Received 26 June 2023; accepted 11 July 2023. Date of publication 3 August 2023; date of current version 22 September 2023.

Digital Object Identifier 10.1109/OJCOMS.2023.3301679

6G-Enabled Mobile Access Point Placement via Dynamic Federated Learning Strategies

PAUL MIRDITA[1] (Student Member, IEEE), YAHUZA BELLO[2], AHMED REFAEY[2] (Senior Member, IEEE), AND AYMAN RADWAN[3,4] (Senior Member, IEEE)

[1]Electrical and Computer Engineering Department, Manhattan College, Riverdale, NY 10463, USA

[2]School of Engineering, University of Guelph, Guelph, ON N1G 2W1, Canada

[3]DETI, Universidade de Aveiro, 3810-193 Aveiro, Portugal

[4]Instituto de Telecomunicações, 3810-193 Aveiro, Portugal

CORRESPONDING AUTHOR: A. REFAEY (e-mail: ahmed.refaey@ieee.org)

ABSTRACT Advanced Indoor Positioning Systems (IPS) based on Received Signal Strength (RSS) fingerprints have been paramount in 6G network research and commercial exploitation due to their cost-effectiveness and simplicity. Despite their popularity, the advent of 6G has prompted a shift towards exploring Deep Learning algorithms to further enhance their performance and precision. Deep Learning research typically demands large datasets, leading to reliance on data augmentation and crowdsourcing techniques for data collection. However, the traditional centralization of data in crowdsourcing poses privacy risks, and here is where Federated Learning (FL) comes into play. In light of this, our study introduces FL to bridge this divide in a decentralized way, eliminating the need for servers to acquire labeled data directly from users. This approach aims to minimize localization error in RSS fingerprints, preserve user privacy, and reduce system latency, all key goals for 6G networks. Moreover, we explore the use of power transmission techniques to further decrease the latency in the FL system. Our simulation outcomes confirm the superiority of FL over traditional Stochastic Gradient Descent (SGD) methods considering critical evaluation metrics like localization error and global loss, paving the way for efficient 6G implementation.

INDEX TERMS Federated learning, indoor localization, received signal strength, power transmission, edge devices, privacy.

I. INTRODUCTION

THROUGH the journey of innovation over the years, there has been tremendous focus in the areas of cloud computing and Machine Learning (ML). This is because Artificial intelligence (AI), specifically ML is anticipated to be very significant in the design of the sixth generation (6G) networks [1]. As the inclusion of IoT devices in these technologies is projected to rise over the coming years, security has become an underlying issue that must be addressed regarding the technologically evolved world [2], [3]. Advanced Web technologies, ML, and the adoption of a large number of sensors have enabled data collection through mining and scraping, which pave the way for the emergence of big data. Big data creates opportunities for several innovative solutions, however, it comes with the cost of centralized data and the vulnerabilities associated with data storage on central servers [4].

Currently, the Internet is largely based on the traditional client-server model, which involves the end user (client) communicating back and forth with a server in order to gather or act upon the data stored in the server or in a database. The underlying issue with this model is associated with the servers or the database (which are centralized) that hold the data. The data can include a user's personal information which serves as a risk and concern for the user. Thus, the idea of decentralization was widely adopted in both academia and industries, which encourage the explosive research performed on Federated Learning (FL) [5].

The rise in use cases of FL applications is foreseeable due to the rise in demand for data as well as its security. The traditional approach in training models requires users' data to be exchanged from the server and the user and vice versa (this does not account for a shared model amongst users in a network). To this end, the FL technique includes a centralized server (i.e., edge server in this context) communicating with users (i.e., edge devices in this context). This technique acts as a data security protocol that issues a global model to edge devices. The edge devices proceed to use their own local data to train the given model. Once trained, the local model's results (excluding the local data) are transferred to the edge server from every edge device, and the new global model is aggregated on the central server.

Indoor localization is another heavily researched topic given that it can be used as an alternative to Global Positioning System (GPS) in areas where GPS signals are not available [6], and applications that require user's location such as museums tours, the guiding system for the visually impaired, etc. Whilst this area of study is beneficial for several applications, it may pose numerous risks in user privacy if not properly managed.

One of the major drawbacks of indoor localization systems is acquiring information on users' location through the central server [7]. This introduces the opportunities for unethical measures that may include tracking a client's location in real-time. Location tracking is generally unethical since the user's data gathered can be used for malicious intent or can be sold to a third party for profit [8]. Along with security issues, there is also a potential latency issue as well that is faced when transmitting and receiving data to and from a server. To solve latency-related issues, Multi-access Edge Computing (MEC) emerges, where edge devices send their computational tasks to what is known as an edge server in an effort to complete a task [9]. Several task-uploading schemes that consider the communication of multiple edge devices with the edge servers were proposed in the literature [10], [11].

To this end, FL can be implemented in an effort to mitigate the latency concerns as well as security risks that come with including the WiFi fingerprinting technique in client-server communication within the domain of indoor localization. For example, dynamic APs can be utilized to distribute local models used in FL system. Using these dynamic APs, the updated models can be efficiently distributed to participating edge devices as the models improve and evolve. As a result, the latest model versions are available to all FL devices, improving indoor localization accuracy and reliability. Optimizing the positioning of these dynamic APs to assist in the FL process is crucial especially in 6G networks, where optimum network performance without compromising user privacy is vital.

Therefore, this research paper focuses on integrating data privacy and reducing latency in an indoor localization system by utilizing FL. The primary objective is to enhance the existing system model for dynamic APs [12]. The utilization of dynamic APs offers several advantages, including improved localization accuracy, addressing connection and latency issues, and serving as a dynamic feature that extends coverage. Specifically, the system incorporates mobile APs, referred to as dynamic devices, which move through areas where clients are not in close proximity to static APs. These dynamic APs expand the coverage area, thereby providing better service to users in various sections of the indoor environment. Consequently, this approach ensures sufficient service provision for clients throughout the indoor environment while safeguarding the privacy of location data stored on edge devices.

The main contributions of this paper can be summarized as follows:

- Integration of dynamic APs with FL to achieve reduced localization error according to the Received Signal Strength (RSS) fingerprints. This approach simultaneously maintains user privacy and minimizes system latency.
- Creation of a real-time indoor environment simulation involving multiple users, replicating typical scenarios accurately. This simulation aids in evaluating the effectiveness of the proposed approach.
- Implementation and analysis of the FL technique using the UJIIndoorLoc dataset to demonstrate its performance in terms of data security and latency reduction. This dataset serves as a reliable benchmark for evaluating the proposed FL system.

