Enhanced Reconfigurable Intelligent Surface Assisted mmWave Communication: A Federated Learning Approach

Lixin Li[1,*], Donghui Ma[1], Huan Ren[1], Dawei Wang[1], Xiao Tang[1], Wei Liang[1], Tong Bai[2]

[1] School of Electronics and Information, Northwestern Polytechnical University, Xi'an 710129, China
[2] School of Electronic Engineering and Computer Science, Queen Mary University of London, London E1 4NS, U.K.
* The corresponding author, email: lilixin@nwpu.edu.cn

Abstract: Reconfigurable intelligent surface (RIS) has been proposed as a potential solution to improve the coverage and spectrum efficiency for future wireless communication. However, the privacy of users' data is often ignored in previous works, such as the user's location information during channel estimation. In this paper, we propose a privacy-preserving design paradigm combining federated learning (FL) with RIS in the mmWave communication system. Based on FL, the local models are trained and encrypted using the private data managed on each local device. Following this, a global model is generated by aggregating them at the central server. The optimal model is trained for establishing the mapping function between channel state information (CSI) and RIS' configuration matrix in order to maximize the achievable rate of the received signal. Simulation results demonstrate that the proposed scheme can effectively approach to the theoretical value generated by centralized machine learning (ML), while protecting user' privacy.

Keywords: reconfigurable intelligent surface; privacy; federated learning; achievable rate

I. INTRODUCTION

With the advance of the 5G [1] and Internet of Things technology, massive terminal equipment [2] and limited spectrum resources give rise to many challenges to high-speed communication. To overcome these challenges, the technique of millimeter-wave (mmWave) communication has been proposed to improve the system throughput by expanding the available frequency band (30-300GHz). In order to achieve stable and reliable mmWave wireless communication, diverse new technologies have been conceived. For example, ultra-dense network (UDN) has been proposed to establish stronger communication links, and achieve better spatial reuse by deploying relatively dense base station (BS) or access point (AP) in hotspots [3]. However, it also means higher hardware cost and power consumption, meanwhile, the interference between users are more serious, including intra-cell interference and inter-cell interference, which reduce the energy efficiency (EE). Similarly, massive multiple-input multiple-output (MIMO) has been proposed to improve EE and spectral

Received: Feb. 27, 2020
Revised: Jun. 19, 2020
Editor: Chuan Huang

In this paper, we propose a privacy-preserving design paradigm combining federated learning (FL) with RIS in the mmWave communication system.

efficiency (SE) by deploying large-scale antenna array [4]. However, the complex signal processing algorithms and a large number of radio frequency (RF) chains are essential for massive MIMO which greatly increases the hardware cost.

In addition, the transmission of electromagnetic wave (EM) is largely uncontrollable due to the scattering and diffraction of EM in complex environments. Hence, the transmission of EM is also largely uncontrollable. To solve the above issues, a novel technology has attracted attention recently: reconfigurable intelligent surface (RIS). RIS is a general term for a class of special surfaces that can change the propagation characteristics of incident EMs, including RIS based on reflective antennas array and RIS based on meta-surface [5]. RIS consists of a large number of passive units, each of which can adjust the propagation of EMs by changing the phase, amplitude or frequency of incident waves [6], thereby forming a corresponding "smart electromagnetic environment" [7]. Based on this excellent characteristic, RIS has shown its huge potential to solve wireless communication problems. For example, establishing virtual line-of-sight (LOS) link to expand the coverage of multi-user millimeter-wave communication [8], increasing the channel capacity [9] [10] [11] and communication rate [12] [13] [14] of mmWave communication, improving wireless communication EE and SE [15] [16] [17] [18]. Besides, RIS can also be deployed to ensure the physical layer security of wireless communication [19] [20].

As a benefit of the promising performance of machine learning (ML) in solving wireless communication problems, there are several cases where people combine RIS and ML [12] [14] [21] [22]. For example, in view of the energy consumption and hardware cost brought by the large-scale RF chains in the traditional channel estimation, the authors in [14] proposed a method based on deep learning (DL) to establish the relationship between limited CSI and the configuration of the RIS so as to optimize the RIS configuration, and thus, the optimal communication rate can be achieved. However, in the previous work about the channel estimation of RIS-assisted wireless communication system, the challenge of user's private data protection still remains.

Against this background, in this paper, we conceive a RIS-assisted millimeter-wave communication scheme based on the privacy-protected distributed ML framework, i.e. federated learning (FL), which protects user's private data while realizing high-speed wireless communication.

1.1 Related work and motivation

A lot of research has been done on CSI acquisition for RIS-assisted wireless communications. According to whether the RF receiving chain is deployed on the elements of RIS, it is mainly divided into two categories [5].

The first type is to send pilot signals from BS and deploy several RF receiving chains on the RIS elements to perform channel estimation. In [23], the authors assume that the AP has perfect CSI, which is, by deploying an RF receiving chain on each element of RIS, using the pilot signal transmitted by AP for uplink training, and utilizing the channel reciprocity to obtain downlink CSI. However, this will bring a series of inevitable problems: unaffordable power consumption and hardware complexity. In [24], a channel estimation protocol based on minimum mean square error (MMSE) is proposed by utilizing time division duplex (TDD) protocol and channel reciprocity. The entire channel estimation time is divided into multiple sub-stages, and each stage performs channel estimation for only one RIS element. Finally, the results of all sub-stages are synthesized, and a complete channel estimation result is obtained by using the MMSE method.

The second type is not to perform channel estimation explicitly, but to optimize the configuration of RIS directly based on the feedback of receiver [25]. However, the size of the predefined codebook which containing the RIS configuration matrix is proportional to the number of RIS elements. Therefore, for those

RISs with large-scale elements, training takes a long time and the training burden is correspondingly more serious [14], which makes dynamic reconfiguration of RIS very difficult.

In order to solve the above problems, the authors in [14] proposed a method based on DL, which matches the CSI and the optimal RIS configuration based on the limited CSI sampled by the sparse activation elements. However, during the channel sampling process, the defined "environment descriptor" contains not only surrounding environment information, but also location information of user equipment (UE). Similarly, the fingerprint defined in [12] also corresponds to the location of the device. The location information of the device is also a kind of private data to a certain extent, which needs to be protected especially during wireless communication

In recent years, a distributed ML method: FL, has been proposed [26]. Our prior work in [27] has studied the distributed rate optimization problem using optimal beam reflection based on federated learning (OBR-FL). Unlike traditional machine learning, which processes data centrally, the physical framework of FL includes several clients and a central server. And the data for training is distributed to each client which means managed and processed locally. The training process of FL is mainly divided into three parts:

1. Each client that participating in FL trains a local model based on their locally stored dataset
2. Upload the local model to the central server for aggregation to generate a global model
3. Download global model to each client for the next training process.

Due to the necessity of privacy protection in wireless communication and the outstanding privacy protection characteristics of FL, the combination of FL and wireless communication has gradually emerged. For example, FL was applied to realize ultra-reliable low-latency Vehicle-to-Vehicle (V2V) communications in [28]. By establishing a FL framework, the roadside unit (RSU) is set up as the central server, and the vehicular users (VUEs) are clients. Queue State Information (QSI) is the training data, which only processed locally.

