Spectrum Breathing: Protecting Over-the-Air Federated Learning Against Interference

Zhanwei Wang, Kaibin Huang, and Yonina C. Eldar

Abstract

Federated Learning (FL) is a widely embraced paradigm for distilling artificial intelligence from distributed mobile data. However, the deployment of FL in mobile networks can be compromised by exposure to interference from neighboring cells or jammers. Existing interference mitigation techniques require multi-cell cooperation or at least interference channel state information, which is expensive in practice. On the other hand, power control that treats interference as noise may not be effective due to limited power budgets, and also that this mechanism can trigger countermeasures by interference sources. As a practical approach for protecting FL against interference, we propose Spectrum Breathing, which cascades stochastic-gradient pruning and spread spectrum to suppress interference without bandwidth expansion. The cost is higher learning latency by exploiting the graceful degradation of learning speed due to pruning. We synchronize the two operations such that their levels are controlled by the same parameter, Breathing Depth. To optimally control the parameter, we develop a martingale-based approach to convergence analysis of Over-the-Air FL with spectrum breathing, termed AirBreathing FL. We show a performance tradeoff between gradient-pruning and interference-induced error as regulated by the breathing depth. Given receive SIR and model size, the optimization of the tradeoff yields two schemes for controlling the breathing depth that can be either fixed or adaptive to channels and the learning process. As shown by experiments, in scenarios where traditional Over-the-Air FL fails to converge in the presence of strong interference, AirBreathing FL with either fixed or adaptive breathing depth can ensure convergence where the adaptive scheme achieves close-to-ideal performance.

Index Terms

Over-the-Air federated learning, gradient pruning, spread spectrum, interference suppression.

Z. Wang and K. Huang are with the Department of Electrical and Electronic Engineering, The University of Hong Kong (HKU), Hong Kong (Email: {zhanweiw, huangkb}@eee.hku.hk). Y. C. Eldar is with the Faculty of Math and CS, Weizmann Institute of Science, Rehovot, Israel (Email: yonina.eldar@weizmann.ac.il). The corresponding author is K. Huang.
I. INTRODUCTION

A key operation of the sixth-generation (6G) mobile network is to distill intelligence from enormous mobile data at the network edge using distributed machine learning algorithms, resulting in an active area termed edge learning [1], [2]. The obtained Artificial Intelligence (AI) is expected to empower many Internet-of-Things (IoT) applications ranging from smart cities to auto-pilots to extended reality. Federated Learning (FL) is arguably the most popular edge-learning framework for its preservation of data ownership and being considered for the 6G standard [3], [4]. FL protects users’ data privacy by distributing the learning task and requiring users to upload local model updates instead of raw data [5]. Among others, two key challenges stymieing the deployment of FL in a mobile network are 1) a communication bottleneck resulting from the transmission of high-dimensional model updates and 2) exposure to interference from neighboring cells, and jammers [2], [6]–[8]. To simultaneously tackle these two challenges, we propose a spectrum-efficient method for suppressing interference to FL in mobile networks, termed Spectrum Breathing.

The key operation of FL is for a server to upload local updates from devices, which are computed using local data, for aggregation to update the global model. To overcome the resultant communication bottleneck, previous works focus on designing task-oriented wireless techniques for FL with the aim to alleviate the effects of channel hostility on learning performance. Diversified approaches have been proposed including radio resource management [9], [10], power control [11], [12], and device scheduling [13], [14]. On the other hand, the direct approach to reduce communication overhead is to prune local model updates, namely local models or stochastic gradients, and furthermore adapt the pruning operation to wireless channels [15]–[17]. Instead of incurring unrecoverable distortion, gradient pruning can be translated via randomization into longer learning latency with small accuracy degradation [18].

