features.

2.4 Evaluation Metrics

We evaluated three algorithms and compared their performance using common neural network evaluation metrics, including Accuracy, Loss and AUC. The Accuracy metric is computed as the number of hits (positive) divided by the total number of examples and is used for data with examples for each class and when a miss occurs. However, this metric yields flawed results in the case of disproportionate classes, as it gives a false impression of good performance. The Loss metric, on the other hand, compares the target and predicted output values and helps determine how well the neural network models the training data. It calculates the average Loss, weights, and biases in that case.

The accuracy metric is essential for evaluating the performance of CNNs used in image and time series classification tasks. Accuracy measures the proportion of correctly classified samples and provides insight into how well the model is performing overall. However, it is important to also consider other evaluation metrics, as accuracy alone may not capture all aspects of the model's performance.

During training, the loss metric plays a crucial role in guiding the optimization process. Loss quantifies the difference between the predicted outputs and the true labels, serving as the objective function that the model minimizes during backpropagation. The choice of loss function depends on the nature of the problem; for example, cross-entropy loss is commonly used in classification tasks. Minimizing the loss improves the model's predictions and generalization capabilities, making it a critical component of the training process. The selection of the loss function also influences how the gradients are computed and updated, impacting the stability and convergence of the CNN model.

The AUC score is a performance measurement for classification problems at various threshold settings. AUC represents the degree of separability and indicates how well the model can distinguish between classes. Higher AUC values signify better model performance in predicting class distinctions. For instance, a higher AUC suggests the model better distinguishes between patients with and without a disease.

The AUC score is used in conjunction with the Receiver Operating Characteristic (ROC) curve. The ROC curve is a graphical plot illustrating the diagnostic ability of a binary classifier system as its discrimination threshold varies. It is created by plotting the true positive rate (TPR) against the false positive rate (FPR) at various threshold settings. The true positive rate is also known as sensitivity, recall, or probability of detection in ML, while the false positive rate is also known as the probability of false alarm and can be calculated as (1 - specificity).

The AUC score can range from 0 to 1:

- AUC = 1: The model has perfect ability to distinguish between positive and negative classes.
- $0.5 <$ AUC < 1: The model can distinguish between positive and negative classes.
- AUC = 0.5: The model cannot distinguish between positive and negative classes, equivalent to random guessing.
- AUC < 0.5: The model reciprocates the classes, predicting negative classes as positive and vice versa.

AUC score is essentially the area under the ROC curve. Mathematically, the ROC curve plots the TPR against FPR at various threshold settings. The AUC score, being an area, does not have a simple closed-form formula but can be calculated through numerical integration or summation methods over the ROC curve. The AUC of the ROC curve can be interpreted as the probability that a classifier will rank a randomly chosen positive instance higher than a randomly chosen negative one.

When calculating the AUC score manually, especially in a discrete setting, one common approach is to use the trapezoidal rule, a method of numerical integration. This approach sums the areas of trapezoids under the ROC curve, plotted as TPR against FPR across different thresholds:

$$\int_{x=0}^{1} TPR(x)dx \tag{2.2}$$

Where x is the False Positive Rate (FPR) and TPR(x) is the True Positive Rate as a function of x. In a discrete setting, this can be approximated as:

$$AUC \approx \sum_{i=1}^{n} \frac{(FPR_i - FPR_{i-1}) \times (TPR_i + TPR_{i-1})}{2} \tag{2.3}$$

In 2.3, n is the number of thresholds, and FPR_i and TPR_i are the false positive and true positive rates at the i-th threshold, respectively. This formula computes the area of trapezoids under the ROC curve, effectively estimating the AUC.

2.5 Chapter Conclusions

This chapter introduced some of the fundamental concepts relevant to our master thesis proposal. We discussed the principles of FL and its application in vehicular networks, highlighting the unique challenges such as non-IID data distribution, communication overhead, and client variability. We also explored the concept of data diversity and its impact on model performance, as well as the advanced technologies integrated into CAVs that facilitate their operation and communication.

Despite the challenges faced by FL in the vehicular scenario, the use of entropy-based client selection mechanisms shows promise for enhancing model performance while preserving data privacy. By selecting clients with diverse and relevant data, these mechanisms can improve model generalization and convergence speed, offering a viable path forward for intelligent transportation systems. This chapter laid the groundwork for understanding these key concepts, setting the stage for the detailed exploration and analysis in the subsequent chapters.

CHAPTER 3

Related Works

This chapter delves into the latest research on client selection in FL environments, particularly in vehicular scenarios where data diversity and device heterogeneity pose significant challenges. We explore various approaches and algorithms employed to manage and optimize client selection in these settings, highlighting techniques that address data heterogeneity and connectivity issues. Additionally, we introduce methods for evaluating the effectiveness and efficiency of these techniques in dynamic and distributed environments. While our work shares some influences and concepts with these studies, it distinguishes itself by investigating innovative aspects related to the application of entropy-based mechanisms for client selection, aiming to enhance the robustness and reliability of FL in vehicular networks.

3.1 State-of-the-art

Prior research has explored the challenges of FL in the context of vehicular networks, focusing on issues related to non-IID data scenarios and biased device data distributions. For instance, Zhu et al. [35] introduced that the prevalence of non-IID data on local devices poses a substantial challenge, impacting model performance compared to centralized learning. This work examines the influence of non-IID data on both parametric and non-parametric ML models in horizontal and vertical FL settings. It reviews existing research efforts, discusses tailored strategies, and weighs the advantages and disadvantages of these approaches. Additionally, client failures increase the challenge of training with heterogeneous data, exacerbating the non-IID problem, and current algorithm-based methods fall short of addressing the fundamental disparity between local and global empirical loss minimization. However, the work has limited emphasis on resilience and does not specifically highlight how these algorithms perform in dynamic and mobile challenging scenarios like client failure.

Chellapandi et al. [36] explored the application of FL to CAVs. They discuss how FL can enhance the functionality of CAVs by enabling multiple vehicles to collaboratively train machine learning models without sharing raw data. This approach significantly addresses privacy and security concerns associated with the vast amounts of data generated by these vehicles. FL in CAVs can be implemented through centralized or decentralized frameworks, with applications ranging from driver monitoring and object detection to traffic flow prediction. The paper also identifies significant challenges, such as managing data heterogeneity, ensuring communication efficiency, and maintaining a balance between privacy protection and model accuracy. Advanced security techniques like differential privacy and secure multi-party computation are also discussed to protect data during the FL process.

Shanmugarasa et al. [22] highlighted issues stemming from security, privacy concerns, and the intricacies of FL processes, particularly the increased computational burden on clients. These challenges may impact specific clients or affect the entire network, with privacy management being a universal concern. The study concludes that collaborative efforts between servers, platforms, and clients are imperative to address client-side challenges in the FL ecosystem effectively. While advocating for collaborative solutions, the work does not extensively explore the intersection of these challenges with a scenario involving client failures. Client Failures in FL

Wang et al. [37] explored the challenges posed by client failures in FL, emphasizing a key distinction from client sampling. They note that failure introduces uncontrollable client participation, an aspect less explored in existing literature. This perspective adds valuable insights into the impact of unplanned client failure on the performance and robustness of FL algorithms.

Liu et al. [38] discussed the transition towards 5G and beyond (B5G) technologies, which offer promising solutions to the demands for efficient and secure FL applications in vehicular networks. However, these advancements introduce complexities, notably in achieving consistent connectivity and optimizing client selection within 5G/B5G networks. Liu et al. address these challenges by applying martingale theory to effectively manage access delays, optimizing client selection to enhance global learning performance within an energy budget. This approach is crucial for maintaining communication efficiency, learning performance, and energy efficiency in dynamically evolving vehicular environments. However, the work does not delve deeply into scenarios involving client failures.

Mariano et al. [39] addressed communication challenges and scalability issues by dynamically adapting the number of participating devices and training rounds through a client selection strategy using the developed algorithm DEEV. Using a containerized environment, DEEV showcases significant reductions in communication and computation overhead compared to existing approaches. Its robust performance in scenarios with non-IID data underscores its potential for enhancing FL model efficiency. However, the work considers only an environment where every client is available and stationary, differing from typical vehicular network scenarios.

Tang et al. [1] proposed a fair and efficient FL algorithm for autonomous driving to address the challenges of imbalanced data distribution and fluctuating channel conditions among CAVs. The authors highlight the unfairness in energy and time costs caused by traditional FL algorithms due to discrepancies in local training costs and model upload durations between different CAVs. To achieve fairness, the proposed algorithm employs a personalized approach for local training rounds of each CAV, considering the volume of data and channel conditions. This approach ensures fairness in energy and time costs while accelerating the convergence of the global model. Extensive simulations demonstrate the effectiveness of the proposed algorithm in achieving fairness in energy costs and reducing the duration of each round of global iteration.

Sun et al. [21] studied the convergence performance of the classic FedAVG aggregation algorithm in scenarios involving arbitrary client failures. The theoretical analysis indicated that client failures lead to biased updates in each training iteration. When employing the commonly used strategy of a decaying learning rate, the model trained by FedAvg may exhibit oscillations around a stationary point of the global loss function. A cross-device FL system simulation was carried out to validate these findings, incorporating various client failure patterns.

Huang et al. [20] investigated the vital topic of client selection in a fluctuating environment. They acknowledged that choosing particular clients for each synchronous round in FL training significantly affects both training efficiency and the ultimate performance of the model. Their research defined the client selection problem by considering effective participation and fairness, introducing E3CS, a stochastic client selection strategy. Experimental results using a public dataset showed that E3CS leads to quicker convergence towards a predetermined model accuracy while retaining the same level of final model accuracy compared to leading-edge selection methods.