The rest of this paper is organized as follows: Section II addresses the constraints associated with data security in an indoor localization system. This includes the challenges posed by transmitting a user's complete WiFi fingerprint to a central server. Furthermore, it explores relevant previous work in tackling this issue and examines the application of FL in the context of localization. Section III provides a comprehensive explanation of FL, encompassing its algorithmic aspects and implementation details. In Section IV, the experiment itself is described, along with a step-by-step account of the FL process employed. Section V presents the results obtained from the experiment, highlighting the performance of the FL technique in comparison to alternative approaches. Furthermore, it discusses the findings related to energy consumption within the system and investigates the impact of power transmission among static APs. Section VI entails a discussion of the obtained results and offers concluding remarks. Additionally, it provides insights into potential future advancements that can be explored using the approach proposed in this research.

II. RELATED WORK

In recent years, the issue of privacy in indoor localization has received significant attention, leading to various experimental approaches aimed at addressing this concern. Concurrently, FL is used to address security issues related to storing clients' private information on centralized servers. This section gives background on the latest advancements in the field, exploring state-of-the-art research that investigates data security

in Indoor Positioning Systems (IPS) and the methodologies employed to tackle this fundamental challenge.

A. FEDLOC: FEDERATED LEARNING FRAMEWORK

The development of the FedLoc framework, which employs Federated Learning (FL) in the context of indoor localization, aims to overcome various limitations faced by indoor localization applications. The paper examines the algorithms commonly used in FL and explores practical applications of this technique [13]. The authors highlight the drawbacks of traditional training and testing models, particularly the substantial storage requirements associated with storing large volumes of data. In response, the FedLoc framework is introduced to address these challenges by focusing on optimizing server space utilization, scaling network capacity to accommodate more users, preserving data privacy, and enhancing the overall network performance. The core principle of the FedLoc framework involves restricting mobile users/agents from locally collecting data on their devices, instead leveraging local data from a network of users to approximate a global model [13].

To present the performance of the FedLoc framework, the authors conducted experiments using a Gaussian Process State Space Model (GPSSM) for indoor target tracking. The objective was to develop a collaborative and data-driven approach to learn human walking trajectories. This involved collecting 50 trajectories comprising a total of 25,000 samples. During training, three mobile users contributed 15 trajectories each, which were used to train both the local and global models stored on the edge server. The intent was to leverage these trajectories to improve the global model's accuracy [13].

However, upon comparing the training and testing results of the recorded movements within the experimental area, the authors observed unsatisfactory outcomes. The accuracy of trajectory estimation was compromised due to the choice of the Gaussian Process model. Consequently, it became apparent that a greater number of Access Points (APs) were required to achieve more precise positioning, along with the potential need for additional data to improve the model's performance. Our approach addresses this issue by utilizing dynamic APs strategically distributed throughout the indoor environment in our model, ensuring a significant improvement in performance.

B. LIGHTWEIGHT PRIVACY PRESERVING SCHEME (LWP^2)

To tackle the challenges of cost and privacy in localization applications, a Lightweight Privacy-Preserving Scheme (LWP^2) was introduced in a previous work [14]. This scheme was specifically developed to overcome the limitations of existing data privacy frameworks employed in the field of indoor localization. The primary focus of this experiment was on reducing the time required for transmitting and receiving data between the end device and the localization server (i.e., the central server).

The LWP^2 framework was inspired by the observation of traditional approaches to the problem. In these approaches, users' locations are calculated by the server using an algorithm in ciphertext space, and the encrypted results are returned to ensure privacy and data protection. Building on this concept, the LWP^2 scheme encrypts a user's Wi-Fi RSS and transmits it to the server. Upon receiving the RSS information from the end user, the server searches for the k closest fingerprints resembling that user and performs matrix operations to determine the user's location in space.

While this experiment successfully improves data privacy, it introduces a reliance on matrix operations that can be computationally intensive and costly, particularly in systems with numerous end users. Furthermore, the experiment did not consider the latency associated with the localization process after undergoing matrix operations. Real-time localization applications face constraints not only in terms of result accuracy but also in achieving these results within an acceptable time frame. In light of these observations, our approach takes into account the missing latency component in the LWP^2 framework and incorporates it into our model. By addressing both the accuracy and latency aspects, our approach aims to overcome the limitations identified in the [14], ensuring efficient real-time localization results while maintaining data privacy.

C. PSEUDO LABEL-DRIVEN FEDERATED LEARNING

One significant challenge in ML today is the scarcity of data available for various applications. To address this issue, mobile crowdsourcing has emerged as a method to collect large volumes of information for system calibration. Despite the growing popularity of indoor localization, there is a pressing need for approaches that can efficiently gather a substantial number of RSS fingerprints to train accurate models. In response to this challenge, a Centralized Indoor Localization method using Pseudo-labels (CRNP) was introduced, which leverages FL to ensure data privacy during experimentation.

The CRNP technique involves collecting a limited number of labeled data (RSS fingerprints) alongside a large set of unlabeled data. This approach reduces the reliance on collecting labeled data while improving system performance. The experiment revealed that the utilization of extensive location data while preserving privacy can result in high network costs due to the expenses associated with data transmission and storage. This led to the development of CRNP.

While CRNP facilitates the collection of labeled fingerprint data, the pseudo-label technique is employed to extract information from the unlabeled crowdsourced data. By combining these methods with the FL approach, a decentralized solution is achieved, resulting in a robust indoor localization system. The experimental results demonstrate improved training and testing accuracy using this approach, although the network cost performance remains consistent when comparing the centralized and decentralized approaches.

TABLE 1. Federated learning timeline.