In this paper, we proposed two FL-based mmWave wireless communication scenarios: RIS assisted outdoor mmWave communication and mmWave communication within the IoT network with the assistance of multiple RIS. For the RIS assisted outdoor mmWave communication, we regard the controller of RIS as the central server, such as FPGA or single computer, which responses for the RIS control and local model aggregation at the same time, and the user equipment participating in communication as the client. The dataset held by the client consists of a series of sampled data points within its range of activity, each of which consists of the CSI corresponding to its location and the optimal configuration of RIS. By utilizing FL, an optimal global model is trained to maximize the achievable rate of user in the communication area. In the second scenario, an AP connected to multiple RISs is regarded as the central server, where each RIS as client, and the data set held by each RIS is composed of a series of optimal RIS configurations and the sampled IoT devices location information pairs. Through the FL of all RISs, the optimal model is trained to achieve the optimal sum rate of wireless communication in IoT network.

1.2 Contributions and outcomes

Compared with the existing work, this paper introduces FL into RIS assisted mmWave communication system. By utilizing FL, mapping the function between sparsely sampled CSI and optimal RIS configuration to realize high speed wireless communication.

In this paper, we propose a privacy-preserving design paradigm in ML enhanced wireless communication through introducing FL in RIS-assisted wireless communication. Meanwhile, we design two novel communication models, including single RIS assisted outdoor communication and multiple RIS-assisted IoT network communication, and the LOS and NLOS are jointly considered. In addition, the FL method is applied to RIS assisted communications to realize the achievable rate maximization while considering the privacy issue in the communication networks. Specifically, different FL algorithms are designed for UEs and RISs with the different scenes mentioned above. And the simulation results demonstrate that the proposed scheme can effectively approach to the theoretical value and reach to higher than 95% of that generated by centralized ML while guarantying the security of users' private data.

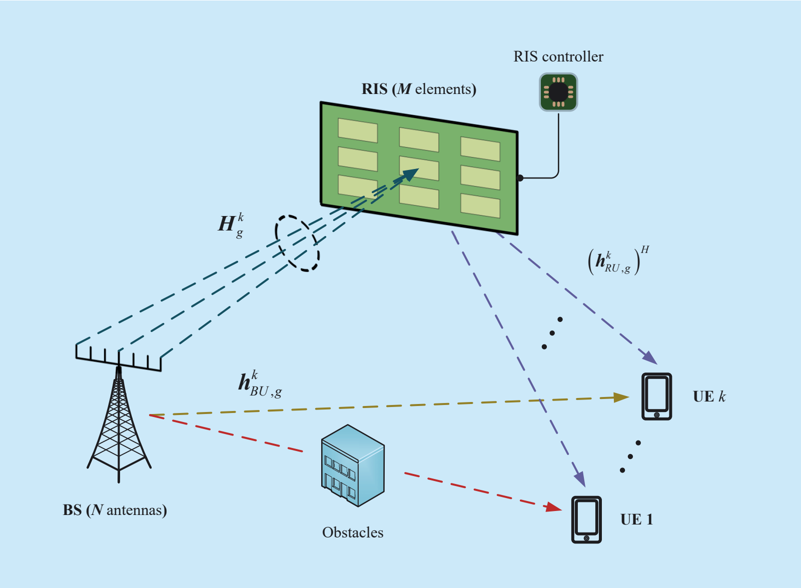


Fig. 1. *Model of RIS assisted outdoor communication.*

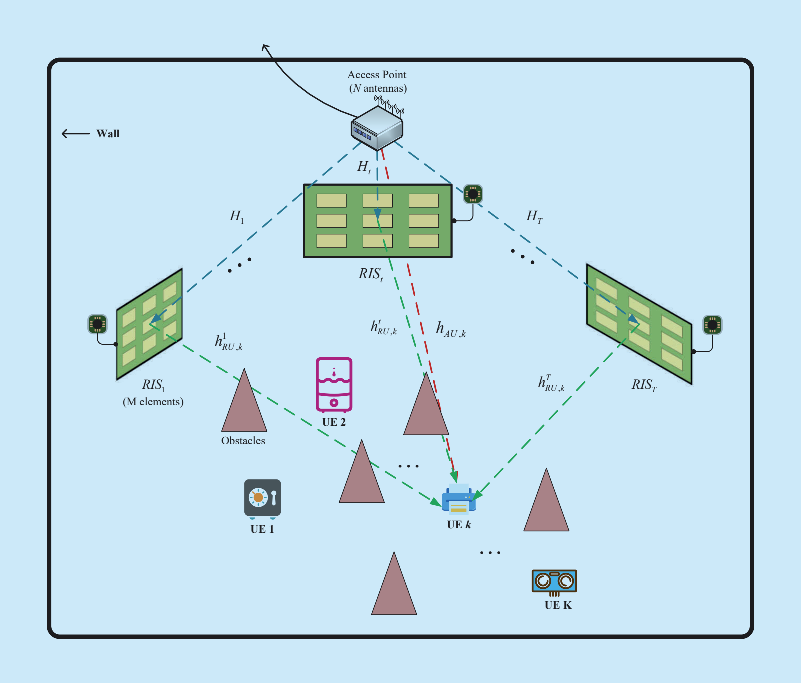


Fig. 2. *Model of RIS assisted IoT network communication.*

The rest of this paper is organized as follows. Section II describes the system models and problem formulation. In Section III, we introduce the design of FL-based RIS assisted communication scheme in different scenarios. The simulation results are in Section IV. Section V is the conclusion.

Notation: In this paper, scalar is represented by italics, matrix and vector are represented by bold-face letters. $|\boldsymbol{B}|$ and $\boldsymbol{B}^H$ represent the determinant and conjugate transpose of the matrix, respectively, and $\boldsymbol{B}_k$ represents the kth column vector of the matrix.

II. SYSTEM MODEL AND PROBLEM FORMULATION

2.1 System model

In this paper, a privacy-preserving design paradigm is introduced in the ML-enhanced wireless communication, as shown in Figure 1 and Figure 2. We comprehensively design two RIS-assisted mmWave communication scenarios, namely single RIS- assisted outdoor communication and multiple RIS-assisted IoT network communication.

2.1.1 RIS assisted outdoor mmWave communication

Figure 1 illustrates an outdoor communication system assisted by a single RIS in mmWave band that contains a BS and k UEs, and a controller is connected to RIS to configure it. We assume that the number of antennas in the BS and the number of RIS elements are N and M, respectively, and each UE is equipped with a single antenna. At the same time, we consider the direct LOS link and the virtual LOS, where the latter is established through RIS, which is used to achieve effective and stable communication when the direct LOS between the BS and UE is blocked by obstacles. Meanwhile, we refer to the structure of RIS with sparse sensors proposed in [14], a tiny fraction of RIS elements $\overline{M} \ll M$, which are called "active elements" with extra ability about perceive CSI among the system. It means that they can switch the working mode between reflecting incident signals normally and channel sensing, and these active elements are randomly distributed among RIS elements.