Araujo et al. [40] effectively demonstrated the use of advanced information theory quantifiers and causal planes to distinguish and classify various modes of transportation using speed dynamics derived from GPS data. A key strength of this research is its novel application of entropy-based measures to provide a robust framework for analyzing and understanding complex mobility patterns, which enhances urban planning and intelligent transportation systems. The methodology's ability to detect transitions between different transportation modes further underscores its practical utility. However, the study's reliance on the Geolife dataset, which may not fully represent all urban mobility scenarios, and the complexity of implementing the described techniques in real-time applications are notable shortcomings.

Veiga et al. [41] introduced RiCA (Resilience-aware Client Selection Mechanism) to enhance FL environments by addressing non-IID data and malicious clients. A key aspect of RiCA is its use of entropy as a method for client selection. By calculating the entropy of clients' data, RiCA prioritizes clients with more diverse and informative data, which enhances the generalization and robustness of the global model. Additionally, RiCA incorporates Centroid-Based Kernel Alignment (CKA) to identify and exclude potentially malicious clients, further protecting the model from poisoning attacks. The paper demonstrates that RiCA, combined with CKA, significantly improves model accuracy and resilience, achieving up to 90% accuracy in scenarios with malicious clients compared to only around 30% with a default random selection approach. This dual approach of leveraging entropy for client diversity and CKA for security underscores the effectiveness of RiCA in maintaining robust FL environments.

Another work by Santos et al. [30] addressed the communication and privacy challenges in FL by introducing a novel client selection mechanism. MESFLA leverages a CKA algorithm to group clients based on the similarity of their data distributions and then selects the most relevant clients within each group based on data weight and entropy. This approach improves model accuracy and convergence speed by optimizing the selection of clients that contribute the most valuable updates to the global model. The comprehensive evaluation of MESFLA using datasets such as MNIST, CIFAR-10, and CIFAR-100 demonstrates its superior performance over traditional FL algorithms in terms of accuracy and communication efficiency. However, the study acknowledges potential biases in client selection and suggests future work on refining the weighting scheme and testing the algorithm in scenarios with client failures and malicious behavior

Significant advancements have been made in the realm of FL for vehicular networks, notably with the introduction of FLEXE by Lobato et al. [32], an extension to the Veins simulation framework. FLEXE integrates Veins with OpenCV to implement vehicular FL applications, addressing key challenges such as vehicular mobility and intermittent communication. It enhances the evaluation of FL applications by providing a realistic simulation environment, crucial for understanding the dynamic nature of vehicular networks. FLEXE's advantages lie in its comprehensive simulation capabilities and its focus on realistic vehicular characteristics, which are often overlooked in existing approaches. However, while FLEXE effectively addresses communication and mobility, it falls short in investigating client failures, a critical aspect thoroughly examined in this dissertation.

3.2 Chapter Conclusions

In reviewing the literature on client selection mechanisms in FL within vehicular networks, this study has identified a critical gap concerning the resilience and efficiency of these mechanisms in the face of client failures—a common issue in dynamic vehicular environments, due to signal failure, vehicles getting out-of-range from a RSU or vehicle disconnection. This dissertation proposes to address these gaps by implementing an entropy-based client selection framework specifically tailored for high-failure scenarios in vehicular networks. The expected contribution of this research is twofold: it will validate the theoretical benefits of entropy-based selection through real-world implementation and refine existing frameworks to enhance their resilience and reliability in the face of client failures. The methodology, detailed in the following chapter, employs a mixed-methods approach that combines simulation and real-world experimentation to provide a comprehensive evaluation of the proposed model.

Table 1 summarizes the main characteristics of prior studies focused on client selection mechanisms, detailing data distribution types, machine learning algorithms used, and the scenarios considered for client failures in vehicular FL environments. This research advances the field by refining data preprocessing techniques utilized in these CNN methods and exploring their application in a FL context, specifically investigating the impact of client failures. The metrics employed in our analysis were chosen to highlight these characteristics within our proposed framework, as presented in Table 1. This allows for a deeper understanding of how CNNs perform in classifying vehicle behaviors in a continuous authentication setting within a FL model, especially under conditions of client failures.

Table 1: Summary of client selection methods in FL

Works	Non-IID	CAV	Client Selection	Client Failures
[35]	✓			
[36]		✓		
[22]				✓
[37]		✓	✓	
[38]	✓	✓	✓	
[39]	✓	✓	✓	
[21]	✓		✓	
[20]	✓		✓	
[40]	✓		✓	
[41]	✓	✓	✓	
[30]	✓		✓	
[32]	✓	✓	✓	

CHAPTER 4

Entropy-based Client Selection Mechanism and Analysis under Client Failure Scenario

This section discusses the experimental methodology of an Entropy-based Client Selection Mechanism and its expected contributions to a vehicular scenario and its advantages and shortcomings in a scenario with client failures as well.

4.1 Scenario Overview for Client Selection

In a typical Centralized FL paradigm, model parameters, be it weights or gradients, are transmitted to a central server, often a RSU, where the FL server-side aggregation process occurs. Most of the existing library relies on FedAVG algorithm for the FL process aggregation process on the server, then it applies SGD optimization to local vehicles and performs a weighted averaging of the weights of the vehicles on the central server.

In this specific scenario, we envisage a scenario involving a set of n CAVs navigating an urban environment and equipped with a variety of sensors, such as cameras mounted at various points on the vehicle and capture visual information about the surroundings, LiDAR providing precise distance measurements by emitting laser beams and measuring the reflection times to create detailed three-dimensional maps of the environment, radars that monitor the distance, speed and object directions in the surroundings and other minor sensors. Each CAV, denoted by an index i within the range $[1, n]$ and represented as $C = \{c_1, c_2, c_3, ..., c_n\}$. Every CAV c_i in the moves in a specific direction and maintains a speed s_i within the range of the minimum speed (s_{min}) and maximum speed (s_{max}). Each CAV c_i is equipped with the range of sensors described earlier and collects data crucial for ML applications, such as recognition or image classification. In this way, each CAV c_i has local dataset $D_i \in \{D_1, \ldots, D_N\}$ distributed in a non-IID manner, which contains a set of *features* $x_{k,i}$ with $k \in \{1, \ldots, \|D_i\|\}$ associated with a *label* $y_{k,i}$.

In addition, each CAV c_i is equipped with a Vehicle-to-Infrastructure (V2I) communication interface, such as Dedicated Short Range Communication (DSRC) or 5G, which is used to communicate with the edge server ES through the core network. The edge server ES that plays a pivotal role in distributing ML parameters for the initial or updated global model ω to all CAVs during each communication round μ. Moreover, the edge server ES assumes responsibility for collecting and analyzing entropy data, and also for model aggregation.

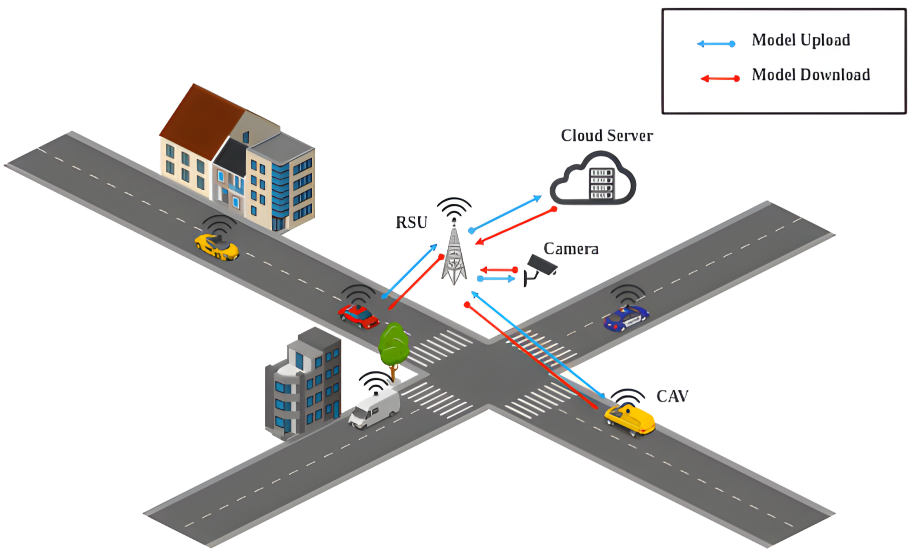


Figure 2: Representation of a vehicular FL scenario

We considered the typical FL architecture, where the process starts with initializing a global model M_g on a central server. At each communication round μ, a subset of k CAVs denoted as $V = \{v_1, v_2, v_3, ..., v_k\}$ is selected to receive the global model M_g and perform the training based on its Dataset D_i. Each selected client v_i can train a model architecture A to obtain the local model W_i based on the local dataset D_i. In this way, each client v_i trains the local model W_i to minimize a loss function l for better convergence with a minimum accuracy value across users. Specifically, the local loss $l(W_i, D_i)$ is defined as the average loss based on the prediction error, across all predictions for the dataset D_i using the weights W_i, which is computed based on Eq. 4.1.

$$l(W_i, D_i) = \frac{1}{\|D_i\|} \sum_{k=1}^{\|D_i\|} f(W_i, x_{k,i}, y_{k,i}) \tag{4.1}$$

In the aggregation phase, the model updates, *i.e.*, , learned parameters or gradients W_i, are sent periodically to the edge server ES, which applies a given aggregation policy, such as FedAVG. Specifically, FedAVG computes an average of the shared local models W_i at edge server ES to produce an accurate global model M_g, transmitted back to the participating CAVs. In addition, the edge server ES defines the number of k

selected clients based on a client selection mechanism, such as entropy-based.

4.2 Client Failures in Federated Learning

Client failure in FL over CAVs refers to clients' cessation of active participation in the collaborative model training process, as opposed to intentional client dropout [37]. This phenomenon could result from different factors, such as vehicle mobility due to intermittent connectivity issues during transitions between RSU; connectivity problems caused by temporary or permanent disconnection due to network disruptions; intentional withdrawal, where clients opt out voluntarily due to privacy concerns or limited resources; and resource limitations, as seen in devices with constrained battery life choosing to drop out strategically.