Recently, a new class of techniques, termed Over-the-Air FL (AirFL), has emerged to address the scalability issue in multi-access by many devices under a constraint on radio resources [19]–[21]. Underpinning AirFL is the use of so-called Over-the-Air Computing (AirComp) to realize over-the-air aggregation of local updates by exploiting the waveform superposition property of a multi-access channel, and thereby enable simultaneous access [22]. Building on AirComp, the efficiency of AirFL can be enhanced by beamforming [20], gradient pruning [21], broadband transmission [19] and power control [12], [23], and even the use of Intelligent Reflecting Surface
Different from traditional designs, such techniques aim to realize the required signal-magnitude alignment at the server to implement AirComp despite channel distortion. For instance, an IRS can help to overcome such distortion to suppress the alignment error. Furthermore, the optimization of AirFL techniques enables them to be adapted to not only channel states but also learning operations (e.g., gradient statistics in the current round). The effectiveness of AirFL and AirComp at large hinges on the use of uncoded linear analog modulation for transmission. This exposes AirFL to interference and gives rise to the challenge of how to make AirFL robust. Gradient pruning techniques mentioned earlier do not address this challenge as they merely reduce communication overhead without making any attempt at interference suppression. An alternative approach is to treat interference as noise and regulate it using existing power-control techniques for AirFL. This class of techniques’ effectiveness in dealing with interference is limited for two reasons. First, interference power may be comparable with that of the signal if not larger and far exceeds the noise power. Second, unlike noise, an interference source (e.g., a neighboring access point or a jammer) is active and can react to the power control of a signal source in a way that renders it ineffective.

An additional line of work is to adapt the rich set of existing interference-mitigation techniques to suit AirFL. Previous works share the common principle of relying on cooperation between interfering nodes to mitigate the effects of their mutual interference on the learning performance. This principle is materialized in diversified techniques for multi-cell AirFL systems, including spatial interference cancellation, signal-and-interference alignment into orthogonal signal sub-spaces, and cooperative power control and devices scheduling. However, their implementation requires accurate Channel State Information (CSI) of interference channels. Acquiring such information can incur extra overhead and latency due to inter-cell messaging in multi-cell systems, and is infeasible in scenarios where the interference sources are in other networks or jammers.

One classic interference mitigation technique, called spread spectrum, has no such limitations but has not been explored in the context of AirFL due to its low efficiency in spectrum utilization. This technique can reduce interference power by a factor, called the Processing Gain denoted as $G$, if a narrowband signal is spread in the spectrum by $G$ via scrambling using a Pseudo-Noise (PN) sequence at the transmitter and using the same sequence to reverse the operation, called despreading, at the receiver. These operations neither require multi-cell cooperation nor interference CSI. Its invention served the purpose of anti-jamming for secured...
communication in World War II while its commercial success was due to the use for mitigating multi-user interference in a resultant multi-access scheme, termed Code-Divison Multi-Access (CDMA), for 3G [30], [31].

Gradient pruning and spread spectrum are two well-known techniques. The novelty of the proposed spectrum breathing approach lies in their integration to cope with interference in an AirFL system under a bandwidth constraint. Specifically, deployed at each device, the technique cascades two operations before transmission – random pruning of local gradient, called spectrum contraction, and spread spectrum on the pruned gradient. Note that random pruning is more suitable for AirFL than the alternative of magnitude-based pruning [32] (also see discussion in Sec. III). The spectrum contraction and spreading are governed by parameter, call breathing depth. As mentioned, the former mainly results in lengthened learning latency; the latter suppresses interference power by the factor of breathing depth. As a result, AirFL can converge even in the presence of strong interference. In the iterative FL algorithm, the alternating spectrum contraction and spreading are analogous to human breathing, giving the technique its name. We optimally control the spectrum breathing parameter so as to maximize its performance gain.

The contributions of this paper are summarized as follows.

• **Convergence Analysis:** Adjusting the breathing depth provides a mechanism for controlling AirFL using spectrum breathing, termed AirBreathing FL. To facilitate optimal control, we analyze the learning convergence by extending an existing supermartingale-based approach to account for AirComp, spectrum breathing and fading. The derived results reveal a tradeoff as regulated by the breathing depth. Specifically, increasing the parameter has two opposite effects – one is to improve the successful convergence probability by interference suppression and the other is to decrease it due to more aggressive gradient pruning. This gives rise to the need of optimal control.

• **Control of Spectrum Breathing:** Using the preceding tradeoff, the optimization of breathing depth yields two schemes for controlling AirBreathing FL under given receive SIR and model size. First, without CSI and Gradient State Information (GSI) at the server, the parameter is fixed over rounds and its optimal value is derived in closed form. Second, when CSI and GSI are available as in [12], the optimal strategy is designed to be adapted to CSI and GSI.