We assume all the channels among BS, RIS and UEs are based on Orthogonal Frequency Division Multiplexing (OFDM) modulation with G subcarriers. The uplink channel from BS and UE to RIS at gth subcarrier of kth UE are defined as $\boldsymbol{H}_g^k \in \mathbb{C}^{M\times N}$ and $\boldsymbol{h}_{RU,g}^k \in \mathbb{C}^{M\times 1}$, where $g = 1,2,...,G, k = 1,2,...,K$. Accordingly, the downlink channel from RIS to UE can be denoted as $\left(\boldsymbol{h}_{RU,g}^k\right)^H \in \mathbb{C}^{1\times M}$, and $\boldsymbol{h}_{BU,g}^k \in \mathbb{C}^{1\times N}$ represents the direct LOS between BS and UE. $\boldsymbol{x}_g \in \mathbb{C}^{N\times 1}$ is the transmitted signal at gth subcarrier of BS. Based on the above prerequisites, the received signal at gth subcarrier of kth UE can be expressed as:

$$y_g^k = \left[\left(\boldsymbol{h}_{RU,g}^k\right)^H \boldsymbol{\Phi}_g^k \boldsymbol{H}_g^k + \boldsymbol{h}_{BU,g}^k\right]\boldsymbol{x}_g + \omega_g^k, \quad (1)$$

where

$$\boldsymbol{x}_g = \boldsymbol{V}\boldsymbol{s}_g, \quad (2)$$

$\boldsymbol{V} \in \mathbb{C}^{N\times K}$ represents the digital beamforming matrix at BS, $\boldsymbol{s}_g \in \mathbb{C}^{K\times 1}$ is the intended signal of K UEs at gth subcarrier and $\boldsymbol{\Phi}_g^k \in \mathbb{C}^{M\times M}$ is the configuration matrix of RIS at gth subcarrier of kth UE. For simplicity, we assume that all subcarriers under the same UE are implemented same RIS configuration matrix, which means $\boldsymbol{\Phi}_1^k = ... = \boldsymbol{\Phi}_g^k = \boldsymbol{\Phi}_G^k = \boldsymbol{\Phi}^k$, where $\boldsymbol{\Phi}^k = diag[\varphi_1, \varphi_2, ..., \varphi_M]$. In this paper, the reflecting elements of RIS can only change the phase of incident signal, but not amplitude. Specifically, $\varphi_m = e^{j\theta_m}, \theta_m \in [0, 2\pi)$ for any $m = 1,2,...,M$. The normalized additive white Gaussian noise (AWGN) at gth subcarrier of kth UE can be denoted as $\omega_g^k \sim \mathcal{CN}(0, \sigma_{k,g}^2)$.

2.1.2 RIS assisted indoor IoT network communication

With the advent of industry 4.0 [29], IoT is constantly developing as a critical part of it. The deployment of a large number of edge intelligent devices brings huge challenges to the realization of stable and efficient millimeter communications. Meanwhile, IoT devices are usually located at key nodes in the system for control functions, which makes them unable to rely entirely on unstable remote control, and some computing tasks need to be completed locally [30]. Due to the characteristics of low power consumption, poor computing resources and slow transmission rate of edge devices, the traditional centralized machine learning is hard to deploy because of its demand for computing resources and communication bandwidth. For these reasons, the deployment of FL to wireless networks has recently emerged [31]. Therefore, this paper proposes a RIS assisted IoT network communication scheme based on FL.

The scenario of intra-IoT network communication assisted by multiple RISs is shown in Figure 2. Considering the massive indoor environment edge IoT devices, such as intelligent furniture, sensors, printer, etc. Under the complex distribution of obstacles, RIS is used to solve the problem of weak link caused by the particularity of indoor EM environment (e.g., the high penetrate loss produced by surrounding walls or buildings [32]) to improve the quality of indoor wireless communication.

As described in the figure, an indoor IoT wireless communication network is constructed with an AP and K UEs assisted by T RISs and several randomly distributed obstacles, where the antennas number of AP is N, number of RIS elements is M, all UEs equipped with single antenna. The downlink channel from AP to RIS t and RIS t to UE k is $H_t \in \mathbb{C}^{M\times N}$ and $\boldsymbol{h}_{RU,k}^t \in \mathbb{C}^{1\times M}$, respectively, where $t = 1,2,...,T, k = 1,2,...,K$. And the direct LOS link between AP and UE k is $\boldsymbol{h}_{AU,k} \in \mathbb{C}^{1\times N}$. According to these assumptions, the received signal of UE k from RIS t can be expressed as:

$$y_k^t = \left(\boldsymbol{h}_{RU,k}^t \boldsymbol{\Phi}_t \boldsymbol{H}_t + \boldsymbol{h}_{AU,k}\right)\boldsymbol{x} + \omega_k^t, \tag{3}$$

where $\boldsymbol{\Phi}_t \in \mathbb{C}^{M\times M}$ represents the configuration matrix of RIS t, $\boldsymbol{x} \in \mathbb{C}^{N\times 1}$ is the transmitted signal from AP. Same as previous assumptions, $\omega_k^t \sim \mathcal{CN}(0,\sigma_k^2)$ is the normalized AWGN generated by UE k in receiving the signal from RIS t. By superposing the signals of UE k from all RIS, the superimposed signal can be written as:

$$y_k = \sum_{t=1}^{T} y_k^t. \tag{4}$$

2.2 Channel model

In this paper, we consider two different scenarios about RIS assisted mmWave communications. However, because of the distinction between indoor and outdoor environment, such as the large-scale fading and small-scale fading, the modeling of wireless channels is also different.

The wideband geometric channel model is adopted to the channels $\boldsymbol{H}_g^k$, $\boldsymbol{h}_{RU,g}^k$ and $\boldsymbol{h}_{BU,g}^k$ within the RIS assisted outdoor communication. Considering the multipath effect of the wireless channel, we assume the path number of each channel is L. Taking $\boldsymbol{h}_{RU,g}^k$ for example, it can be expressed as:

$$\boldsymbol{h}_{RU,g}^k = \sqrt{\frac{M}{\rho}} \sum_{d=0}^{D-1}\sum_{l=1}^{L} \beta_l p(dE-\eta_l)\boldsymbol{a}(\theta_l,\phi_l)e^{-j\frac{2\pi g}{G}d}, \tag{5}$$

where ρ represents the path loss between BS and RIS, η_l and $\boldsymbol{a}(\theta_l,\phi_l) \in \mathbb{C}^{M\times 1}$ are the time delay of lth path and the response vector of RIS with the angle of arrival (AoA) $\theta_l, \phi_l \in (0, 2\pi]$. E and D are the sampling time and cycle prefix length, respectively. p describes the pulse shaping function.

As for the indoor environment of RIS assisted IoT network communications, we adopt the similar assumption in [12], that is, the large-scale fading does not change with the frequency, and the small-scale fading follows the complex Gaussian distribution

2.3 Problem formulation

2.3.1 RIS assisted outdoor mmWave communication

All in all, this paper mainly utilizes RIS to enhance the achievable rate performance in different communication scenarios. Specifically, for RIS-assisted outdoor millimeter-wave communication, we use a single RIS to assist users in a certain area for millimeter-wave communication. According to Figure 1 and the aforementioned formulas, the signal to interference plus noise ratio (SINR) of the gth subcarrier signal received by the kth UE can be written as:

$$\gamma_g^k = \frac{\left|\left[\left(\boldsymbol{h}_{RU,g}^k\right)^H \boldsymbol{\Phi}^k \boldsymbol{H}_g^k + \boldsymbol{h}_{BU,g}^k\right]\boldsymbol{V}_k\right|^2}{\sum_{j\neq k}^{K}\left|\left[(\boldsymbol{h}_{RU,g}^k)^H \boldsymbol{\Phi}^k \boldsymbol{H}_g^k + \boldsymbol{h}_{BU,g}^k\right]\boldsymbol{V}_j\right|^2 + \sigma_{k,g}^2}. \tag{6}$$

Then, the corresponding signal rate R_g^k is represented as:

$$R_g^k = \log_2(1+\gamma_g^k), \tag{7}$$

therefore, the average achievable rate of UE k can be expressed as:

$$R^k = \frac{1}{G}\sum_{g=1}^{G} R_g^k. \tag{8}$$

In this paper, the Deep Neural Network (DNN) trained by distributed learning based on FL, which is used to map the function between UEs channel $\boldsymbol{H}_g^k$, $\boldsymbol{h}_{RU,g}^k$ and optimal RIS configuration matrix $\widehat{\boldsymbol{\Phi}}^k$, which can be expressed as:

$$\widehat{\boldsymbol{\Phi}}^k = \arg\max_{\boldsymbol{\Phi}^k \in \boldsymbol{O}} R^k, \tag{9}$$

where $\boldsymbol{O}$ is a predefined set which contains a series of RIS configuration matrix $\boldsymbol{\Phi}^k$ randomly generated by Discrete Fourier transform (DFT) [14]. The optimal RIS configuration matrix corresponding to the CSI of UE can be obtained by exhaustive searching through $\boldsymbol{O}$. Regarding the CSI acquisition of $\boldsymbol{H}_g^k$, $\boldsymbol{h}_{RU,g}^k$, we utilize the active elements of RIS mentioned in 2.1.1.