To better illustrate the concept, we consider a standard FL algorithm where clients collaborate to train the same global model. In the event of client failure, only a random subset of selected clients will participate in each training round. This failure disrupts the FL system, reducing accuracy, increasing bias, and compromising fairness. Client failures, along with mobility, result in inconsistent data contributions, which ultimately impede model convergence. Reliable and robust FL algorithms must adapt to sporadic client participation and mobility. By accommodating intermittent client presence and optimizing model aggregation under varying network conditions, these strategies can enhance stability in dynamic FL environments.

Figure 3 illustrates a typical FL environment in the context of CAVs with client failures. In this scenario, each client v_i has a probability $P(v_i)$ of being selected for participation in the FL process. This probability depends on the specific selection metric used. For example, $P(v_i)$ might be a random value in a random selection approach, proportional to the entropy (representing data randomness or unpredictability) in an entropy-based selection mechanism [17], or based on clients whose accuracy is lower than the average of all participating clients [39]. Furthermore, let $Q(v_i)$ represent the probability of a client v_i being disconnected from the training process, which can be influenced by different factors, such as network stability, device power, or communication issues.

The overall probability of a client v_i being selected and then dropping out during training is given by the product of the selection and failure probabilities:

$$P_{failure}(v_i) = P(v_i) \times Q(v_i) \tag{4.2}$$

If we want to consider multiple clients potentially failing independently, we can define an overall failure probability for the entire set of clients:

$$P_{totalfailure}(V) = \Pi_{i=1}^{k} P_{failure}(v_i) \tag{4.3}$$

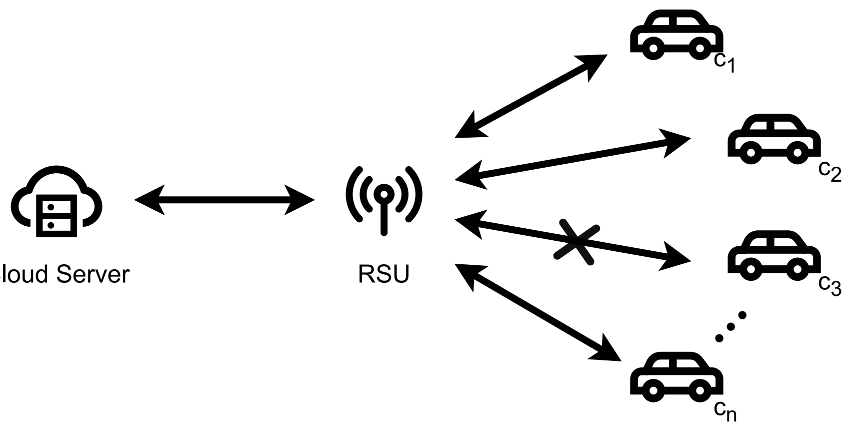


Figure 3: Representation of client failures in a FL over CAV environment

Clients can fail by a multitude of reasons, with mobility being one of the most significant factors. The dynamic nature of CAVs means that vehicles frequently move between different geographical locations and RSUs, leading to a process known as handover. During handovers, vehicles temporarily disconnect from one RSU and establish a connection with another. This transition period can introduce brief but critical communication disruptions, causing delays in data transmission and reception. These disruptions can prevent vehicles from uploading their local model updates or receiving the latest global model parameters in a timely manner, thereby missing out on important synchronization points in the FL process. This process also can lead to inconsistent data contributions, skewing the training data towards specific areas or driving patterns, hindering the model's ability to generalize to unseen scenarios. Frequent handovers disrupt the training process, as vehicles participate in updates only when connected to a specific RSU. This can lead to slower convergence of the global model compared to a scenario with consistent participation. Another factor is that vehicles might opt out of FL participation due to concerns about their data privacy, which thus reduces the amount of available data, potentially hindering the model's overall accuracy.

Additionally, the handover process is often accompanied by increased network latency. This latency can vary depending on the distance between RSUs, the current network load, and the speed at which the vehicle is moving. High latency can exacerbate communication delays, leading to further inconsistencies in data contributions from mobile clients. The variability in network conditions and the frequent need for handovers results in a highly dynamic and unstable communication environment.

The intermittent connectivity not only affects the immediate participation of clients but also has longer-term implications for the overall FL system. For instance, vehicles in regions with poor network coverage or those frequently moving through network dead zones may consistently fail to contribute their local updates. This leads to an uneven distribution of data contributions, with some regions being overrepresented while others are underrepresented. Such an imbalance can introduce bias into the training process, as the global model may become more attuned to the driving conditions and patterns prevalent in well-connected areas while neglecting those in poorly connected regions.

Moreover, the reliability of the FL system depends on the assumption that clients can participate consistently over multiple training rounds. Intermittent connectivity disrupts this assumption, making it difficult to predict which clients will be available at any given time. This unpredictability necessitates the development of more robust client selection and aggregation strategies that can accommodate fluctuating client participation. For example, FL algorithms might incorporate mechanisms to prioritize clients with more stable connections or to buffer updates from intermittently connected clients until they can be reliably transmitted.

4.3 Entropy-Based Client Selection Overview

By definition, in information theory, the entropy of data labels is a measure of the uncertainty or randomness within a client's dataset. The idea behind using entropy for client selection is intuitive. A high entropy dataset is generally diverse in content and contains a wide range of information, while a low entropy dataset is more homogeneous. High entropy clients are more likely to contribute unique and valuable updates to the global model. Their diverse data helps the model generalize better to a wider range of scenarios. Meanwhile, low entropy clients, while still important, might not provide as much novel information in a given training round, resulting in potentially redundant updates.

Also, selecting clients based on the entropy of their datasets can significantly improve the training process. By prioritizing high entropy clients, it ensures the model learns from a broader spectrum of data distributions, which is particularly beneficial in non-IID scenarios. This approach improves the global model's performance and robustness by providing diverse inputs. Additionally, entropy-based client selection helps mitigate overfitting by introducing variability and complexity into the training data, promoting a more balanced and generalized model. This is crucial in applications like autonomous driving or healthcare, where adaptability to various real-world conditions is essential.

FL for CAV environments presents unique challenges due to the ever-changing nature of CAV mobility and the critical objectives of enhanced privacy and reduced server load. The issues of client failure and varying data diversity can significantly impact the FL process. To tackle these challenges effectively, adopting entropy as a criterion for client selection is necessary.

To illustrate the concept of entropy-based client selection, let us consider a typical FL model designed for autonomous driving, as represented in Figure 4. Let's assume Client A possesses a dataset with diverse sensor data collected from various environments, including urban areas, highways, rural roads, and weather conditions. This dataset exhibits high entropy due to its diverse content. Conversely, Client N holds a dataset predominantly consisting of sensor data from a single type of environment, such as urban roads in clear weather conditions, which indicates lower entropy due to its homogeneity.

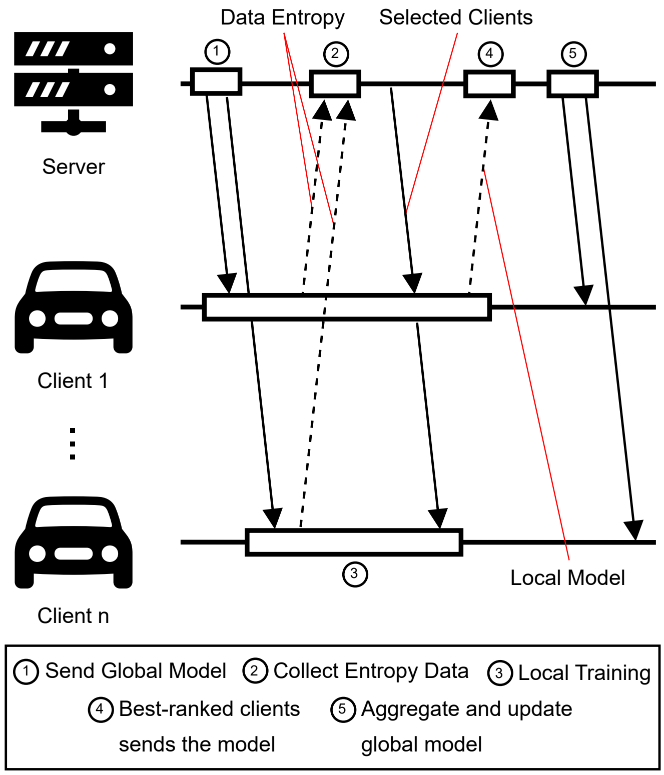


Figure 4: Entropy-based client selection mechanism

In this scenario, Client A's dataset, with its higher entropy, is more likely to contribute significant updates that enhance the model's ability to operate effectively in a wide range of driving conditions. The diverse nature of the data ensures that the model is exposed to varied features and patterns, thereby improving its generalization capability. Client N's updates, while less diverse, can still be valuable in later stages of training when fine-tuning the model's performance for specific scenarios, such as navigating specific urban environments.

This example demonstrates how entropy-based client selection prioritizes clients whose data can provide the most informative updates, leading to a more effective and efficient training process. By systematically incorporating clients with high entropy, the FL system can achieve superior model performance across diverse driving scenarios.

In this context, entropy-based client selection mechanisms give preference to selecting clients based on the entropy of their data, using it as an indicator of data diversity and representativeness. By selecting clients with high entropy, FL algorithms can ensure that the learned models represent the entire network and capture the variations in driving behavior, traffic patterns, and network connectivity. This approach also has the potential to enhance the model's robustness in the face of unpredictability in vehicular networks. Hence, entropy-based client selection mechanisms have shown promise in significantly reducing data variability contributions and managing the challenges associated with uncertain client availability.