• **Experimental Results:** The results from experiments on AirBreathing FL demonstrate satisfactory learning performance even in the cases with strong interference that could fail
Fig. 1. System diagram of AirFL system perturbed by interference.

the learning task without spectrum breathing. Moreover, spectrum breathing with depth adaptation outperforms the case with a fixed breathing depth.

The remainder of this paper is organized as follows. Models and metrics are introduced in Sec. II. The effects of pruning on generic data and FL is demonstrated in Sec. III. Overview design of spectrum breathing is illustrated in Sec. IV. Convergence analysis and breathing depth optimization are analyzed in Sec. V and VI, respectively. Experimental results are provided in Sec. VII, followed by concluding remarks in Sec. VIII.

II. MODELS AND METRICS

We consider an AirFL system as illustrated in Fig. 1 that comprises one server and $K$ devices. The learning process is perturbed by external interference (e.g. from other cells). The learning and communication models are described separately in the following sub-sections.

A. Learning Model

We first describe the FL process underpinning AirFL. Each device, say $k$, maintains its local dataset $\mathcal{D}_k$ including $|\mathcal{D}_k|$ pairs of data sample $x_j$ and label $y_j$, denoted as $\{(x_j, y_j)\} \in \mathcal{D}_k, j \in \{1, 2, \ldots, |\mathcal{D}_k|\}$. The server coordinates $K$ devices to optimize the weights of the global model $w \in \mathbb{R}^D$ where $D$ is the model size, under the criterion of minimizing a global loss defined as

$$F(w) \triangleq \frac{1}{\sum_{k=1}^{K} |\mathcal{D}_k|} \sum_{k=1}^{K} \sum_{(x_j, y_j) \in \mathcal{D}_k} f(w, x_j, y_j), \quad (1)$$
where \( f(w, x_j, y_j) \) is the empirical loss function indicating the prediction error on model \( w \) using a data sample \((x_j, y_j)\). For simplicity, we denote \( f(w, x_j, y_j) \) as \( f_j(w) \). Distributed Stochastic Gradient Descent (SGD) is applied to minimize the global loss. Specifically, time is divided into \( N \) rounds with index \( n \in \{0, 1, \ldots, N - 1\} \). Considering round \( n \), each device computes the gradient of the empirical loss function using a mini-batch of local dataset. The gradient of device \( k \) is given as
\[
g_k(n) = \frac{1}{|B_k|} \sum_{j \in B_k} \nabla f_j(w(n)),
\]
where \( B_k \subseteq D_k \) is the selected mini-batch of \( D_k \), and \( \nabla \) represents the gradient operation. If local gradients can be reliably transmitted to the server, the global estimate of the gradient of the loss function in (1) is obtained as
\[
g(n) = \frac{1}{K} \sum_{k=1}^K g_k(n).
\]
Then, \( g(n) \) is broadcast back to each device, by which the current model is updated via gradient descent:
\[
w(n+1) = w(n) - \eta \cdot g(n),
\]
where \( \eta \) denotes the learning rate. The distributed SGD is thus to iterate (2) and (4) until a convergence condition is met.

**B. Communication Model**

The uploading of the gradients using AirComp is perturbed by interference. To combat interference, each transmitted signal undergoes the operations of random pruning and spread spectrum. The two operations of AirBreathing FL are elaborated in Section [IV]. For the current exposition, some useful notation is introduced. Considering round \( n \), the \( s \)-th element of the pruned local gradient transmitted by device \( k \) is scrambled by spread spectrum into a sequence, denoted \( \tilde{g}_{k,s}(n) \), with each element called a chip and the \( \ell \)-th chip denoted as \( \tilde{g}_{k,s}^{(n)}[\ell] \).

Using the above notation, AirComp can be modelled as follows. Assume chip-level synchronization between devices using a standard technique such as Timing Advance [33]. The simultaneous transmission of the \((s, \ell)\)-th chips, i.e., \( \tilde{g}_{k,s}(n)[\ell] \), enables AirComp to yield the corresponding received chip symbol, given as
\[
[y_s(n)]_{\ell} = \sum_{k=1}^K h_k(n) \sqrt{p_k(n)} [\tilde{g}_{k,s}(n)]_{\ell} + [z_s(n)]_{\ell}, \quad \forall (s, \ell),
\]
where \( h_k(n) \sim \mathcal{N}(0,1) \) represents the \( k \)-th fading channel-gain that remains constant with round \( n \), \( p_k(n) \) the transmission power, \([z_a(n)]_\ell \sim \mathcal{N}(0,P_I)\) is additive Gaussian interference. We consider the worst-case interference distribution that is Gaussian over chip duration \([34]\). Given an interference-limited system, channel noise is assumed negligible.