2.3.2 RIS assisted IoT network mmWave communication

For the RIS assisted IoT network communications, according to Figure 2 and corresponding system model assumptions, the rate of received signal at UE k from RIS t can be written as:

$$R_t^k = \log_2(1+\gamma_t^k), \tag{10}$$

where the SINR γ_t^k is defined as:

$$\gamma_t^k = \frac{\left|\left[\boldsymbol{h}_{RU,k}^t \boldsymbol{\Phi}_t \boldsymbol{H}_t + \boldsymbol{h}_{AU,k}\right]\boldsymbol{V}_k\right|^2}{\sum_{j\neq k}^K \left|\left[\boldsymbol{h}_{RU,k}^t \boldsymbol{\Phi}_t \boldsymbol{H}_t + \boldsymbol{h}_{AU,k}\right]\boldsymbol{V}_j\right|^2 + \sigma_k^2}. \tag{11}$$

By superimposing signals from all RIS $t, t=1,2,\ldots,T$, the combined signal at UE k can be written as:

$$R^k = \sum_{t=1}^T R_t^k. \tag{12}$$

This paper proposes an algorithm based on FL to realize the RIS optimization in parallel. Concretely, to establish the mapping relationship between channels of UE and multiple RISs parallelly so as to maximize the R^k.

III. RIS Assisted Communication Scheme Based on Federated Learning

As a branch of distributed machine learning, FL has the advantages of strong private protection and distributed computing, and so on. According to the analysis in the previous sections, the goal of this paper is to establish the mapping function between the user's CSI and the optimal configuration of RIS by applying FL to improve the achievable communication rate.

According to different communication scenarios, the FL algorithm framework for outdoor millimeter wave communications and IoT network communications are proposed. Specifically, the clients during the FL process are UEs and RISs, respectively. The basic framework of FL is shown in Figure 3.

Each client $U^k, \forall k=1,2,\ldots,K$ involved in the FL has its own unique dataset $Q^k, \forall k=1,2,\ldots,K$, which means that other devices cannot access it. In other words, it can only be managed and processed locally. The training process of FL is mainly separated into three parts:

- Training the local dataset $Q^k, k=1,2,\ldots,K$ on each client $U^k, k=1,2,\ldots,K$ to obtain local models $\boldsymbol{W}_i^k, i=1,2,\ldots,I$, where i represents the ith training round, and I is the total training times.
- To upload all local models $\boldsymbol{W}_i^k, k=1,2,\ldots,K$ to the central server via the uplink and the global model $\boldsymbol{W}_i$ for ith training is obtained by aggregating all local models in a certain way.
- The global model $\boldsymbol{W}_i$ is downloaded to all clients via the downlink as the initial model for next training round.

For the sake of simplicity, we assume that the wireless links during the process of FL is, that is, there is no data errors or communication interruptions during the model parameters transmission. The global model aggregation method in this paper is as follows:

$$\boldsymbol{W}_{i+1}^k = \frac{1}{K}\sum_{k=1}^K \boldsymbol{W}_i^k. \tag{13}$$

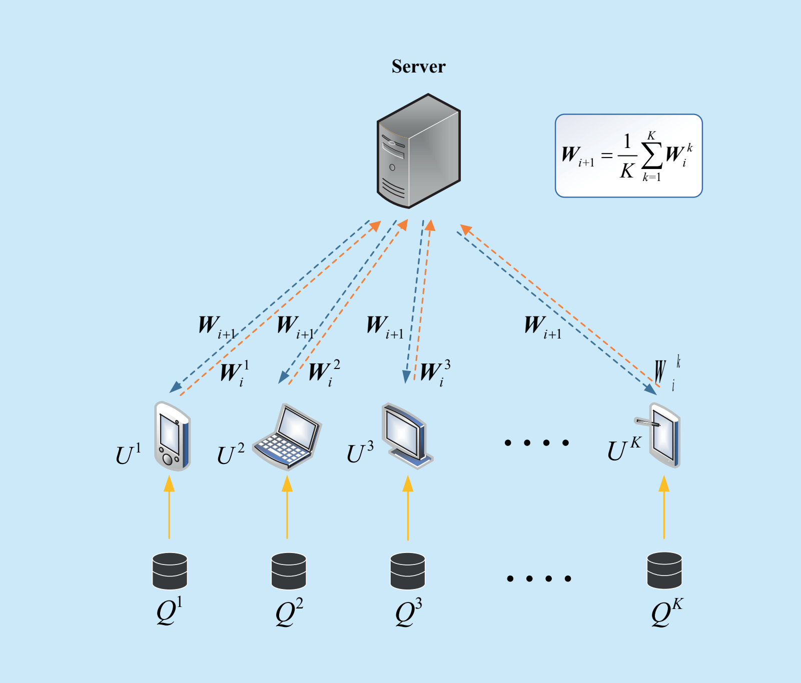


Fig. 3. *The framework of federated learning among several different devices.*

3.1 Algorithm framework of FL for outdoor mmWave communication

The whole FL algorithm framework is divided into two parts: training phase and validation phase.

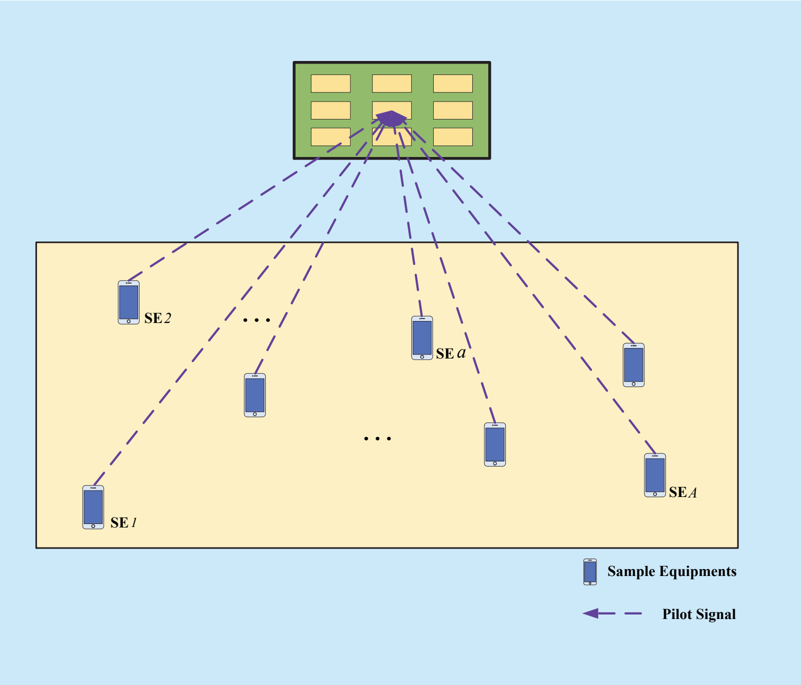


Fig. 4. *The process of channel estimation by pilot signals emitted from sample equipment to RIS.*