We consider Shannon Entropy to calculate the data entropy $H(x)$, where $P(x)$

denotes the probability of observing a particular value x in the dataset, and log is the natural logarithm, as described in Equation 4.4.

$$H(X) = -\sum_x P(x) \log P(x) \tag{4.4}$$

Clients whose datasets have a high level of entropy are selected because they contain diverse and informative data that can improve the performance of the FL model, as described in Equation 4.5. K_m refers to the class of the data point d_{ni}, which represents an individual data point in d_n.

$$H(d_n) = -\sum_{j=1}^{m} P(k_m) \log P(k_m) \tag{4.5}$$

Figure 4 depicts the entropy-based client selection workflow, encompassing entropy calculation, local model training and testing, as well as global model aggregation and update.

The communication round involves five steps:

1. The edge server ES sends the current global model M_g to all CAVs V.
2. Each CAV C_i sends its calculated data entropy $H(d_n)$ to the edge servers ES.
3. The edge server ES selects a set of clients C from the set of CAVs V that meets a specified threshold θ based on entropy ranking, described as $H(d_n) \geq \theta$. These clients will be selected to perform local model training.
4. The trained local models W_i are sent to the edge server ES for aggregation.
5. The edge server ES generates an updated global model M_g based on the aggregated local models, which is then sent back to all participants.

Selecting clients based on entropy boosts FL by improving model accuracy and efficiency. High-entropy clients contribute diverse, unique updates, helping the model generalize better and converge faster. This method also reduces communication costs by involving fewer, more informative clients. It effectively handles non-IID data, enhancing robustness against client failures and ensuring consistent model performance despite unpredictable client availability.

4.4 Algorithm Description

Similar to our prior work [17], the entropy-based strategy algorithm is described in Algorithm 1, with an addition of client failure mechanics. The algorithm starts by

Algorithm 1: FedAvg with Entropy-Based Client Selection and Client Failures

Input : C_t: the fraction of clients participating in round t, K: the total number of clients, θ: the entropy threshold, T: number of rounds, E: number of local epochs, P_f: the percentage of failing clients

Output: Global model $\mathbf{w}^*$

Initialize global model $\mathbf{w}_0$;
for $t = 1$ **to** T **do**
  Entropy-Based Client Selection;
  Each client computes its entropy scores using the validation set;
  Sort clients in descending order of entropy scores;
  Select top $m = \lfloor C_t \cdot K \rfloor$ clients whose entropy scores exceed θ;
  Simulate Client Failures;
  Randomly select $P_f \cdot m$ clients from the selected clients to fail and exclude them from the training round;
  $S_t \leftarrow$ remaining selected clients after excluding the failed clients;
  Local Model Training;
  for $i \in S_t$ **do**
    $\mathbf{w}_i \leftarrow \text{LocalUpdate}(\mathbf{w}_{t-1}, i, E)$;
  end
  Global Model Aggregation;
  $\mathbf{w}_t \leftarrow \text{FedAvg}(\{\mathbf{w}_i\}_{i \in S_t})$;
end
return $\mathbf{w}^* = \mathbf{w}_T$;

initializing the global model $\mathbf{w}_0$. For each round t from 1 to T, the following steps are executed:

- Entropy-Based Client Selection: Each client computes its entropy scores using its validation set. The clients are then sorted in descending order based on these scores. The top $m = \lfloor C_t \cdot K \rfloor$ clients whose entropy scores exceed a specified threshold θ are selected for participation in the current round.

- Simulate Client Failures: To introduce client failure mechanics, a certain percentage P_f of the selected clients are randomly chosen to fail and are excluded from the training round. This simulates the real-world scenario where some clients may drop out or fail to participate due to various reasons. The remaining clients after excluding the failed ones are denoted as S_t.

- Local Model Training: Each client in the set S_t performs local model training. Specifically, each client i updates its local model $\mathbf{w}i$ based on the global model from the previous round $\mathbf{w}t - 1$ over a specified number of local epochs E.

- Global Model Aggregation: The locally updated models from the clients in S_t are aggregated to update the global model. This aggregation is done using the Federated Averaging (FedAvg) algorithm, resulting in the global model $\mathbf{w}_t$ for the current round.

After completing T rounds, the final global model $\mathbf{w}^*$ is obtained as $\mathbf{w}_T$. This modified algorithm not only incorporates an entropy-based client selection strategy but also accounts for potential client failures, making possible the investigation and comparison with different client selection strategies under variable client and network failure conditions.

4.5 Chapter Conclusions

In this chapter, we introduced a client selection mechanism for vehicular FL environments based on the entropy of the labels in the client's data. This approach aims to enhance the efficiency and effectiveness of FL by prioritizing clients with diverse and informative data, ultimately improving model generalization and convergence speed.

Moreover, we discussed the impacts of client failures on this proposed method. By analyzing scenarios with varying levels of client participation, we highlighted the resilience of entropy-based client selection in maintaining robust model performance despite client dropouts and communication failures. The method shows promise in mitigating the adverse effects of client failures by ensuring that the most informative clients are prioritized, thereby sustaining the overall learning process even in dynamic and challenging environments. This chapter sets the stage for further exploration and refinement of entropy-based techniques in FL, highlighting their potential to address the challenges of non-IID data, client variability, and client failures in intelligent transportation systems.

CHAPTER 5

Evaluation Results

This chapter presents the evaluation and impact of the entropy-based client selection method in vehicular FL environments and a posterior analysis focusing on scenarios with client failures. The proposed method is compared to traditional random selection approaches to highlight its effectiveness. The evaluation begins by detailing the methodology used in the simulations, including the simulation parameters and metrics assessed. Following this, the results are thoroughly discussed, emphasizing the performance and stability of the entropy-based selection method under various conditions, including non-IID data distributions and client failuress.

5.1 Environmental Scenario and Parameters

We conducted a comprehensive simulation study using the PFLib, which is a flexible framework presented by [42] and available on GitHub[1]. The framework runs in a server with the following specs: i9-13900K(32), 128 GB RAM and Dual RTX 4090 on a Ubuntu Server operating system. We consider a widely used public dataset, called FMNIST, to train and test model validations. The CNN model used in the experiment has two convolutional layers with filter sizes of 5x5. Each convolutional layer is succeeded by a 2x2 max-pooling operation. Furthermore, it's important to take into account that the data employed in this experiment follows a non-IID arrangement, resembling a realistic data distribution scenario, and is modeled using a Dirichlet distribution. This non-iid configuration was generated by a tool in PFLib, wich defined the rate of the Dirichlet distribution at 0.1. We consider a grid scenario with 1km^2 composed of 58 clients as proposed by [43] and use the Luxembourg SUMO Traffic (LuST) environment presented by [44].

[1]https://github.com/TsingZ0/PFLlib

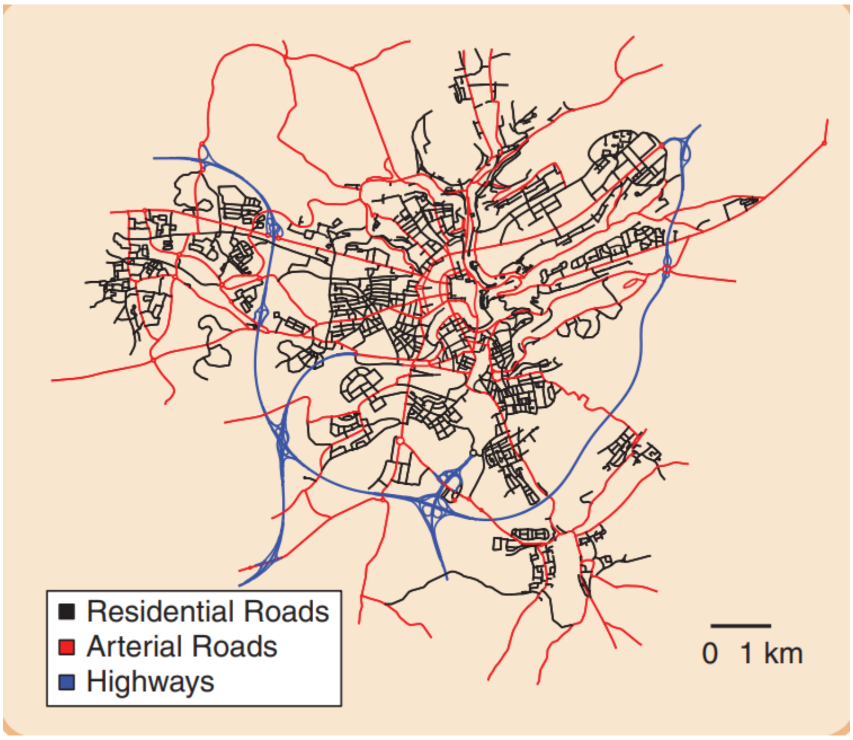


Figure 5: LuST scenario in SUMO

We consider a built-in feature within the framework to simulate client failures, such as introduced on Section 3.2. This feature operates by randomly selecting a client to refrain from sending updates and receiving models during a particular round. This capability allows us to explore the consequences of client failure on the reliability and robustness of client selection mechanisms in FL over CAV scenarios. It is worth noting that the failure rate is adjustable, providing the flexibility to control the extent of simulated failure events. We evaluate the impact of various failure rates in the scenario, considering scenarios with no failure, 16%, 33%, and 50% client failure rates. Table 2 summarizes the main simulation parameters used in our evaluation.

Table 2: Simulation parameters for experiment

Parameters	Value
Total Participant Clients	58 vehicles
Number of Rounds	100 Rounds
Learning Rate	0.001
Client Failure Rate	16%, 33%, 50%
Number of Epochs	1
Network Model	CNN
Batch Size	10

We conducted a comparative analysis of the three client selection methods: i) Random selection is a baseline method that does not consider the quality or diversity of clients' data. It simply selects a random subset of clients to participate in each round of training; ii) DEEV selects clients that have lower accuracy than the average accuracy of all participating clients [39]; iii) Entropy-based client selection leverages data entropy to choose clients that contain diverse and informative data, such as introduced in Section 3.3.