Year and Ref.	Summary
2018 [15]	Evaluates the threats faced by FL in the form of sybil-based poisoning attacks and proposes FoolsGold, a mechanism that identifies poisoning sybils based on the differences in client updates, without bounding the number of attackers, requiring external information, or making extensive predictions about users and their information.
2018 [16]	Reveals an unintended information leakage about participants' training data in FL systems and presents passive and active inference attacks that gives an attacker a way to infer specific data points and properties of others' training data.
2019 [17]	Presents FL framework on mobile devices that can be scaled in production environment, utilizing TensorFlow, and discusses its high-level design, challenges, solutions, and future directions.
2020 [18]	Introduces sparse ternary compression (STC), a compression framework tailored for FL, which combines top-k gradient sparsification with downstream compression, ternarization, and encoding of weight updates.
2020 [19]	Proposes a novel framework called noising before model aggregation FL (NbAFL) that adds artificial noise to client parameters before aggregation to ensure differential privacy, and provides theoretical analysis on convergence and tradeoffs between convergence performance and privacy protection levels in NbAFL.
2021 [20]	Addresses the dynamic FL problem in a power grid mobile edge computing setting by proposing a delay deadline constrained FL framework and formulating a dynamic client selection problem, with two online client selection algorithms proposed to optimize utility in the learning framework.
2021 [21]	Explores the resource allocation problem in Wireless FL networks (WFLNs), emphasizing the interdependence and fluctuating levels of learning rounds for the final learning outcome, highlighting the need for an optimized long-term perspective in allocating limited wireless resources for FL in classic wireless networks.
2022 [22]	Proposes a new method to improve indoor localization in FL by considering the reliability of local clients, using Monte Carlo dropout with Bayesian technique to improved efficiency in using computational resources.
2022 [23]	Introduces a Prediction based Semi-supervised Online Personalized FL (PSO-PFL) method to address the challenges of frequent data collection, privacy exposure, and user-specific localization requirements in fingerprint-based indoor localization using deep learning and FL.
2023 [24]	Proposes a FL framework called FedLoc3D to address the challenges of classifying building-floor classification and Latitude-Longitude Regression (LLR) in fingerprinting-based indoor localization, using a Convolutional Neural Network (CNN) with depth-wise separable convolutions for classification of the building floors and a Deep Neural Network (DNN) with autoencoder and data augmentation for LLR. The framework enables collaborative learning on data that are decentralized and heterogeneous and are operating over an imperfect network in a wide 3-D space.

D. PRESERVING PRIVACY IN WIFI LOCALIZATION WITH PLAUSIBLE

Privacy preservation is a critical area of focus in the domain of localization, particularly indoor localization, and researchers are devoting significant efforts to enhance the existing systems. In this context, the experiment introduces a novel approach called the Location Preservation Algorithm with Plausible Dummies (LPPD) [25], which sets itself apart from other related works.

The LPPD process begins when a user initiates a request for indoor localization services and collects RSS measurements associated with their precise location. To protect the privacy of a user, the user identifies an available Cloaking Region (CR) where their location can be concealed. Within this chosen CR, "dummy locations" are mapped to corresponding "dummy signals." Instead of transmitting the exact user location to the central server, this approach involves sending queries containing both the user's location and the dummy locations to the localization server. The server then calculates estimated locations for both the dummy locations and the user, which are subsequently returned to the user. By comparing the received locations, the user can determine their own location using the RSS signals privately, without disclosing the exact location to the central server. Table 1 provides a summary of recent research studies from the literature that propose the adoption of FL in indoor localization systems.

III. FEDERATED LEARNING ALGORITHM

FL is optimally elaborated by separating the system into their own entities; edge device(s) and edge server. This section discusses the overview of the FL algorithm and the methods used to achieve the desired performance in the context of IPS.

A. OVERVIEW

The significance of FL arises from addressing vulnerabilities in data transmission and reception between entities. Recent efforts have introduced various FL variants, including centralized, decentralized, and heterogeneous FL. In traditional approaches, a data pipeline with a central server hosting machine learning models is used for predictions, but this compromises data privacy. In contrast, FL enables real-time

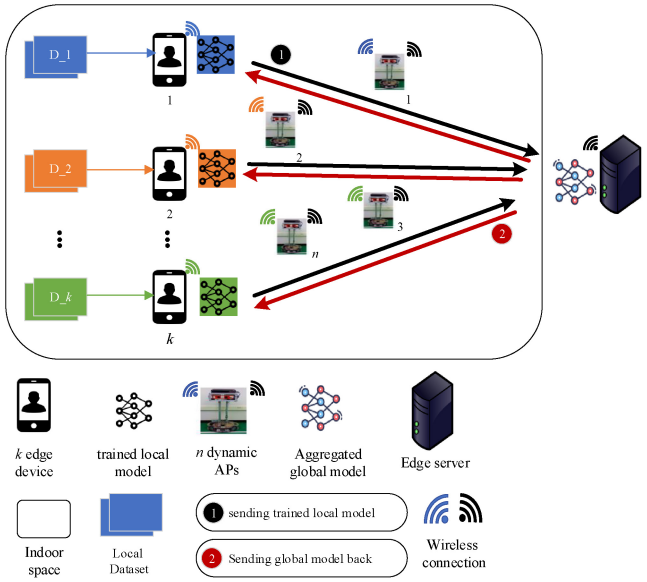


FIGURE 1. Model Setup.

model training and privacy preservation by updating models directly on client devices (edge devices) using local data. The updated models are then aggregated on the central server to create a global model by averaging the weights, enhancing learning efficiency and reducing global communication frequency. The consolidated global model is sent to all edge devices, and this cycle is repeated iteratively as depicted in Figure 1.

The concept of federated learning FL is rooted in collaborative machine learning, where edge devices, such as mobile devices, work together to keep local data on their respective devices rather than on a central server. FL offers benefits such as reducing latency by avoiding sending data to a central server and back to edge devices. Furthermore, FL enables edge devices to make predictions even without Internet connectivity by training models directly on the devices. Additionally, FL helps reduce the overall system cost by mitigating the burden on the central server, as it receives smaller models from individual edge devices instead of continuous raw data. This distribution of overhead to the devices reduces the need for expensive hardware.

While initially introduced in [26] to address privacy concerns, it was later recognized that the FL also has a significant impact on reducing latency during training. The time taken to transfer data from the server to edge device(s) is used to determine the effectiveness of FL, and improved latency opens up new use cases. One such use case, as depicted in Figure 2, involves dynamic access points (APs) that can change their location based on the RSS strength at a given moment, depending on the user's proximity.