The downloading of the aggregated gradient can be implemented using digital or analog transmission \([35]\). Besides the availability of full bandwidth, transmission power at the server is much larger than that of the devices. Thus, gradient broadcasting is much more reliable than local gradient uploading such that the distortion to downlink is negligible.

C. Performance Metric

To quantify the distortion from gradient-pruning and interference, we introduce an AirComp error. Consider round \( n \) and active device set \( \mathcal{K}(n) \subseteq \{1,2,\ldots,K\} \). After post-processing the received signal \( y(n) \) in (5), the output at the server is denoted as \( y'(n) \) specified in Sec. IV. Then AirComp error is defined as the \textit{Mean Squared Error} (MSE) between \( y'(n) \) and its desired ground-truth, namely \( \frac{1}{|\mathcal{K}(n)|} \sum_{k \in \mathcal{K}(n)} g_k(n) \), as

\[
\text{MSE}(n) = \mathbb{E} \left[ \left\| \frac{1}{|\mathcal{K}(n)|} \sum_{k \in \mathcal{K}(n)} g_k(n) - y'(n) \right\|^2 \right],
\]

where the expectation is taken over the distributions of the transmitted symbols, interference, channel fading, and pruning pattern.

III. DISTORTION FROM PRUNING - GENERIC DATA VERSUS FEDERATED LEARNING

The spectrum-contraction operation of AirBreathing FL is realized via pruning local gradients in the FL process. Its effect on the system performance is fundamentally different from that of pruning a generic data sequence. This can be better understood by analyzing and comparing the two effects in the remainder of this section.

A. Generic Data Pruning

Consider gradient \( g_k(n) \in \mathbb{R}^D \), that is i.i.d. distributed with each element having zero-mean and variance of \( \sigma^2 \). The desired ground truth \( \frac{1}{|\mathcal{K}(n)|} \sum_{k \in \mathcal{K}(n)} g_k(n) \) is compressed by random pruning, namely a function that randomly replaces elements with zeros. Let \( g^{sp}(n) \) and \( \gamma \) denote the pruned gradient and the remaining fraction of nonzero elements, called the pruning ratio.
For generic data, the distortion from pruning is commonly quantified as the MSE between the pruned sequence and its ideal version:

$$\text{MSE}(n) = \mathbb{E} \left[ \left\| \mathbf{g}_{sp}(n) - \frac{1}{|\mathcal{K}(n)|} \sum_{k \in \mathcal{K}(n)} \mathbf{g}_k(n) \right\|^2 \right] = (1 - \gamma) \frac{D\sigma^2}{|\mathcal{K}(n)|}. \quad (7)$$

One can see that the distortion increases linearly with the level of pruning $(1 - \gamma)$. If the pruning represents channel erasures, then the lost information can not be recovered at the server.

**B. Stochastic Gradient Pruning**

The reliability of a generic communication system is measured by data distortion as we have discussed. On the contrary, the performance of an FL system is measured using an *End-to-End* (E2E) metric such as convergence rate or learning accuracy. In such a system, the pruning of transmitted data has the effect of slowing down the learning speed. Recall that FL is essentially a distributed implementation of SGD. To substantiate the above claim, we consider randomly pruned SGD implemented using classic *Block Coordinate Descent* (BCD) [18]. Let the loss function, $F(\mathbf{w})$ comprise a smooth and convex loss function, $f(\mathbf{w})$, that is regularized by a block separable function, $\Phi(\mathbf{w})$:

$$F(\mathbf{w}) = f(\mathbf{w}) + \Phi(\mathbf{w}). \quad (8)$$

The regularization $\Phi(\mathbf{w}) = \sum_{b=1}^{B} \Phi_b(\mathbf{w}_b)$ is a sum of $B$ convex, closed functions $\Phi_b(\mathbf{w}_b)$ where $\mathbf{w}_b$ is a block of model parameters. The blocks are non-overlapping and together they constitute the whole model. Considering round $n$, the server selects one block randomly and notifies devices. Then each device computes the gradient locally based on $\mathbf{w}(n)$ and uploads the specified block of coefficients to the server. Thus, only one selected block is updated using a pruned gradient aggregated from devices, i.e., $\mathbf{g}_{sp}(n)$, while others remain unchanged. Mathematically,