5.2 Evaluation of Entropy-Based Client Selection Mechanism

In non-IID scenarios, as depicted in Figures 6, 7 and 8, the proposed method achieved higher accuracy and AUC scores compared to the random selection approach. This improvement can be attributed to our method's selection of clients with diverse data distributions, which reduces the impact of biased data on the training process. This suggests that selecting clients based on data entropy can effectively address the challenges posed by non-IID data in vehicular FL environments. The lower training loss also indicates better convergence during training. However, it is important to note that the proposed method may require more communication overhead to collect entropy information from all clients, potentially limiting its scalability in large FL systems. Overall, these results highlight an important finding for vehicular networks, especially in scenarios where non-IID data is prevalent.

Tables 3 and 4 further demonstrate the advantage of the entropy-based selection method over random selection. Specifically, the entropy-based selection method achieves higher scores across all metrics, even in scenarios with client failure. The large oscillations in the metrics during the rounds in non-IID scenarios, both in normal and random client failure, for the random selection approach, are due to the highly unbalanced and diverse data distributions of the randomly selected clients. Consequently, some clients may have much better data quality than others, leading to significant variations in training performance during each round. This can cause the model to overfit on some clients while underfitting on others, resulting in unstable and inconsistent performance over time. The entropy-based selection approach mitigates this issue by selecting clients with more diverse and balanced data distributions, leading to more stable and consistent performance during training and by selecting clients based on data entropy, the method ensures that each round of training includes a diverse set of data distributions, which prevents the model from becoming overly specialized to specific data patterns. This leads to improved generalization, higher accuracy, and more stable performance, even in the face of client failures and highly variable data distributions.

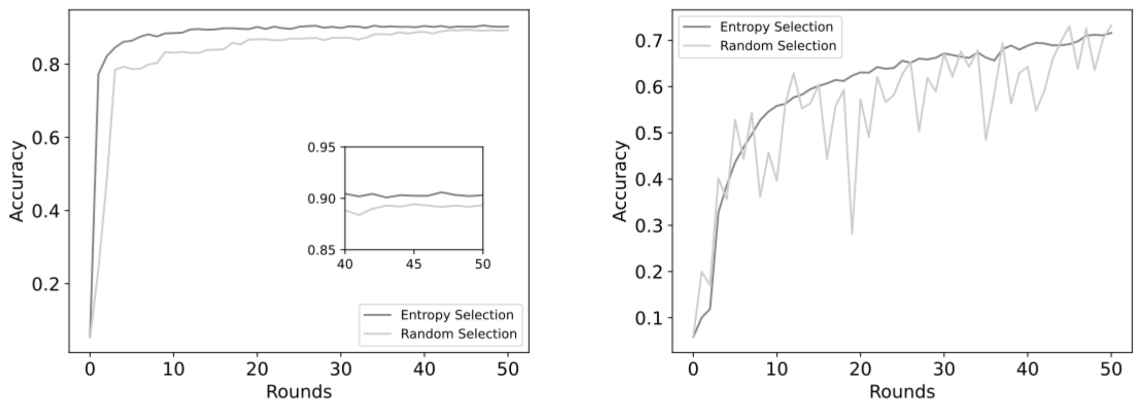
The large oscillations in metrics during non-IID scenarios with random client selection are due to the inherent variability in this specific data distribution, potentially leading to inconsistent model updates as the selected clients may differ significantly from round to round. In contrast, the entropy-based selection approach mitigates this issue by strategically choosing a set of clients that collectively provide a more balanced and representative sample of the overall data distribution. This approach doesn't necessarily select individual clients with the highest data diversity (entropy), but rather aims to create a

Table 3: Performance metrics of random client selection mode.

Metric	**IID**	**Client Dropout IID**	**Non-IID**	**Client Dropout non-IID**
Test Accuracy	0.7159	0.7091	0.7026	0.6849
Train Loss	1.0693	1.1628	0.9972	1.0443
AUC Score	0.9380	0.9064	0.9380	0.9064

Table 4: Performance metrics of entropy client selection mode.

Metric	**IID**	**Client Dropout IID**	**Non-IID**	**Client Dropout non-IID**
Test Accuracy	0.7323	0.7301	0.7121	0.7103
Train Loss	0.7862	0.8081	0.7862	0.8081
AUC Score	0.9841	0.9840	0.9485	0.9474

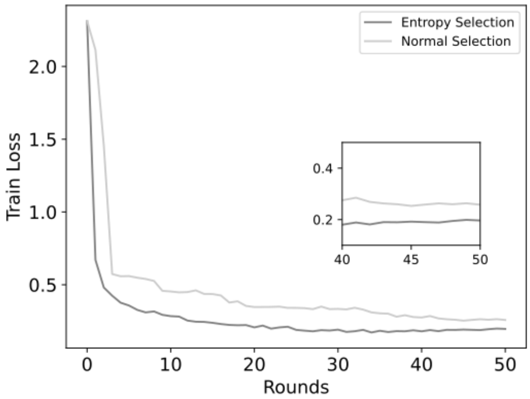


(a) IID Accuracy (b) Non-IID Accuracy

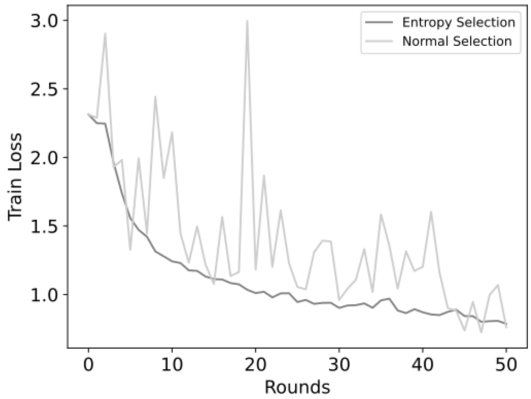
Figure 6: Accuracy for different client selection strategies

group whose combined data closely approximates the global dataset. By maintaining a more consistent representation of the overall data distribution across training rounds, the entropy-based method stabilizes the learning process, resulting in more gradual and consistent model improvements. This reduces extreme fluctuations in performance metrics, minimizes overfitting to particular data subsets, and leads to better generalization and more robust performance across diverse client data distributions.

These findings show that the suggested entropy-based selection strategy can improve performance and stability while working with non-IID data, indicating that the proposed client selection could greatly improve the performance of vehicular FL by selecting higher quality data for the training of the model. In the IID scenario, presented in 6, 7 and 8, both selection methods perform similarly across all three metrics, with a slight

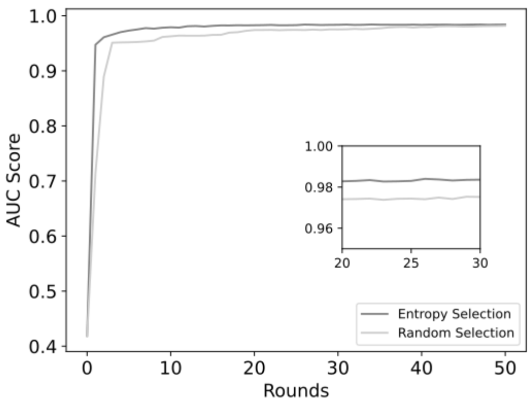


(a) IID Train Loss

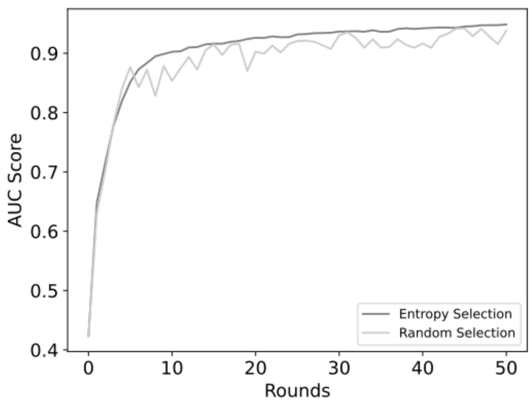


(b) Non-IID Train Loss

Figure 7: Train loss for different client selection strategies



(a) IID AUC Score



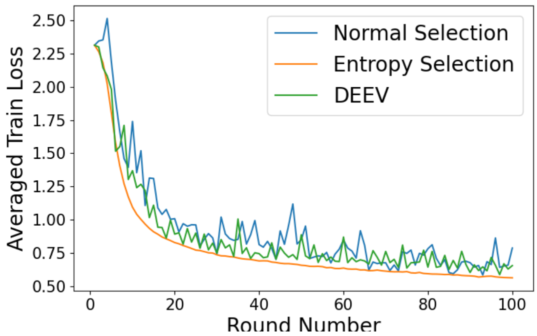
(b) Non-IID AUC Score

Figure 8: AUC Score for different client selection strategies

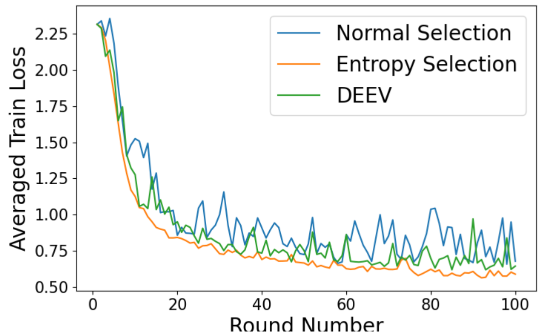
advantage for the entropy-based selection method when dealing with data that follows an IID distribution.