B. ALGORITHM

Federated averaging is very significant in the context of FL, as it is a fundamental concept introduced in [26]. While the initial introduction of FL defines the concept, algorithm 1 provides a clear presentation of the underlying process as it unfolds. In a nutshell, The Federated Averaging algorithm involves initializing a global model, distributing it to selected clients (i.e., q clients chosen randomly, where parameter C controls the fraction of selected clients stored in S_t) for local training, aggregating their updated models through averaging, and iteratively updating the global model. The client update is done by splitting $\mathcal{D}_k$ datasets into batches of size B, which is stored in $\mathcal{B}$ as shown in Algorithm 1.

Algorithm 1: K Clients Are Indexed by k; B Is the Local Minibatch Size, E Is the Number of Local Epochs, and η Is the Learning Rate

Server Executes:
initialize w_0
for *each round* $t = 1, 2, \ldots$ **do**
  $q \leftarrow \max(C \cdot K, 1)$
  $S_t \leftarrow$(random set of q clients)
  for *each client* $k \in S_t$ *in parallel* **do**
    $w_{t+1}^k \leftarrow$ ClientUpdate (k, w_t)
  end
  $w_{t+1} \leftarrow \sum_{k=1}^{K} \frac{n_k}{n} w_{t+1}^k$
end
ClientUpdate (k, w):
$\mathcal{B} \leftarrow$ (split $\mathcal{D}_k$ into batches of size B)
for *each local epoch i from 1 to E* **do**
  for *batch* $b \in \mathcal{B}$ **do**
    $w \leftarrow w - \eta \nabla \ell(w; b)$
  end
end
return w to server

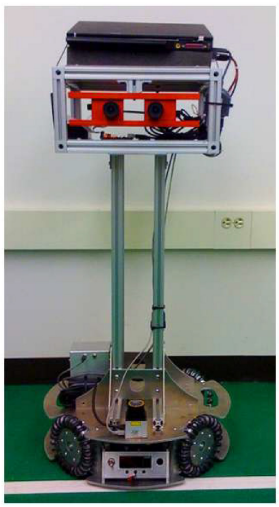


FIGURE 2. Mobile AP Acting as a Dynamic AP [12].

IV. EXPERIMENT

Having presented the federated averaging algorithm, it is time to focus on the equations pertaining to the utilization of

RSS measurements. As mentioned earlier, the initial iteration involves initializing a global model based on locally trained models, which are then collected by the central server, as shown in Figure 1. The RSS fingerprints are initially collected by edge devices, indicating that the initial models originate from these devices. The inputs (n) represent the number of access points (APs) distributed in the indoor environment, which is set to 520 based on the UJIIndoorLoc dataset. Essentially, m data points (RSS measurements) are collected from n APs, and each AP is associated with k sets of clients acquiring RSS measurements.

A. PREPROCESSING PHASE

Each location coordinate obtained from an RSS fingerprint is represented as the i-th sample per measurement, given in Cartesian coordinates as

$$Y_i = \left[x_i, y_i\right]^T, \forall_i \in M \tag{1}$$

where x_i and y_i represent the x and y coordinates, respectively, and M denotes the set RSS training samples.

Considering that each training sample i includes l_i RSS values obtained from a subset of the total APs in the building, it follows that $l_i \leq k$, since not every edge device will have access to all APs. Thus, the measurement vector is represented as

$$s_i = \left[r_{ij_1} \ldots r_{ij} \ldots r_{ij_{L_i}}\right], \forall_i \in M, j \in L_i \tag{2}$$

where r_{ij} denotes the RSS value for the j-th AP in the i-th training sample, M represents the set of all RSS training samples, and L_i represents the subset of APs with RSS values in the i-th training sample.

During the initialization of the Multi-Layer Perceptron (MLP) model, the input layer size is determined by the number of users or clients, denoted as k. If an AP is not in proximity for coverage during the i-th sample, the corresponding RSS value in the input vector is set to a predefined minimum value Q, indicating the absence of coverage. The input vector for the MLP model during the i-th sample is represented as

$$\boldsymbol{X_i} = \left[r_{i1} \cdots r_{ij} \cdots r_{ik}\right] \tag{3}$$

with $r_{ij} = Q$ for $j \notin L_i$, indicating the RSS values for APs that are not included in the subset near the client. In other words, the unreadable APs are marked as constants.

B. SERVER-SIDE TRAINING PHASE

After preprocessing the data and dividing the training samples into batches, the server starts by initializing the global model, which in this case is an MLP. As mentioned earlier, the number of input nodes in the MLP is determined by the number of access points (APs) in the building. The number of hidden nodes and hidden layers is based on the size of the training samples and the likelihood of the model overfitting or underfitting with these hyperparameter settings. Additionally, the output layer of the MLP consists of two nodes to output the x and y coordinates.

Similar to a typical neural network, the MLP model used in the federated averaging algorithm employs backpropagation, which leads to a minimization problem. The equation involved in this process is similar to the one presented in [27], highlighting the dependence on the loss function f.

$$\min_{\boldsymbol{w}} \frac{1}{\gamma} \sum_{i=1}^{m} f(\boldsymbol{w}, \boldsymbol{u_i}, \boldsymbol{v_i}) \tag{4}$$

The minimization process begins once the global model is distributed to the edge devices. In this context, u_i represents the label for the i_{th} sample, v_i denotes the input training vector, w corresponds to the model weights, and γ indicates the number of training vectors used in the global model. It's important to note that the minimization process takes place exclusively within the server, where the global model is aggregated.

C. DISTRIBUTION PHASE

During the communication rounds in the federated averaging algorithm, which represent the iterations of transmitting the global model and receiving local models from edge devices, the averaging and distribution of training samples occur. Each round involves k clients collecting training data (RSS measurements) from the APs in their proximity, indicated by their respective measurement locations within the building. As the positions of APs is dynamic throughout the experiment, the mobility of edge devices leads to changes in training samples based on their location in the building. Equations (5) and (6) capture the essence of federated averaging, a fundamental concept described in [28], within this technique:

$$\boldsymbol{w}^{t+1} = \frac{1}{H^t} \sum_{p=1}^{N} m_p^t \boldsymbol{w_p^t} \tag{5}$$

$$H^t = \sum_{p=1}^{N} m_p^t \tag{6}$$

Once the federated averaging process is finished, the updated global model is sent back to the edge devices, where they repeat the local model training process using the updated global model, and this cycle continues until convergence is achieved. Table 2 presents a list of parameters that provide a concise description of the equations presented in the context.