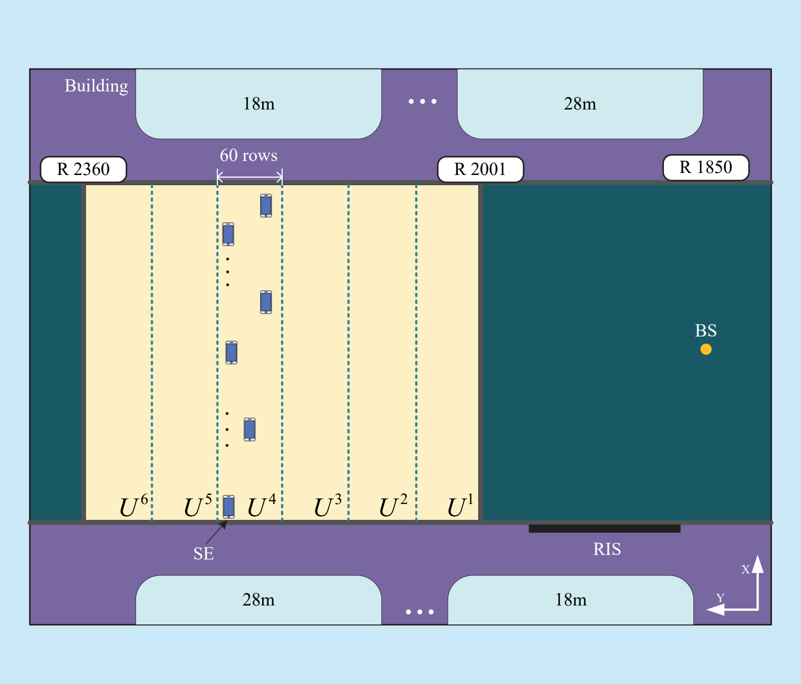


Fig. 5. *The experimental scenario of FL algorithm for RIS assisted mmWave communications.*

Training phase: Since the basic of FL is still DL, datasets are essential for the training process, so the first task is to build the local datasets $Q^k, k=1,2,...,K$, and all of these local datasets have the same scale. Dataset is composed of a series of data points, since the purpose of this paper is to reveal the relationship between CSI of UE and the optimal RIS configuration which means the optimal achievable communication rate. Therefore, the acquisition of sampled CSI is indispensable by utilizing the active elements of RIS. Since RIS itself does not have the ability to emit signal, two pilot signals are transmitted from BS and UE to RIS and do channel estimation, according to channel reciprocity, the sampled CSI from BS to RIS and RIS to UE can be obtained, denoted as $(\tilde{\boldsymbol{h}}_{RU,g}^{k,a})^H$ and $\widetilde{\boldsymbol{H}}_g^{k,a}$ respectively. However, the CSI between RIS and UE implies the private information of user, so we deploy a set of sample equipment (SE) for pilot signal emitting within the user's range of activity which similar to RP in [12] and the size of this set is A. As shown in Figure 4, the region of UE k is drawn in pale yellow and A SEs are randomly distributed, so the sampled channel of subcarrier g of UE k at SE a can be expressed as:

$$\tilde{\boldsymbol{h}}_g^{k,a} = (\tilde{\boldsymbol{h}}_{RU,g}^{k,a})^H \widetilde{\boldsymbol{H}}_g^{k,a}, \tag{14}$$

where $(\tilde{\boldsymbol{h}}_{RU,g}^{k,a})^H$ and $\widetilde{\boldsymbol{H}}_g^{k,a}$ can be further written as:

$$(\tilde{\boldsymbol{h}}_{RU,g}^{k,a})^H = (\bar{\boldsymbol{h}}_{RU,g}^{k,a})^H + \boldsymbol{\omega}_{g,RU}^k, \tag{15}$$

$$\widetilde{\boldsymbol{H}}_g^{k,a} = \overline{\boldsymbol{H}}_g^{k,a} + \boldsymbol{\omega}_{g,BR}^k, \tag{16}$$

$(\bar{\boldsymbol{h}}_{RU,g}^{k,a})^H$ and $\overline{\boldsymbol{H}}_g^{k,a}$ are the original sampled channel vectors, $\boldsymbol{\omega}_{g,RU}^k \in \mathbb{C}^{1\times M}$ and $\boldsymbol{\omega}_{g,BR}^k \in \mathbb{C}^{M\times N}$ represent their received noise vectors respectively, the type of noise is same as defined in section II. Then, we build the vector $\tilde{\boldsymbol{h}}^{k,a}$=vec($[\tilde{\boldsymbol{h}}_1^{k,a}, \tilde{\boldsymbol{h}}_2^{k,a}, ..., \tilde{\boldsymbol{h}}_G^{k,a}]$) which contains CSI of all subcarriers. After the sampled channel estimation, the next step is label matching, the label is a vector contains a series of achievable rate by traversing the predefined RIS configuration set $\boldsymbol{O}$ according to formula (8), denoted as $\widehat{\boldsymbol{R}}^{k,a}=[R_1^{k,a},R_2^{k,a},...,R_{|\boldsymbol{O}|}^{k,a}]$. Then, the data point $(\widetilde{\boldsymbol{h}}^{k,a},\boldsymbol{R}^{k,a})$ finish construction and added into local dataset Q^k of UE k. After all the work of CSI acquisition and label matching, the full version of local dataset $Q^k \triangleq [(\widetilde{\boldsymbol{h}}^{k,1},\widehat{\boldsymbol{R}}^{k,1}),...,(\widetilde{\boldsymbol{h}}^{k,a},\widehat{\boldsymbol{R}}^{k,a}),...,(\widetilde{\boldsymbol{h}}^{k,A},\widehat{\boldsymbol{R}}^{k,A})]$ can be constructed.

In this paper, we adopt Multi-Layer-Perceptron (MLP) as the basic DNN architecture for FL which include Z full-connected layers, Rectified Linear Units (ReLU) and Root-Mean-Squared-Error (RMSE) are selected as active function and loss function, respectively. Meanwhile, we employ Stochastic Gradient Descent (SGD) as optimizer to implement gradient descent. The loss function can be expressed as:

$$\boldsymbol{Loss}=RMSE(\overline{\boldsymbol{R}}^{k,a},\widehat{\boldsymbol{R}}^{k,a}), \tag{17}$$

where $\overline{\boldsymbol{R}}^{k,a}$ is predicted rate vector.

Validation phase: All the local dataset of UEs is divided into training set and validation set in proportion to 80% and 20%. The performance of trained model is verified by validation set. Specifically, the process of validation is to compare the consistency of predicted rate vector $\overline{\boldsymbol{R}}^{k,a}$ and the actual rate vector $\widehat{\boldsymbol{R}}^{k,a}$.

3.2 Algorithm framework of FL for IoT network communication

Different with outdoor communication, for indoor IoT communication, the objects participating in FL are no longer UEs but RISs. The main reason is that the target of optimization has changed. In this scenario, the goal of this subsection is to optimize multiple RISs in parallel under the distributed training and encrypted model aggregation, also to save the computing resources compared with individual training.