5.3 Evaluation of Client Selection Mechanism Resiliency under Client Failures

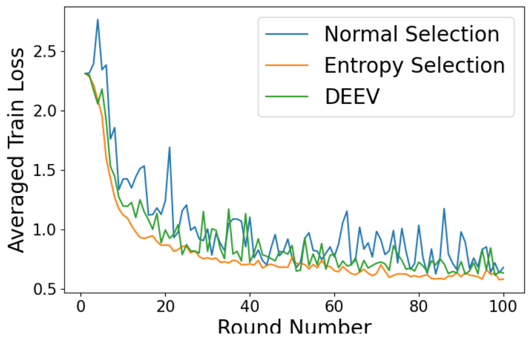
The initial evaluation of the entropy-based client selection mechanism demonstrates its effectiveness in enhancing model performance within vehicular FL environments. By selecting clients with diverse data distributions, the method significantly improves accuracy, AUC scores, and training stability compared to random selection. This section detailed how the entropy-based approach mitigates the challenges posed by non-IID data, leading to more robust and reliable model convergence. Having established the baseline effectiveness of the entropy-based mechanism, it is important to evaluate its resilience in more challenging conditions, specifically scenarios involving client failures. Vehicular networks are prone to intermittent connectivity and client failuress, which can adversely affect FL processes. Therefore, this section examines how the entropy-based selection method performs under these adverse conditions, assessing its ability to maintain high performance and stability despite client failures.



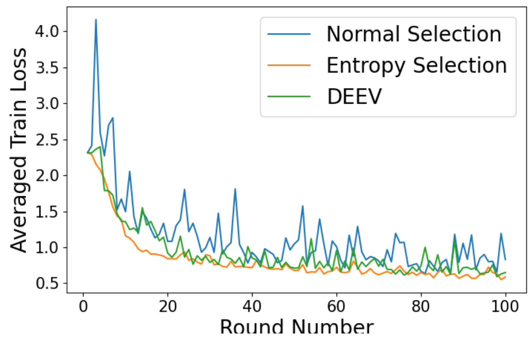
(a) Without client failures



(b) 16% of client failures



(c) 33% of client failures

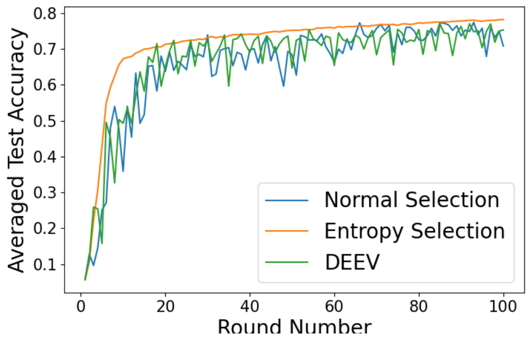


(d) 50% of client failures

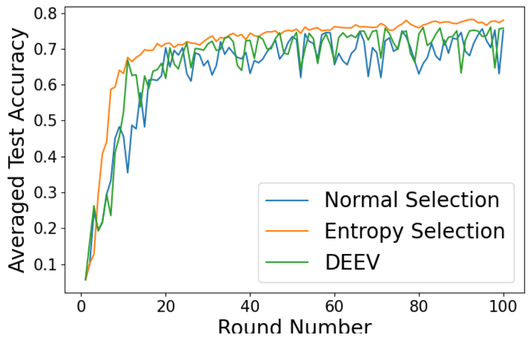
Figure 9: Train Loss for different client selection mechanism

Figure 9 shows the train loss for different client selection mechanism under different client failure rates. By analyzing Figure 9 (a), we can conclude that the entropy-based mechanism exhibits faster convergence compared to the other client selection mechanisms. As the client failure rate increases, all methods experience a decline in performance. However, the entropy-based mechanism maintains a slight advantage over the others. On the other hand, the DEEV strategy deteriorates to the extent that it exhibits slightly inferior performance compared to random selection, as can be also observed.

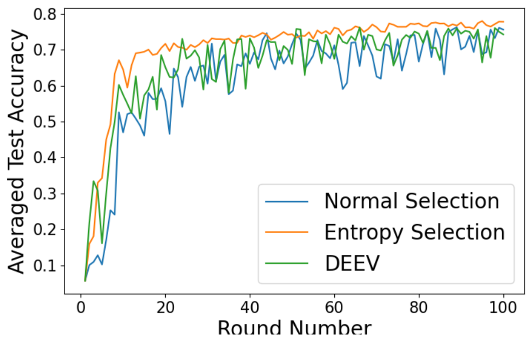
The entropy-based client selection mechanism harnesses information entropy as its guiding principle, prioritizing clients that contribute diverse and informative data, ultimately creating a more representative model. In this way, the mechanism demonstrates reduced instability in train loss metrics, exhibits faster convergence and maintains higher levels of accuracy compared to random selection and DEEV mechanisms. This adaptability of the entropy-based mechanism to varying data distributions and the dynamic nature of FL over CAV scenarios contributes to its effectiveness in mitigating the impact of client failure with different level of failure frequency, making it a valuable strategy for ensuring stability and top-notch performance in FL over CAV. Hence, the superiority of the entropy-based client selection mechanism shines through when faced with challenges related to client failure, as observed in [37].



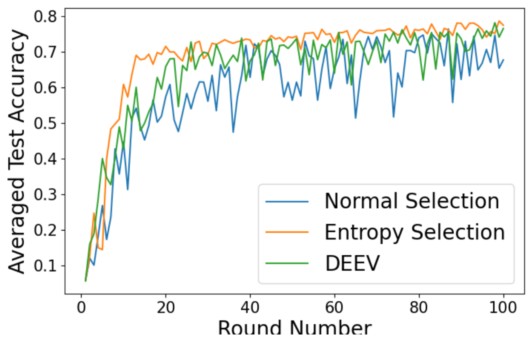
(a) Without client failures



(b) 16% of client failures



(c) 33% of client failures

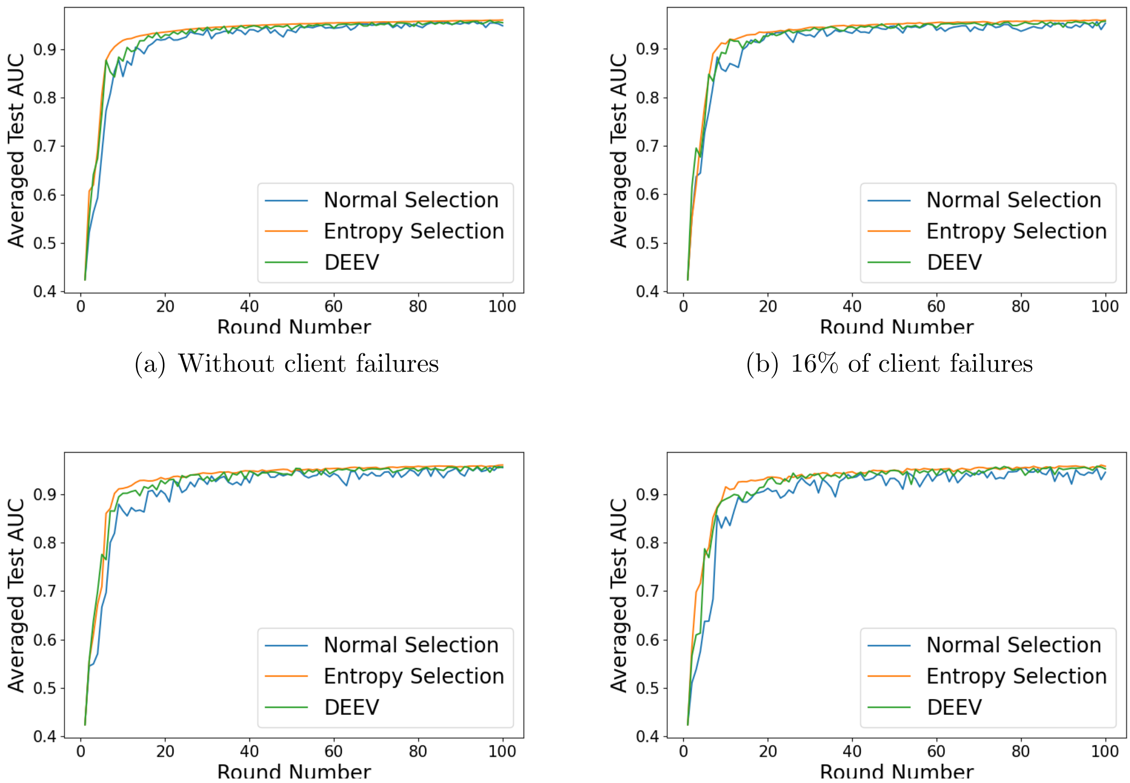


(d) 50% of client failures

Figure 10: Accuracy for different client selection mechanism

Figure 10 shows the accuracy results for different client selection mechanisms under different client failure rates. By analyzing the accuracy results, we notice a similar trend where the accuracy of all tested mechanisms deteriorates as the client failure rate increases. Notably, the entropy-based method consistently outperforms the other two mechanisms, even with high failure rates. In contrast, the DEEV mechanism exhibits a decline in performance to the extent that it falls below the performance of random selection, reaching its lowest point at a 0.5 client failure rate.

The entropy-based selection method consistently exhibited a performance advantage, even in scenarios with high failure rates. This remarkable reliability and robustness can be attributed to its core principle of selecting clients with diverse datasets. Prioritizing clients based on entropy ensures the selection of clients that offer a wide spectrum of data characteristics, resulting in the maintenance of a robust and representative model. This mechanism proves to be effective even in challenging scenarios with high failure rates. In such situations, where clients' participation may significantly decrease, leading to a potential loss in data diversity and model accuracy, the entropy-based method shines



(a) Without client failures

(b) 16% of client failures

(c) 33% of client failures

(d) 50% of client failures

Figure 11: AUC Score for different client selection mechanism

through by preserving the model's performance and adaptability.