V. RESULTS AND DISCUSSIONS

A. EXPERIMENT SETTINGS AND RESULTS ANALYSIS

The experiment focused on accuracy and computing time per training round using the UJIndoorLoc dataset, which contains approximately 20,000 samples from a 4-floor building covering an area of 105,300 square meters. Each sample includes RSS readings from 520 static APs, location data, and a time stamp. Two cases, classical Stochastic Gradient Descent (SGD) and FL, were considered with different

TABLE 2. Parameter description.

Parameters	
$\mathbf{Y}_i$	ith sample per RSS measurement
y_i	y-axis location
x_i	x-axis location
$\mathbf{s}_i$	RSS values per i training sample
r_{ij}	RSS value from AP
i	ith training sample
j	jth AP
M	Set of all the RSS training samples
L	APs in the training sample
$\mathbf{X}_i$	Input vector for model
w	Model weights
f	Loss function
m	Number of training vectors in model
H	total number of training samples
t	Communication round

TABLE 3. FL parameters.

Parameter	Value
Adopted Libraries	TensorFlow & Keras
Optimizers	Adam, Adaddelta, Adagrad and Adamax
Learning Rate	0.0001
β_1, β_2	0.1,0.99
Hidden Layer Formation	$20 \times 10 \times 10 \times 10 \times 10$
Activation Function	ReLu
Loss Function	Mean Absolute Error (MAE)
Batch Size	100
Number of Epochs in a Round	10
Number of Access Points n	520
Number of Users k	15 to 40
Number of Training Samples	3000 to 15000
Number of Test Samples	3000

parameters. The FL technique utilized an MLP model with $20x10x10x10x10$ layers, taking into account the hardware limitations of mobile devices. The number of epochs was set to 20, the batch size to 100, and the experiment analyzed the impact of FL (with different optimizers) on completion time per iteration while considering the constraints of power consumption and computational time. The experiment also included numerous hidden layers in the MLP model to explore the potential for extracting additional features. The conclusions were drawn based on the effect of FL on completion time per iteration, considering both time and accuracy and expanding the number of clients. Table 3 presents the hyperparameters for the FL system.

Figure 3 displays the comparison of five optimizers, including four federated learning (FL) approaches and the classical SGD optimizer. Adagrad, Adadelta, and Adam optimizers demonstrated convergence with minimal noise during the training phase, while SGD and Adamax did not converge

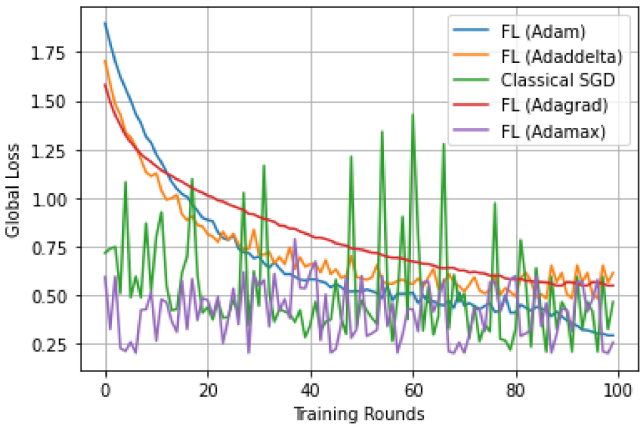


FIGURE 3. Global Loss per Training Round.

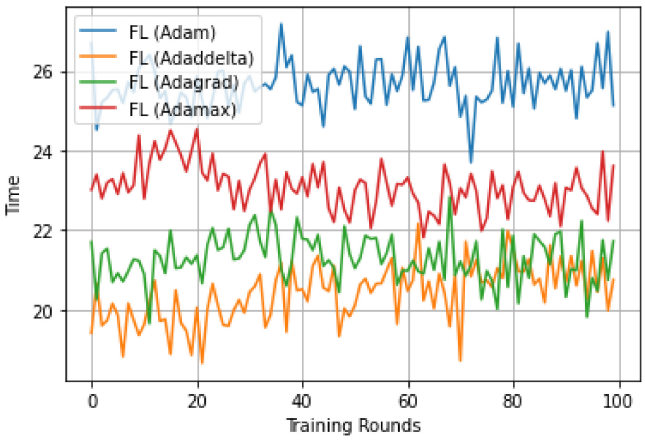


FIGURE 4. Communication Round Time per Training Round.

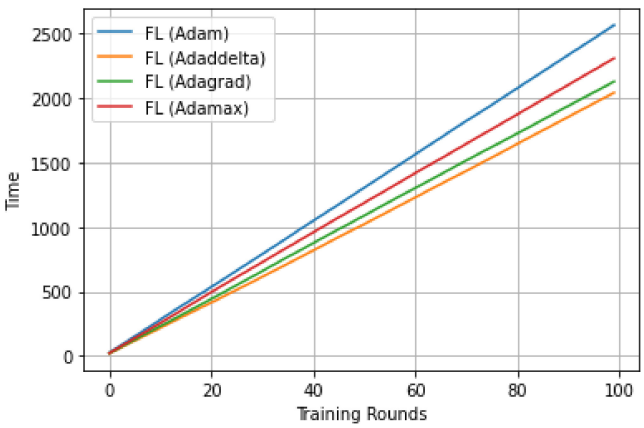


FIGURE 5. Cumulative Communication Round Time per Training Round.

and showed noise in their predictions. Despite starting with low global loss, SGD failed to achieve convergence, while Adamax, despite incorporating FL, also failed to converge, although it performed better than SGD.

Figure 4 illustrates the training time for each training round, with noticeable differences in completion times among the optimizers. Adadelta outperformed the other optimizers in terms of speed. Additionally, Figure 5 presents

the cumulative time taken to complete 100 training rounds, further confirming Adadelta's superior performance.

Based on these results, FL yielded comparable benchmarking metrics to training and testing with classical SGD. While these results may be considered insignificant by some engineers, adopting FL in an indoor environment ensures privacy preservation among clients, low latency, and high accuracy.

B. ANALYSIS OF THE ENERGY CONSUMPTION CONSTRAINTS

FL, renowned for its privacy preservation, has the potential to reduce overall energy consumption. In applications involving access points (APs), power measurements play a crucial role in assessing the sustainability of an indoor positioning system (IPS) based on energy efficiency [29]. This section considers evaluations of power transmission from APs in relation to completion time and incorporates the convergence of localization error when adjusting the training ratio.