Meanwhile, the composition of the local dataset is also different. For the purpose of optimizing RIS, the dataset should consist of the of each UE and the corresponding optimal RIS configuration. The local dataset Q_t can be written as:

$$Q_t \triangleq \left\{(\widetilde{\boldsymbol{h}}_t^1,\widehat{\boldsymbol{\Phi}}_t^1),(\widetilde{\boldsymbol{h}}_t^2,\widehat{\boldsymbol{\Phi}}_t^2),...,(\widetilde{\boldsymbol{h}}_t^K,\widehat{\boldsymbol{\Phi}}_t^K)\right\}, \tag{18}$$

where $\widetilde{\boldsymbol{h}}_t^k$ is the sampled channel vector of UE k constructed by A SEs which can be further written as:

$$\widetilde{\boldsymbol{h}}_t^k=\mathrm{vec}([\widetilde{\boldsymbol{h}}_t^{k,1},\widetilde{\boldsymbol{h}}_t^{k,2},...,\widetilde{\boldsymbol{h}}_t^{k,A}]), \tag{19}$$

$\widetilde{\boldsymbol{h}}_t^{k,a}\in\mathbb{C}^{1\times N}$ is the sampled channel at UE k by SE a. Specifically, is can be decomposed to two parts, where

$$\widetilde{\boldsymbol{h}}_t^{k,a}=\widetilde{\boldsymbol{h}}_{RU,t}^{k,a}\widetilde{\boldsymbol{H}}_t, \tag{20}$$

$\widetilde{\boldsymbol{h}}_{RU,t}^{k,a}$ and $\widetilde{\boldsymbol{H}}_t$ are the sampled channel added with random noise vectors from AP to RIS k and RIS to UE k by SE a, respectively. $\widehat{\boldsymbol{\Phi}}_t^k$ is the optimal RIS configuration matrix selected through formula (9).

After the construction of local datasets $Q_t, t=1,2,...,T$, the next step is local training of FL, which is completed on RIS controller mentioned before according to the local dataset. A series of local models $\boldsymbol{W}_i^t, t=1,2,...,T$ are trained by each RIS for ith training. Then, all of these local models are upload to central server through wireless uplink for aggregation to generate a global model $\boldsymbol{W}_i$ for round i, and the equipment for aggregation is AP. After this, all RISs download this global model as the initial model for next training round.

Specifically, as mentioned above, the local model training process of each IRS is executed by the IRS controller. And the stability assumption of wireless link within the FL process is consistent with the previous content. And the basic structure of chosen DNN for FL is also unchanged, only the neurons number of input and output layer changes, corresponding with the dimension of dataset, are A and M, respectively.

The loss function can be expressed as:

$$\boldsymbol{Loss}=RMSE(\overline{\boldsymbol{\Phi}}_t^k,\widehat{\boldsymbol{\Phi}}_t^k),$$

where $\overline{\boldsymbol{\Phi}}_t^k$ is predicted RIS configuration matrix.

After several training rounds, an optimal global model is trained for all RIS to build the mapping function between channel of UE and the optimal RIS configuration of all RISs, to realize the RIS reconfiguration in real time when meeting new device or the moving of device. At the same time, the proposed scheme training all RIS in parallel, saving the training time and computing resources while protecting the private information of UE effectively.

IV. Experiment and Discussion

In this section, we provide simulation results for the RIS assisted mmWave communications based on FL. The simulation settings and parameters are given firstly. The rate performance comparison between the proposed algorithm and centralized ML is also carried out at the same time. Finally, we test the performance of FL algorithm under different settings of parameters.

Table I. *Simulation parameters.*

Active BS	7
Grid of UEs (rows)	R2001 to R2360
Location of BS	Row R1850 Column 90
Number of SEs	5400
Antennas of RIS	M=576
Subcarriers number of OFDM channel	G=512
System bandwidth	100MHz
Number of selected subcarriers	64
Operating frequency	28GHz
Number of paths	L=10

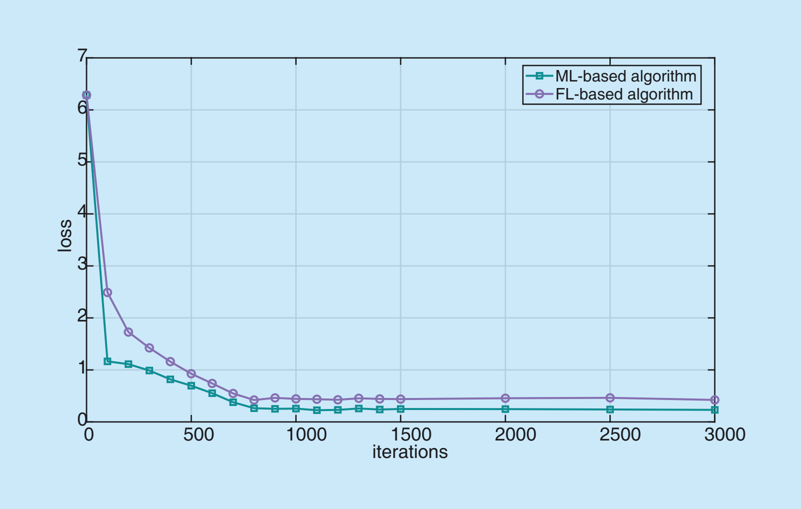


Fig. 6. *The convergence performance of FL-based algorithm and centralized ML-based algorithm.*

4.1 Simulation settings

As the algorithm described in section III, it is crucially important to generate sampled CSI to construct datasets. Consequently, the open dataset DeepMIMO is employed in this paper [33]. The sampled CSI is generated by utilizing '**O1**' ray-tracing scenario which contains the significant environment descriptors (e.g., the operating frequency, shape of buildings and the location of BS/UEs) that imply the influence of the environment on wireless channel[34].

The test bench we build is illustrated in Figure 5. Specifically, the BS 7 in original scenario is activated as RIS. The BS is located at row R1850 column 90. Meanwhile, UEs' grid is constructed with 65160 points from R2001 to R2360 where each row contains 181 points. In this paper, UEs' region is divided in to 6 parts which means $K = 6$, denoted as $U^k, k = 1,2,...,6$, respectively. Each region of UE contains 60 rows with 10860 points totally. For CSI sampling and estimation, we deploy 90 SEs each column in the region of UE. As for the distribution of these SEs, they are placed at even points from top to bottom in each column. Thus, the number of A is 5400, which implies the scale of local dataset, 80% and 20% of it are training set and validation set respectively. Besides, the default antenna configuration of RIS in this test bench is 24× 24 ($M = 576$) and the operating frequency is 28GHz. The system bandwidth of OFDM channel is 100MHz and the subcarriers number is $G = 512$. However, only the first 64 subcarriers are selected for the reason to reduce the complexity of DNN. As for the multipath effect of the wireless channel, we set $L = 10$. For the antennas of UEs and BS, the gain is set to 5dBi. And we implement DFT to establish the predefined interaction matrix set $\boldsymbol{O}$, all of the parameters in this experiment is given in Table 1.

Meanwhile, we adopt the same architecture of DNN on the setting of centralized ML for comparison. So the dataset of ML is the collection of all local datasets which contains 32400 data points totally.

4.2 Simulation results and discussion

In this subsection, the simulation results are demonstrated in three aspects as follows:

- The convergence performance comparison of the FL based algorithm and centralized ML algorithm.
- The achievable rate performance in bps/Hz based on proposed algorithm and centralized ML under the different number of active elements, and compared with theoretical value for reference which is refers to Perfect-Channel-Information (PCI).
- The rate performance of the proposed algorithm and centralized ML under the participation of different number of UEs and a comparison of several experimental groups is established according to different number of active elements.

The convergence performance of proposed algorithm and centralized ML is shown in Figure 7, where the rationality of FL-based algorithm is proved. Obviously, both the models of FL and ML converge after several iterations. However, the rate and effect of convergence are different. The convergence speed of ML is a little bit faster than that of FL, according to the analysis, it is credible that the distinction between convergence speed of FL and ML is caused by the communication delay during the FL process. And the effect of distributed ML is not as good as the centralized ML under the same training data scale and training time, which is reflected in the accuracy of the training model specifically. This also explains the existence of different convergence effect between FL and centralized ML.