Figure 11 shows the AUC results for different client selection mechanisms under different client failure rates. When examining the AUC Score results, we observe a similar trend in metric degradation as observed with accuracy and train loss. The entropy-based strategy consistently outperforms the other two methods, while the DEEV method experiences more significant performance degradation as client failure rates become increasingly severe. The entropy-based method's performance stability is further enhanced by its capability to mitigate the challenges associated with data skewness, a prevalent issue in non-IID data environments like those encountered in FL over CAV. In situations with high client failure rates, where data skewness is likely to be exacerbated, the entropy-based selection method ensures a well-balanced and comprehensive representation of the data. In turn, it diminishes the risks of overfitting specific client data patterns and promotes more efficient training, even when confronted with limited data resources.

5.4 Chapter Conclusions

In this master thesis, we presented a comprehensive evaluation of an entropy-based client selection method in vehicular FL environments. The primary objective was to assess the performance of the proposed method in both IID and non-IID data scenarios compared to a random client selection approach.In non-IID scenarios, the proposed method selects clients based on data entropy, ensuring diverse data distributions. This approach was compared with a random selection method to highlight performance differences, using metrics such as accuracy, AUC score, and training loss. Additionally, both selection methods were assessed in IID scenarios to understand performance differences in more uniform data distributions. We also analyzed client failure scenarios to evaluate the robustness of the selection methods.

In non-IID scenarios, the entropy-based selection method achieved higher accuracy and AUC scores compared to the random selection approach. This improvement is attributed to the selection of clients with diverse data distributions, which reduces the impact of biased data on the training process. The lower training loss observed indicates better convergence during the training process. The method also resulted in more stable and consistent performance over time, mitigating issues related to data imbalance and diversity. However, the entropy-based method requires additional communication to collect entropy information from clients, which could be a limitation in large-scale FL systems. In scenarios involving client failures, the entropy-based selection method maintained better performance metrics and faster convergence compared to the random selection method. The method consistently improved metrics and stability, which is crucial for vehicular networks dealing with non-IID data. In IID scenarios, both selection methods performed similarly, with a slight advantage for the entropy-based method. This suggests that while the entropy-based method excels in non-IID scenarios, it remains competitive in IID environments.

This master thesis demonstrates that entropy-based client selection significantly enhances the performance and stability of FL models in vehicular environments, particularly when dealing with non-IID data. By selecting clients with diverse and balanced data distributions, the proposed method mitigates the issues of overfitting and underfitting, leading to more reliable and consistent model performance. However, the additional communication overhead required to gather entropy information from all clients presents a potential limitation for large-scale implementations. Future work should explore optimizing this aspect to maintain the method's scalability. Overall, the findings of this master thesis underscore the importance of client selection strategies in FL and highlight the potential of entropy-based approaches to improve the robustness and efficiency of vehicular FL systems.

CHAPTER 6

Conclusion

This master thesis investigated the robustness and reliability of an entropy-based client selection mechanism in scenarios where vehicle failures can occur due to various failure events. The mechanism utilizes entropy to identify the most relevant and diverse data, contributing to developing models that effectively encapsulate the heterogeneity in the context of FL in CAV systems. The entropy-based client selection mechanism gives preference to select clients based on data diversity and representativeness, creating a more representative model. Simulation results presented the significance of incorporating entropy-based client selection when addressing the challenges presented by client failure events. Through comprehensive simulations and analyses, several key findings emerged, such as the entropy-based client selection mechanism demonstrated significant improvements in model performance in non-IID data scenarios compared to traditional random selection methods. This approach ensured that clients with more diverse and informative data were prioritized, leading to better generalization and robustness of the global model. Additionally, the mechanism showed superior resilience in scenarios with high client failure rates. By continuously selecting clients with high entropy, the method maintained model accuracy and stability, even when a significant number of clients failed to participate in the training process. Furthermore, the entropy-based selection method resulted in faster model convergence and reduced communication overhead. By involving fewer but more informative clients in each training round, the approach optimized the use of network resources and minimized unnecessary data transmission.

6.1 Concluding Remarks

The findings obtained in this master thesis have several important implications for implementing FL in vehicular networks. The entropy-based client selection mechanism offers a practical solution for improving model accuracy and robustness in environments with heterogeneous and dynamic data distributions. This is particularly relevant for ITS and autonomous driving applications, where data diversity and client variability are inherent challenges. By reducing the communication and computation overhead associated with the FL process, the proposed method enhances the scalability of FL in large-scale vehicular networks. This makes it feasible to implement FL in real-world ITS applications, where efficient use of network resources is crucial. Also, the usage of entropy as a selection criterion indirectly supports privacy preservation by minimizing the need for raw data exchange while the method's resilience to client failures contributes to the overall security and robustness of the FL process, mitigating the risks associated with malicious or unreliable clients.

While the research presented significant advancements, some limitations should be acknowledged. The findings are based on simulations and may not fully capture the complexities of real-world vehicular networks. Further research should involve real-world testing and validation to ensure the practical applicability of the proposed method. This study primarily focused on entropy-based client selection. While effective, it is essential to explore other complementary techniques and hybrid approaches that may offer additional benefits. The research assumed certain levels of client participation and network stability. Variations in these factors in real-world scenarios could impact the performance of the proposed method.

6.2 Future Works

Looking ahead, our future research aims to explore adaptive client selection mechanisms capable of dynamically responding to fluctuations in network conditions and vehicular mobility patterns. Such adaptability would enhance the overall robustness of FL in CAV scenarios, ensuring their effectiveness even in dynamic and challenging environments. Additionally, we intend to investigate the integration of privacy-preserving mechanisms tailored for vehicular settings. This exploration will evaluate how such mechanisms influence the resilience of client selection strategies, contributing further to the development of secure and reliable FL frameworks in dynamic and uncertain scenarios.

Building upon our current findings, we are also researching ways to apply entropy at the model level. This involves leveraging entropy measures to assess and enhance the robustness of the generated models themselves, particularly in scenarios with data alterations or adversarial attacks. By analyzing entropy at the model level, we aim to detect and mitigate the impact of corrupted or maliciously altered data, thereby improving the overall security and reliability of the FL process. Furthermore, we are exploring methods to manage non-static data scenarios effectively. Data is continuously generated and updated in real-world vehicular networks, presenting challenges for traditional FL approaches that assume a static dataset. Our research will focus on developing strategies to accommodate and efficiently learn from streaming data, ensuring that the FL models remain relevant and accurate over time.

By integrating these advanced techniques, we aim to create a more resilient and adaptive FL framework that can thrive in the dynamic and often unpredictable environments of vehicular networks. This comprehensive approach will address both the immediate challenges of client selection and the broader issues of model integrity and data fluidity, paving the way for more robust and secure FL systems in the future.

6.3 Published Works

The results of this master thesis submitted to the MSc. examination in Electric Engineering program at the Federal University of Pará was already accepted and published at a workshop paper(for WPerformance). The subsequent extensions were submitted and accepted in a conference paper(for SBRC) and a journal's article(for JBCS):

1. **Sousa, John**; Lobato, Wellington; Rosário, Denis; Cerqueira, Eduardo; Villas, Leandro. Entropy-based Client Selection Mechanism for Vehicular Federated Environments In: *Workshop em Desempenho de Sistemas Computacionais e de Comunicação (WPERFORMANCE), 2023.*

2. **Sousa, John**; Ribeiro, Eduardo; Bastos, Lucas; Rosário, Denis; Sousa, Allan; Cerqueira, Eduardo. Evaluation of Client Selection Mechanisms in Vehicular Federated Learning Environments with Client Failures In: *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC), 2024.*

3. Veiga, Rafael; **Sousa, John**; Morais, Renan; Rosário, Denis; Cerqueira, Eduardo. A Robust Client Selection Mechanism for Federated Learning Environments In: *Journal of the Brazilian Computer Society, 2024.*

References

[1] X. Tang, J. Zhang, Y. Fu, C. Li, N. Cheng, and X. Yuan, "A fair and efficient federated learning algorithm for autonomous driving," in *2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall)*, 2023, pp. 1–5.

[2] W. Lobato, P. Mendes, D. Rosário, E. Cerqueira, and L. A. Villas, "Redundancy mitigation mechanism for collective perception in connected and autonomous vehicles," *Future Internet*, vol. 15, no. 2, p. 41, 2023.

[3] X. Zhang, Z. Chang, T. Hu, W. Chen, X. Zhang, and G. Min, "Vehicle Selection and Resource Allocation for Federated Learning-Assisted Vehicular Network," *IEEE Transactions on Mobile Computing*, vol. PP, pp. 1–12, 2023.

[4] H. Zhang, J. Bosch, and H. H. Olsson, "End-to-end federated learning for autonomous driving vehicles," in *Proceedings of the International Joint Conference on Neural Networks (IJCNN)*, 2021, pp. 1–8.

[5] K. D. Stergiou, K. E. Psannis, V. Vitsas, and Y. Ishibashi, "A federated learning approach for enhancing autonomous vehicles image recognition," in *2022 4th International Conference on Computer Communication and the Internet (ICCCI)*. IEEE, 2022, pp. 87–90.

[6] L. Fantauzzo, E. Fanì, D. Caldarola, A. Tavera, F. Cermelli, M. Ciccone, and B. Caputo, "Feddrive: Generalizing federated learning to semantic segmentation in autonomous driving," in *prooceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*. IEEE, 2022, pp. 11 504–11 511.

[7] D. Jallepalli, N. C. Ravikumar, P. V. Badarinath, S. Uchil, and M. A. Suresh, "Federated learning for object detection in autonomous vehicles," in *prooceedings of the IEEE Seventh International Conference on Big Data Computing Service and Applications (BigDataService)*, 2021, pp. 107–114.

[8] L. Yuan, L. Su, and Z. Wang, "Federated transfer-ordered-personalized learning for driver monitoring application," *IEEE Internet of Things Journal*, 2023.

[9] M. F. Pervej, R. Jin, and H. Dai, "Resource Constrained Vehicular Edge Federated Learning With Highly Mobile Connected Vehicles," *IEEE Journal on Selected Areas in Communications*, vol. 41, no. 6, pp. 1825–1844, 2023.