1) EDGE DEVICE COMPUTATIONS AND MODELS

Based on the number of edge devices present in the environment, the number of active local models will correspond to the number of edge devices. Each local model is trained on its own batch of size b utilizing D_k (i.e., local data), which is stored exclusively on the edge device denoted by K. As mentioned earlier, local models are trained on edge devices using the distributed local model received from the edge server. Therefore, all edge devices, including the k-th device, receive the same local model but train it with their respective unique local data. The local models undergo a specified number of training steps (epochs) denoted by ε. The following equation represents the local computation delay, indicating the time required for the batch in the local model to complete training for all epochs:

$$T_k^{cmp} = \varepsilon \frac{|D_k|\Phi}{f_k^{\text{cmp}}} \tag{7}$$

f_k^{cmp} represents the clock speed (in GHz) and Φ represents the number of cycles necessary to compute a sample of data in the batch. Thus, this equation leads to the following equation representing the amount of energy required from each edge device in an effort to complete training per local model. The equation equates to E_k^{cmp}

$$E_k^{cmp} = \frac{\alpha_k}{2}\left(f_k^{\text{cmp}}\right)^3 T_k^{cmp} \tag{8}$$

Additionally, α_k represents the capacitance coefficient due to a given edge device. After substituting T_k^{cmp} in the equation, we are left with the following,

$$E_k^{cmp} = \frac{\alpha_k}{2}\left(\varepsilon\left(f_k^{\text{cmp}}\right)^2 |D_k|\Phi\right) \tag{9}$$

As discussed earlier in this work, once the edge devices have completed their local training, they are transmitted to the edge server (central server) to be aggregated via federated averaging and thus the cycle continues until convergence. These equations display the power results that were calculated throughout the steps taken place.

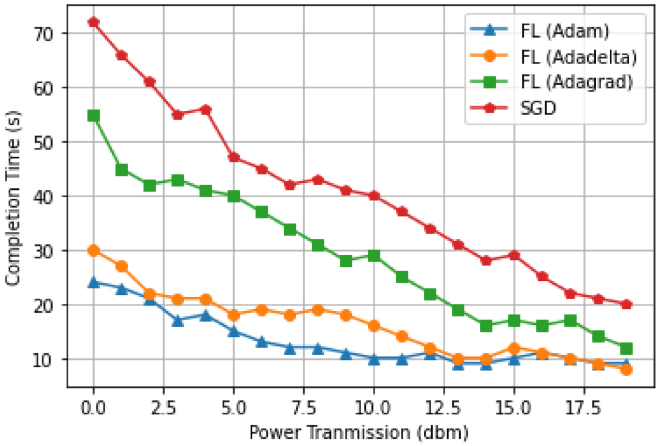


FIGURE 6. Completion Time vs. Power Transmission.

2) TRANSMISSION POWER ADJUSTMENTS

Regarding completion time, Figure 6 demonstrates the correlation between transmission power and the time required for IPS completion, providing insights into power optimization.

In indoor environments, the accuracy of RSSI as a distance estimation metric is affected by obstructions and dynamic environmental conditions, which impact transmission signals. Figure 6 illustrates a power decay curve, where unknown nodes (edge devices) and anchor nodes (APs) are utilized to estimate distances. By comparing different algorithms in terms of completion times and transmission power, this figure offers a cost-effective and efficient solution for IPS. While higher transmission power results in lower completion time, it also leads to increased costs and potentially reduced efficiency. Thus, dynamically adjusting power based on the real-time positioning of edge devices can introduce new ideas and improve system performance.

The importance of efficiency is highlighted, as high transmission power may not be necessary when devices are inactive or out of range. This emphasizes the significance of adjusting transmit power manually or dynamically when the spatial RSSI metric of the AP exceeds a threshold value and meets the coverage criteria.

Typically, RSSI values range from 0 to approximately -100, with 0 indicating optimal signal strength between the AP and the edge device within coverage, while -100 indicates weak or no signal. On the other hand, the transmission power in Figure 6 represents the strength of the AP transmitter. Together with RSSI, transmission power influences the signal strength between the AP and the edge device, with RSSI being proportional to transmission power. Increasing transmission power enhances the AP's signal broadcasting capability, resulting in broader coverage. Improved coverage leads to stronger signals in more areas, reducing instances of high latency. Ultimately, lower latency due to higher power transmission results in reduced localization error and completion time, facilitated by faster data transfer between devices and APs.

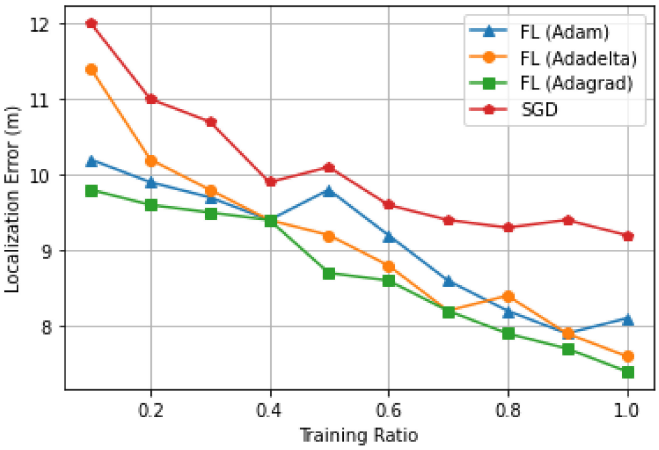


FIGURE 7. Localization Error per Training Ratio.

C. ANALYSIS OF THE POWER MAP POSITIONING

Figure 7 presents the experimental results for localization error with respect to the training ratio adjustment. The observed convergence of the discrepancy indicates improved learning as the training ratio increases. This is consistent with machine learning principles, as utilizing more data for model training in supervised learning leads to better predictions.

The UJIIndoorLoc dataset comprises four subsets: training data, unlabeled fingerprints, validation data, and testing data. To incorporate more data into the experiment, both validation and training data were included in the training ratio. All optimizers were assigned the same batch size, ensuring that every edge device had an equal number of training data samples. This characteristic explains why SGD did not outperform the other optimizers. If the data distribution had been uneven, SGD could have performed better in terms of low localization error. However, in our experiment, the data distribution was balanced.