The achievable rate performance of proposed algorithm and centralized ML are given in Figure 7, as illustrated in the figure, the rate performance of proposed algorithm can effectively approach to the centralized ML, we test the performance under the different number of active elements, where $\overline{M} = 2, 4, 6, 8, 10$ and 20, the achievable rate is increase as the increasing of $\overline{M}$. It is worth noting that the achievable rate can reach to 90% of the theoretical value when $\overline{M}$=8, so we can draw a conclusion that an appreciable communication rate can be realized through the proposed algorithm by only a minuscule fraction of the active elements. Furthermore, the rate performance between FL and ML is really small that can be negligible.

To investigate the performance of FL itself with different number of participators, which

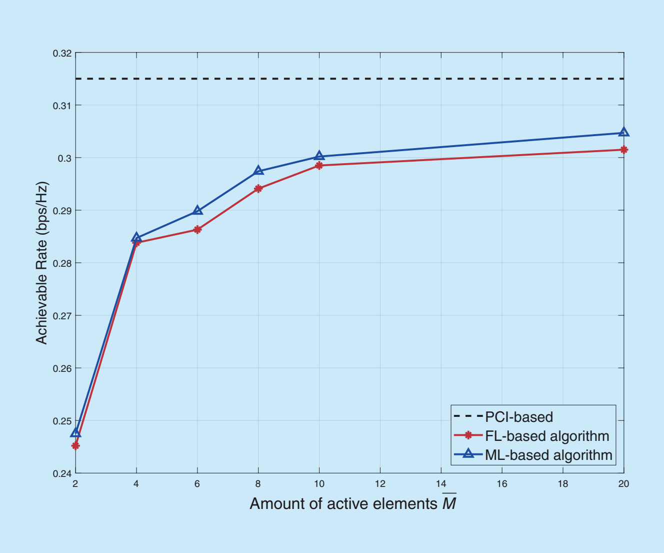


Fig. 7. *The achievable rate performance based on FL and centralized ML.*

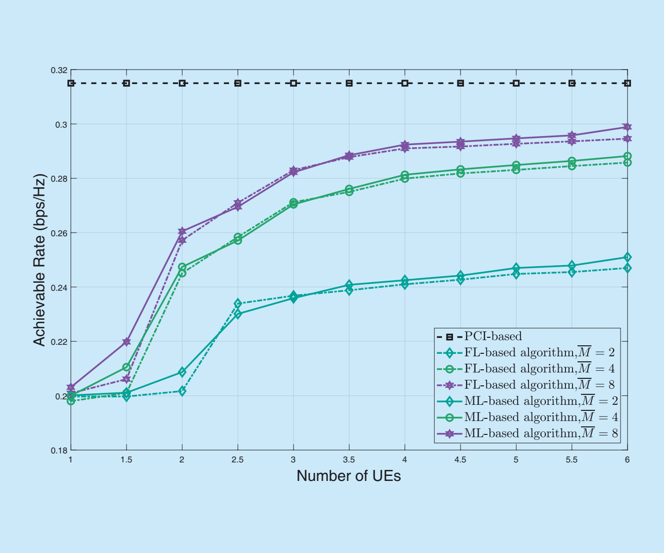


Fig. 8. *The achievable rate performance versus the number of UEs with different active elements of RIS.*

means different amount of training data. We develop the experiment about the rate performance versus different number of UEs under the different conditions of $\overline{M}=2,4,8$. The simulation results are demonstrated in Figure 8. For example, as indicated by the curves in green, the achievable rate is increase gradually with the increasing of UEs when the number of active elements is fixed, which corresponds to a fact that the more training data, the better training effect.

V. Conclusion

In this paper, we have investigated the problem about optimization of RIS and privacy protection. FL is introduced according to its excellent performance about distributed learning and privacy preservation. And we proposed two FL based communication schemes, which are FL-based RIS assisted outdoor communications and FL-based IoT network communications. The former applies FL to train the optimal DNN model for the mapping between user's channels and the optimal configuration matrix of RIS through distributed learning so as to perform high speed mmWave communications while effectively protect user's privacy. For the IoT network communications, the FL is deployed to optimize multiple RISs in parallel under the protection of private CSI, therefore, the optimal achievable rate of combined signal which is the superposition of the signals from all RISs can be reached. Furthermore, the simulations are implemented for the RIS assisted outdoor mmWave communication framework based on the FL, which indicate the rationality of the proposed algorithm and demonstrate that the rate performance of the proposed algorithm can effectively close to theoretical values and that of centralized ML. Moreover, we also compare the performance of the proposed algorithm under several different parameters' settings.

Acknowledgement

This work was supported in part by the National Natural Science Foundation of China under Grant 61901378, 61941119, 61901379, in part by the Natural Science Basic Research Plan in Shaanxi Province of China under Grant 2019JQ-253, in part by the open research fund of National Mobile Communications Research Laboratory, Southeast University under Grant 2020D04, in part by China Postdoctoral Science Foundation under Grant BX20190287. in part by the Aerospace Science and Technology Innovation Fund of China Aerospace Science and Technology Corporation, in part by the Shanghai Aerospace Science and Technology Innovation Fund (No. SAST2018045), in part by the China Fundamental Research Fund for the Central Universities (No. 3102018QD096), in part by the Seed Foundation of Innovation and Creation for Graduate Students in Northwestern Polytechnical University (No. CX2020152).

References

[1] M. Patzold, "It's time to go big with 5G [Mobile Radio]," *IEEE Vehicular Technology Magazine*, vol. 13, no. 4, pp. 4–10, Dec. 2018.

[2] "Cisco visual networking index: Global mobile data traffic forecast update, 2017–2022," available online: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-738429.pdf

[3] S. Samarakoon, M. Bennis, W. Saad, M. Debbah and M. Latva-aho, "Ultra dense small cell networks: Turning density into energy efficiency," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 5, pp. 1267-1280, May 2016.

[4] H. Q. Ngo, E. G. Larsson and T. L. Marzetta, "Energy and spectral efficiency of very large multiuser MIMO systems," *IEEE Transactions on Communications*, vol. 61, no. 4, pp. 1436-1449, April 2013.

[5] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *IEEE Communications Magazine*, vol. 58, no. 1, pp. 106-112, January 2020.

[6] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M. Alouini and R. Zhang, "Wireless communications through reconfigurable intelligent surfaces," *IEEE Access*, vol. 7, pp. 116753-116773, 2019.

[7] M. Di Renzo et al., "Smart radio environments empowered by reconfigurable AI meta-surfaces: An idea whose time has come," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, p. 129, May 2019.

[8] Y. Cao and T. Lv, “Intelligent reflecting surface aided multi-user millimeter-wave communications for coverage enhancement,” *available online: arxiv.org/abs/1910.02398, 2019*.

[9] S. Hu, F. Rusek and O. Edfors, "Beyond massive MIMO: The potential of data transmission with large Intelligent surfaces," *IEEE Transactions on Signal Processing*, vol. 66, no. 10, pp. 2746-2758, 15 May15, 2018.

[10] X. Tan, Z. Sun, J. M. Jornet and D. Pados, "Increasing indoor spectrum sharing capacity using smart reflect-array," *2016 IEEE International Conference on Communications (ICC)*, Kuala Lumpur, 2016, pp. 1-6.

[11] N. S. Perović, M. D. Renzo and Mark F. Flanagan, “Intelligent reflecting surface aided multi-User millimeter-wave communications for coverage enhancement,” *available online: arxiv.org/abs/1910.14310, 2019*.

[12] C. Huang, G. C. Alexandropoulos, C. Yuen and M. Debbah, "Indoor signal focusing with deep learning designed reconfigurable intelligent surfaces," *2019 IEEE 20th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Cannes, France, 2019, pp. 1-5.