[10] C. Zhang, Y. Xie, H. Bai, B. Yu, W. Li, and Y. Gao, "A survey on federated learning," *Knowledge-Based Systems*, vol. 216, p. 106775, 2021.

[11] X. Zhang, J. Liu, T. Hu, Z. Chang, Y. Zhang, and G. Min, "Federated learning-assisted vehicular edge computing: Architecture and research directions," *IEEE Vehicular Technology Magazine*, pp. 2–11, 2023.

[12] X. Lian, B. Yuan, X. Zhu, Y. Wang *et al.*, "Persia: An Open, Hybrid System Scaling Deep Learning-based Recommenders up to 100 Trillion Parameters," in *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2022, pp. 3288–3298.

[13] Z. Du, C. Wu, T. Yoshinaga, K.-L. A. Yau, Y. Ji, and J. Li, "Federated learning for vehicular internet of things: Recent advances and open issues," *IEEE Open Journal of the Computer Society*, vol. 1, pp. 45–61, 2020.

[14] Y. Liu, X. Yuan, Z. Xiong, J. Kang, X. Wang, and D. Niyato, "Federated learning for 6g communications: Challenges, methods, and future directions," *China Communications*, vol. 17, no. 9, pp. 105–118, 2020.

[15] O. A. Wahab, A. Mourad, H. Otrok, and T. Taleb, "Federated machine learning: Survey, multi-level classification, desirable criteria and future directions in communication and networking systems," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 1342–1397, 2021.

[16] Y. Xiong, R. Wang, M. Cheng, F. Yu, and C.-J. Hsieh, "Feddm: Iterative distribution matching for communication-efficient federated learning," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2023, pp. 16 323–16 332.

[17] J. L. R. Sousa, W. Lobato, D. Rosário, E. Cerqueira, and L. A. Villas, "Entropy-based client selection mechanism for vehicular federated environments," in *Proceedings of the 22nd Workshop on Performance of Computer and Communication Systems (WPERFORMANCE)*. SBC, 2023, pp. 37–48.

[18] A. Taïk, Z. Mlika, and S. Cherkaoui, "Clustered vehicular federated learning: Process and optimization," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 12, pp. 25 371–25 383, 2022.

[19] A. Nguyen, T. Do, M. Tran, B. X. Nguyen, C. Duong, T. Phan, E. Tjiputra, and Q. D. Tran, "Deep federated learning for autonomous driving," in *proceedings of the IEEE Intelligent Vehicles Symposium (IV)*. IEEE, 2022, pp. 1824–1830.

[20] T. Huang, W. Lin, L. Shen, K. Li, and A. Y. Zomaya, "Stochastic client selection for federated learning with volatile clients," *IEEE Internet of Things Journal*, vol. 9, no. 20, pp. 20 055–20 070, 2022.

[21] Y. Sun, G. S. Member, Y. Mao, and J. Zhang, "MimiC:Combating Client Dropouts in Federated Learning by Mimicking Central Updates," *arXiv:2306.12212v3*, pp. 1–17, 2023.

[22] Y. Shanmugarasa, H. young Paik, S. S. Kanhere, and L. Zhu, *A systematic review of federated learning from clients' perspective: challenges and solutions.* Springer Netherlands, 2023, vol. 56, no. s2.

[23] H. Yang, P. Qiu, P. Khanduri, M. Fang, and J. Liu, "Understanding server-assisted federated learning in the presence of incomplete client participation," 2024.

[24] X. H. B. Z. T. P. P. P. Hongle Guo, Yingchi Mao, "Improving federated learning through abnormal client detection and incentive," *Computer Modeling in Engineering & Sciences*, vol. 139, no. 1, pp. 383–403, 2024.

[25] J. Sousa, E. Ribeiro, L. Bastos, D. Rosário, A. Sousa, , and E. Cerqueira, "Evaluation of client selection mechanisms in vehicular federated learning environments with client failures," in *Proceedings of the Brazilian Symposium on Computer Networks and Distributed Systems (SBRC).* SBC, 2024.

[26] M. M. Rana and K. Hossain, "Connected and autonomous vehicles and infrastructures: A literature review," *International Journal of Pavement Research and Technology*, vol. 16, no. 2, pp. 264–284, Mar 2023.

[27] D. Elliott, W. Keen, and L. Miao, "Recent advances in connected and automated vehicles," *Journal of Traffic and Transportation Engineering (English Edition)*, vol. 6, no. 2, p. 109–131, Apr. 2019.

[28] L. Pacheco, T. Braun, D. Rosário, A. Di Maio, and E. Cerqueira, "A distributed aggregation approach for vehicular federated learning," *IEEE access*, 2024.

[29] P. Kairouz, H. B. McMahan, B. Avent, A. Bellet, M. Bennis, A. N. Bhagoji, K. Bonawitz, Z. Charles, G. Cormode, R. Cummings, R. G. L. D'Oliveira, H. Eichner, S. E. Rouayheb, D. Evans, J. Gardner, Z. Garrett, A. Gascón, B. Ghazi, P. B. Gibbons, M. Gruteser, Z. Harchaoui, C. He, L. He, Z. Huo, B. Hutchinson, J. Hsu, M. Jaggi, T. Javidi, G. Joshi, M. Khodak, J. Konečný, A. Korolova, F. Koushanfar, S. Koyejo, T. Lepoint, Y. Liu, P. Mittal, M. Mohri, R. Nock, A. Özgür, R. Pagh, M. Raykova, H. Qi, D. Ramage, R. Raskar, D. Song, W. Song, S. U. Stich, Z. Sun, A. T. Suresh, F. Tramèr, P. Vepakomma, J. Wang, L. Xiong, Z. Xu, Q. Yang, F. X. Yu, H. Yu, and S. Zhao, "Advances and open problems in federated learning," 2021.

[30] A. Bastos, R. Veiga, R. Morais, D. Rosário, and E. Cerqueria, "Mesfla: Model efficiency through selective federated learning algorithm," *Journal of Internet Services and Applications*, 2024.

[31] R. Yang, J. Tian, and Y. Zhang, "Regularized mutual learning for personalized federated learning," in *Proceedings of The 13th Asian Conference on Machine Learning*, ser. Proceedings of Machine Learning Research, V. N. Balasubramanian and I. Tsang, Eds., vol. 157. PMLR, 17–19 Nov 2021, pp. 1521–1536.

[32] W. Lobato, J. B. Costa, A. M. Souza, D. Rosario, C. Sommer, and L. A. Villas, "FLEXE: Investigating Federated Learning in Connected Autonomous Vehicle Simulations," *IEEE Vehicular Technology Conference*, vol. 2022-Septe, 2022.

[33] S. Dutta, G. Joshi, S. Ghosh, P. Dube, and P. Nagpurkar, "Slow and stale gradients can win the race: Error-runtime trade-offs in distributed sgd," in *International conference on artificial intelligence and statistics.* PMLR, 2018, pp. 803–812.

[34] F. Araújo, L. Bastos, I. Medeiros, O. A. Rosso, A. L. Aquino, D. Rosário, and E. Cerqueira, "Characterization of human mobility based on information theory quantifiers," *Physica A: Statistical Mechanics and its Applications*, vol. 609, p. 128344, 2023.

[35] H. Zhu, J. Xu, S. Liu, and Y. Jin, "Federated learning on non-IID data: A survey," *Neurocomputing*, vol. 465, pp. 371–390, 2021.

[36] V. P. Chellapandi, L. Yuan, C. G. Brinton, S. H. Żak, and Z. Wang, "Federated learning for connected and automated vehicles: A survey of existing approaches and challenges," *IEEE Transactions on Intelligent Vehicles*, vol. 9, no. 1, pp. 119–137, 2024.

[37] H. Wang and J. Xu, "Combating Client Dropout in Federated Learning via Friend Model Substitution," *arXiv preprint arXiv:2205.13222*, 2023.

[38] T. Liu, H. Zhou, J. Li, F. Shu, and Z. Han, "Uplink and Downlink Decoupled 5G/B5G Vehicular Networks: A Federated Learning Assisted Client Selection Method," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 2, pp. 2280–2292, 2023.

[39] A. Souza, L. Bittencourt, E. Cerqueira, A. Loureiro, and L. Villas, "Dispositivos, eu escolho vocês: Seleção de clientes adaptativa para comunicação eficiente em aprendizado federado," in *Anais do XLI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC).* Porto Alegre, RS, Brasil: SBC, 2023, pp. 1–14.

[40] F. Araújo, L. Bastos, I. Medeiros, O. A. Rosso, A. L. Aquino, D. Rosário, and E. Cerqueira, "Characterization of human mobility based on Information Theory quantifiers," *Physica A: Statistical Mechanics and its Applications*, p. 128344, 2023.

[41] R. Veiga, J. Sousa, R. Morais, L. Bastos, W. Lobato, D. Rosário, and E. Cerqueira, "A robust client selection mechanism for federated learning environments," *Journal of the Brazilian Computer Society*, 2024.

[42] J. Zhang, Y. Hua, H. Wang, T. Song, Z. Xue, R. Ma, and H. Guan, "Fedala: Adaptive local aggregation for personalized federated learning," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 37, no. 9, 2023, pp. 11 237–11 244.

[43] G. S. Pannu, S. Ucar, T. Higuchi, O. Altintas, and F. Dressler, "Dwell time estimation at intersections for improved vehicular micro cloud operations," *Ad Hoc Networks*, vol. 122, p. 102606, 2021.

[44] L. Codeca, R. Frank, S. Faye, and T. Engel, "Luxembourg SUMO Traffic (LuST) Scenario: Traffic Demand Evaluation," *IEEE Intelligent Transportation Systems Magazine*, vol. 9, no. 2, pp. 52–63, 2017.