Figure 6 and Figure 7 can be combined to strike a balance between adjusting the transmit power to the lowest possible setting while maintaining a sufficiently low localization error, as demonstrated in [30]. In Figure 7, the localization error decreases as the training ratio increases. The typical ratio of 80% training data (including validation in this case) and 20% testing data is commonly used for development purposes. The power of FL lies in continuously providing multiple users in the environment with shuffled and random data, effectively acting as a data augmentation technique. Shuffling data and using cross-validation techniques increase variance in experiments with limited data. Each new batch of data presented to the edge device appears as a fresh batch, continuously improving the learning process. This explains why FL algorithms show significant improvement over time. Despite slower initial learning, the algorithms make substantial progress in later training rounds as more training data becomes available.

Similar to a power-varying system, the training-to-testing ratio must be adjusted to an appropriate value to facilitate effective learning and provide sufficient testing data for higher confidence in the system during production. Lastly, establishing constraints is essential for IPS. These constraints can include reducing energy consumption, handling large data volumes, or operating with fewer restrictions to achieve the lowest possible localization error.

VI. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

FL in an indoor environment opens the possibilities in expanding and allowing applications that may lack security or require low latency amongst a network of clients. This work has primarily focused on the effectiveness of a crowd sourced system in an indoor environment. The foreseeable future has and will have this algorithm included in an effort to increase connectivity in the world of growing IoT devices, demand for security, and demand for bandwidth. The results display the similarities that occur whilst comparing a commonly utilized method of training a model and achieving a global minimum (SGD) with several common methods used in a federated manner. We are able to notice that both the time that it took to compute per round as well as the amount of loss that there was per round was similar. Additionally, the results regarding localization error and transmission power encourage the use of FL, as its expansion may allow a system to perform with optimal security, low latency, reduced transmit power, and similar error to that of the traditional approaches within an IPS.

This technique cannot improve independently, therefore the following challenges lie ahead: limited battery and memory, handling non-i.i.d data, and scaling client devices [18]. Though, there are shortcomings and limitations, as our hardware increases in performance, as client participation becomes more predictable, and as improvements are made to equally distributed data to clients in the environment, this algorithm will improve over time. This implementation focuses on latency of the central server, as well as what is lost per iteration according to time.

In regards to the future use cases and implementations of the FL algorithm, it can be extended to several existing project such the one depicted in Figure 2 [12]. Originally, the mobile robot was used in order to traverse the area in which the experiment had taken place in order to gather and conclude location estimates after having collected RSS fingerprints, which were later used to train the model to create these estimates. Additionally, FL has its use case in this experiment which can be further extended. Considering the mobile robot is solely used for the training phase in order to gather and collect fingerprints, it can also have its use in real-time, as well as during the training and testing phases.

Essentially, these mobile APs can best serve as “dynamic” APs, in a system where they are able to dynamically change their locations based on the proximity of the users in the indoor environment. After training, a collection of end users (on their mobile devices) are allowed to travel freely.

Depending on the signal strength read from the mobile device, along with the location estimates learned from training, the mobile robot would act as a dynamic AP and move closer to the proximity of the client(s) to provide better signal strength thus providing better quality of service. As mentioned earlier, the significance of this mobile AP is the alternative to the reduction of power consumption. As opposed to increasing the transmitting power of static APs, the dynamic APs are allowed to move towards the areas in which edge devices may not be covered under the signal strengths of the static APs. This would lead to a continuous system involving no requirements for adjustments in power, but rather a mobile AP(s) that responds during instances involving insufficient coverage.

REFERENCES

[1] M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, "6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 957–975, 2020.

[2] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, "An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10250–10276, Oct. 2020.

[3] Y. Bello, A. R. Hussein, M. Ulema, and J. Koilpillai, "On sustained zero trust conceptualization security for mobile core networks in 5G and beyond," *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 2, pp. 1876–1889, Jun. 2022.

[4] G. D. Samaraweera and J. M. Chang, "Security and privacy implications on database systems in big data era: A survey," *IEEE Trans. Knowl. Data Eng.*, vol. 33, no. 1, pp. 239–258, Jan. 2021.

[5] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4177–4186, Jun. 2020.

[6] P. Mirdita, Z. Khaliq, A. R. Hussein, and X. Wang, "Localization for intelligent systems using unsupervised learning and prediction approaches," *IEEE Can. J. Elect. Comput. Eng.*, vol. 44, no. 4, pp. 443–455, May 2021.

[7] Z. Khaliq, P. Mirdita, A. Refaey, and X. Wang, "Unsupervised manifold alignment for Wifi RSSI indoor localization," in *Proc. IEEE Can. Conf. Elect. Comput. Eng. (CCECE)*, 2020, pp. 1–7.

[8] A. Konstantinidis, G. Chatzimilioudis, D. Zeinalipour-Yazti, P. Mpeis, N. Pelekis, and Y. Theodoridis, "Privacy-preserving indoor localization on smartphones," *IEEE Trans. Knowl. Data Eng.*, vol. 27, no. 11, pp. 3042–3055, Nov. 2015.

[9] U. Saleem, Y. Liu, S. Jangsher, X. Tao, and Y. Li, "Latency minimization for D2D-enabled partial computation offloading in mobile edge computing," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4472–4486, Apr. 2020.

[10] E. Datsika, A. Antonopoulos, N. Zorba, and C. Verikoukis, "Cross-network performance analysis of network coding aided cooperative outband D2D communications," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 3176–3188, May 2017.

[11] N. Zorba and A. I. Perez-Neira, "Robust power allocation schemes for multibeam opportunistic transmission strategies under quality of service constraints," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 6, pp. 1025–1034, Aug. 2008.

[12] J. Biswas and M. Veloso, "WiFi localization and navigation for autonomous indoor mobile robots," in *Proc. 2010 IEEE Int. Conf. Robot. Autom.*, Anchorage, AK, USA, 2010, pp. 4379–4384.

[13] F. Yin et al., "FedLoc: Federated learning framework for data-driven cooperative localization and location data processing," *IEEE Open J. Signal Process.*, vol. 1, no. 1, pp. 187–215, Nov. 2020.

[14] G. Zhang, A. Zhang, P. Zhao, and J. Sun, "Lightweight privacy-preserving scheme in Wi-Fi fingerprint-based indoor localization," *IEEE Syst. J.*, vol. 14, no. 3, pp. 4638–4647, Sep. 2020.