[13] H. Guo, Y. Liang, J. Chen and Erik G. Larsson, “Weighted sum-rate optimization for intelligent reflecting surface enhanced wireless networks,” *available online: arxiv.org/abs/1905.07920, 2019*.

[14] A. Taha, M. Alrabeiah, and A. Alkhateeb, “Enabling large intelligent surfaces with compressive sensing and deep learning,” *available online: arxiv.org/abs/1904.10136, 2019*.

[15] X. Yu, D. Xu and R. Schober, "MISO wireless communication systems via intelligent reflecting surfaces: (Invited Paper)," *2019 IEEE/CIC International Conference on Communications in China (ICCC*), Changchun, China, 2019, pp. 735-740.

[16] C. Huang, A. Zappone, G. C. Alexandropoulos, M. Debbah and C. Yuen, "Reconfigurable intelligent surfaces for energy efficiency in wireless communication," *IEEE Transactions on Wireless Communications*, vol. 18, no. 8, pp. 4157-4170, Aug. 2019.

[17] M. Fu, Y. Zhou, and Y. Shi, “Intelligent reflecting surface for downlink non-orthogonal multiple access networks,” *available online: arxiv.org/abs/1906.09434, 2019*.

[18] M. Jung, W. Saad, and G. Kong, “Performance analysis of large intelligent surfaces (LISs): Uplink spectral efficiency and pilot training,” *available online: arxiv.org/abs/1904.00453, 2019*.

[19] M. Cui, G. Zhang and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Communications Letters*, vol. 8, no. 5, pp. 1410-1414, Oct. 2019.

[20] J. Chen, Y. Liang, Y. Pei and H. Guo, "Intelligent reflecting surface: A programmable wireless environment for physical layer security," *IEEE Access*, vol. 7, pp. 82599-82612, 2019.

[21] S. Khan, S. Y. Shin, “Deep-learning-aided detection for reconfigurable intelligent surfaces,” *available online: arxiv.org/abs/1910.09136, 2019*.

[22] C. Liaskos, A. Tsioliaridou, S. Nie, A. Pitsillides, S. Ioannidis and I. Akyildiz, "An interpretable neural network for configuring programmable wireless environments," *2019 IEEE 20th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Cannes, France, 2019, pp. 1-5.

[23] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network: Joint active and passive beamforming design," *2018 IEEE Global Communications Conference (GLOBECOM)*, Abu Dhabi, United Arab Emirates, 2018, pp. 1-6.

[24] Q.-U.-A. Nadeem, A. Kammoun, A. Chaaban, M. Debbah, and M.- S. Alouini, “Intelligent reflecting surface assisted multi-user MISO communication,” *available online: arxiv.org/abs/1906.02360, 2019*.

[25] Junyi Wang et al., "Beam codebook based beamforming protocol for multi-Gbps millimeter-wave WPAN systems," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 8, pp. 1390-1399, October 2009.

[26] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas “Communication-efficient learning of deep networks from decentralized data,” *available online: arxiv.org/abs/1602.05629, 2016*.

[27] D. Ma, L. Li, H. Ren, D. Wang, X. Li and Z. Han, "Distributed rate optimization for intelligent reflecting surface with federated learning," *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*, Dublin, Ireland, 2020, pp. 1-6.

[28] S. Samarakoon, M. Bennis, W. Saad and M. Debbah, "Federated learning for ultra-reliable low-latency V2V communications," *2018 IEEE Global Communications Conference (GLOBECOM)*, Abu Dhabi, United Arab Emirates, 2018, pp. 1-7.

[29] S. Savazzi, S. Sigg, F. Vicentini, S. Kianoush and R. Findling, "On the use of stray wireless signals for sensing: A look beyond 5G for the next generation of industry," *Computer*, vol. 52, no. 7, pp. 25-36, July 2019.

[30] S. Kianoush, M. Raja, S. Savazzi and S. Sigg, "A cloud-IoT platform for passive radio sensing: Challenges and application case studies," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3624-3636, Oct. 2018.

[31] M. Chen, O. Semiari, W. Saad, X. Liu and C. Yin, "Federated echo state learning for minimizing breaks in presence in wireless virtual reality networks," *IEEE Transactions on Wireless Communi-*

cations, vol. 19, no. 1, pp. 177-191, Jan. 2020.

[32] S. Yeh, S. Talwar, G. Wu, N. Himayat and K. Johnsson, "Capacity and coverage enhancement in heterogeneous networks," *IEEE Wireless Communications*, vol. 18, no. 3, pp. 32-38, June 2011.

[33] A. Alkhateeb, “DeepMIMO: A generic deep learning dataset for millimeter wave and massive MIMO applications,” *available online: arxiv.org/abs/1902.06435, 2019*.

[34] Remcom, *available online: http://www.remcom.com/wireless-insite*.

Biographies

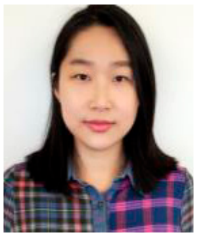
Lixin Li, received the B.Sc. and M.Sc. degrees in communication engineering, and the Ph.D. degree in control theory and its applications from Northwestern Polytechnical University (NPU), Xi’an, China, in 2001, 2004, and 2008, respectively. He was a Post-Doctoral Fellow with NPU from 2008 to 2010. In 2017, He was a visiting scholar at the University of Houston, Texas. He is currently an Associate Professor in the School of Electronics and Information, NPU. He has authored or coauthored more than 150 peer-reviewed papers in many prestigious journals and conferences, and he holds 12 patents. His current research interests include wireless communications, game theory, and machine learning. He received the 2016 NPU Outstanding Young Teacher Award, which is the highest research and education honors for young faculties in NPU.

Donghui Ma, is currently pursuing the master’s degree under supervision of Prof. Lixin Li with the school of electronics and information, Northwestern Polytechnical University, China. His research interests include federated learning and millimeter wave communications.

Huan Ren, is currently a master student under supervision of Prof. Lixin Li with the School of Electronics and Information, Northwestern Polytechnical University, China. Her research interests include hybrid precoding in millimeter massive MIMO and machine learning in wireless communication network.

Dawei Wang, received the B.S degree from University of Jinan, China, in 2011 and the Ph.D. degree from Xi’an Jiaotong University, China in 2018. From 2016 to 2017, he was a Visiting Student with the School of Engineering, The University of British Columbia. He is currently an Associate Professor with the School of Electronics and Information, Northwestern Polythechnical University, Xi’an, China. His research interests include Physical-Layer Security, Cognitive Radio Networks, Cooperative Communication, and Resource Allocation.

Xiao Tang, received his B.S. degree in Information Engineering (Elite Class Named After Tsien Hsue-shen) and Ph.D. degree in Information and Communication Engineering from Xi’an Jiaotong University in 2011 and 2018, respectively. From September 2015 to August 2016, he worked as a visiting student at the Department of Electrical and Computer Engineering in University of Houston. He is now with the Department of Communication Engineering in Northwestern Polytechnical University. His research interests include wireless communications and networking, resource management, game theory, and physical layer security.



Wei Liang, is currently an Associate Professor in the School of Electronics and Information, NPU. Her research interests include matching theory, Non-orthogonal multiple access scheme and Mobile edge computing etc.

Tong Bai, received the B.Sc. degree in telecommunications from Northwestern Polytechnical University, Xi’an, China, in 2013, and the M.Sc. and Ph.D. degrees in communications and signal processing from the University of Southampton, Southampton, U.K., in 2014 and 2019, respectively. Since 2019, he has been a Postdoctoral Researcher with Queen Mary University of London, London, U.K. His research interests include the performance analysis, transceiver design, and utility optimization for power-line and wireless communications as well as for Internet of Things.