[15] C. Fung, C. J. M. Yoon, and I. Beschastnikh, "Mitigating sybils in federated learning poisoning," 2020, *arXiv:1808.04866*.

[16] L. Melis, C. Song, E. De Cristofaro, and V. Shmatikov, "Exploiting unintended feature leakage in collaborative learning," 2018, *arXiv:1805.04049*.

[17] K. Bonawitz et al., "Towards federated learning at scale: System design," 2019, *arXiv:1902.01046*.

[18] F. Sattler, S. Wiedemann, K.-R. Müller, and W. Samek, "Robust and communication-efficient federated learning from non-i.i.d. data," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 31, no. 9, pp. 3400–3413, Sep. 2020.

[19] K. Wei et al., "Federated learning with differential privacy: Algorithms and performance analysis," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3454–3469, 2020.

[20] S. Zhai, X. Jin, L. Wei, H. Luo, and M. Cao, "Dynamic federated learning for GMEC with time-varying wireless link," *IEEE Access*, vol. 9, pp. 10400–10412, 2021.

[21] J. Xu and H. Wang, "Client selection and bandwidth allocation in wireless federated learning networks: A long-term perspective," *IEEE Trans. Wireless Commun.*, vol. 20, no. 2, pp. 1188–1200, Feb. 2021.

[22] J. Park et al., "Federated learning for indoor localization via model reliability with dropout," *IEEE Commun. Lett.*, vol. 26, no. 7, pp. 1553–1557, Jul. 2022.

[23] Z. Wu, X. Wu, and Y. Long, "Prediction based semi-supervised online personalized federated learning for indoor localization," *IEEE Sensors J.*, vol. 22, no. 11, pp. 10640–10654, Jun. 2022.

[24] B. Gao, F. Yang, N. Cui, K. Xiong, Y. Lu, and Y. Wang, "A federated learning framework for fingerprinting-based indoor localization in multibuilding and multifloor environments," *IEEE Internet Things J.*, vol. 10, no. 3, pp. 2615–2629, Feb. 2023.

[25] P. Zhao, W. Liu, G. Zhang, Z. Li, and L. Wang, "Preserving privacy in WiFi Localization with plausible dummy locations," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 11909–11925, Oct. 2020.

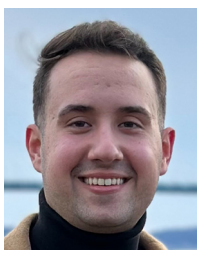
[26] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Proc. Artif. Intell. Statist. PMLR*, 2017, pp. 1273–1282.

[27] M. Chen, N. Shlezinger, H. V. Poor, Y. C. Eldar, and S. Cui, "Communication-efficient federated learning," *Proc. Nat. Acad. Sci. USA*, vol. 118, no. 17, 2021, Art. no. e2024789118.

[28] T. Sun, D. Li, and B. Wang, "Decentralized federated averaging," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 45, no. 4, pp. 4289–4301, Apr. 2023.

[29] S. Subedi, H.-S. Gang, N. Y. Ko, S.-S. Hwang, and J.-Y. Pyun, "Improving indoor fingerprinting positioning with affinity propagation clustering and weighted centroid fingerprint," *IEEE Access*, vol. 7, pp. 31738–31750, 2019.

[30] W. Zang and Y. Li, "Gait-cycle-driven transmission power control scheme for a wireless body area network," *IEEE J. Biomed. Health Inform.*, vol. 22, no. 3, pp. 697–706, May 2018.



PAUL MIRDITA (Student Member, IEEE) received the B.Sc. and M.Sc. degrees in electrical engineering from Manhattan College, Riverdale, NY, USA, in 2019 and 2021, respectively. His research interests include machine learning for indoor localization, data privacy, and electromagnetic.

YAHUZA BELLO received the B.Sc. degree in electronics and communications engineering from the Arab Academy for Science, Technology and Maritime Transport, Egypt, in 2014, and the M.Sc. degree in computer engineering from Manhattan College, Riverdale, NY, USA, in 2020. He is currently pursuing the Ph.D. degree in computer engineering with the University of Guelph, Guelph, ON, Canada. His research interests encompass a wide range of topics, including reinforcement learning, stochastic games, network function virtualization, optimization, and cloud and edge computing security.

AHMED REFAEY (Senior Member, IEEE) received the B.Sc. and M.Sc. degrees from Alexandria University, Egypt, in 2003 and 2005, respectively, and the Ph.D. degree from Laval University, Québec City, QC, Canada, in 2011. He currently serves as an Assistant Professor with the University of Guelph and an Adjunct Research Professor with Western University. He has held various positions throughout his career, including an Associate Professor with Manhattan College from 2016 to 2021, a Senior Embedded Systems Architect with Mircom Technologies Ltd., from 2014 to 2016, a Postdoctoral Fellow with the ECE Department, Western University from 2012 to 2013, and a Professional Researcher with the LRTS Laboratory, Laval University, specializing in wireless communications hardware implementations from 2007 to 2011. Before joining Laval University, he worked as a System/Core Network Engineer, leading teams in the telecom industry for Fujitsu, Vodafone, and Alcatel-Lucent. He has authored and coauthored over 82 technical papers, holds one granted patent, and has filed three patent applications related to his research endeavors.

AYMAN RADWAN (Senior Member, IEEE) received the M.A.Sc. degree in systems and computer engineering with a focus on DSP from Carleton University, Ottawa, ON, Canada, in 2003, and the Ph.D. degree in electrical and computer engineering, specializing in wireless networking, from Queen University, Kingston, ON, Canada, in 2009. He is currently an Assistant Professor with the University of Aveiro and serves as a Senior Researcher with the Institute de Telecomunicações, Aveiro, Portugal. He actively participates in EU projects and has served as the coordinator for multiple EU joint research projects with international partners. He is currently leading the coordination of the EU Project CELTIC-NEXT SAFE-HOME, emphasizing eHealth and energy-efficient fog-cloud networking. He has been involved in successful funding proposals, securing over two million dollars for his institute. He has an extensive publication record, with more than 150 highly cited peer-reviewed articles. His research interests revolve around network architectures, specifically 5G and beyond, fog-cloud networking, IoT, and eHealth. Additionally, he holds the position of Secretary of the IEEE eHealth Technical Committee.