$$\mathbf{w}(n + 1) = \mathbf{w}(n) - \eta \mathbf{g}_{sp}(n). \quad (9)$$

Equivalently, BCD can be seen as distributed SGD updated with pruned gradients where the pruning ratio is $\gamma = \frac{1}{B}$. Its convergence rate is measured by the required number of iterations, say $N_{\epsilon, \rho}$, guaranteeing $\epsilon$-accuracy with probability of at least $1 - \rho$, $\rho \in (0, 1]$:

$$\Pr\{F(\mathbf{w}(N_{\epsilon, \rho})) - F(\mathbf{w}^*) \leq \epsilon\} \geq 1 - \rho, \quad (10)$$
where \(w^*\) represents the global optimality point. It can be proved that \(\text{[18]}\),

\[
N_{\epsilon,\rho} \leq O \left( \frac{B}{\epsilon \log \left( \frac{1}{\rho} \right)} \right) = O \left( \frac{1}{\gamma \epsilon \log \left( \frac{1}{\rho} \right)} \right).
\]

One can observe that the required number of iterations (i.e., learning latency) is inversely proportional to the pruning ratio.

C. Why Random Pruning for AirFL?

Random gradient/model pruning is popularly adopted for FL (see e.g., \([15]\), \([32]\)). The alternative scheme, importance-aware pruning that prunes gradient coefficients with the smallest magnitudes, does not allow efficient implementation for several reasons discussed in \([32]\).

First, AirComp requires local gradient coefficients pruned by different devices to have identical positions in the local gradient vectors. This cannot be guaranteed if devices perform independent importance-aware pruning. Second, doing so requires devices to upload indices of pruned/remaining coefficients to the server to facilitate aggregation, thereby incurring additional, significant communication overhead \([36]\). Finally, importance-aware pruning increases devices’ computation loads due to the coefficient sorting of high-dimensional gradient vectors.

IV. OVERVIEW OF SPECTRUM BREATHING

As illustrated in Fig. 2, the proposed spectrum breathing technique consists of operations at the transmitter of a device and at the receiver of the server. They are described separately in the following sub-sections.

A. Transmitter Design

The transmitter design is shown in Fig. 2(a), comprising three cascaded operations, i.e., spectrum contraction, channel inversion, and spectrum spreading.

1) Spectrum Contraction: The operation is to randomly prune the elements of a local gradient at each device. The purpose is to create extra bandwidth for the latter operation of spread spectrum. The operation compresses the spectrum required for transmitting a local gradient, giving the name of spectrum contraction. Consider round \(n\) and local gradient \(g_k(n)\) at device \(k\). Let \(\psi_n, S_n \triangleq |\psi_n|\), and \(\Omega_n\) denote the selected element set, number of selected elements, and the set of all \(S_n\)-element subsets of \(\{1, 2, \ldots, D\}\), respectively. At the server, \(\psi_n\) is chosen randomly from \(\Omega_n\) before being broadcast to devices. Using \(\psi_n\), device \(k\) compresses \(g_k(n)\) into
an $S_n \times 1$ vector, denoted as $g_{co}^k(n) = \Psi(g_k(n))$, using the pruning function $\Psi(\cdot) : \mathbb{R}^D \rightarrow \mathbb{R}^{S_n}$. Note that the pruning pattern $\psi_n$ is identical for all devices as required for AirComp to realize element alignment. Since the gradient statistics may change over iterations, normalization is needed in each round to meet the power constraint [37]. The normalized pruned gradient of the compressed version is given as

$$\hat{g}_{co}^k(n) = \frac{g_{co}^k(n) - M(n)}{V(n)},$$  \hspace{1cm} (12)

where $1$ is an all-one vector. Considering i.i.d data distribution as in [6], [19] and random pruning, the elements of $g_{co}^k(n)$ can be modeled as identically distributed random variables over $k$ with mean $M(n)$ and variance $V^2(n)$. This enables normalized gradient symbol power, i.e., $\frac{1}{S_n} \mathbb{E}[\|\hat{g}_{co}^k(n)\|^2] = 1$.

2) Channel Inversion: Following [19], truncated channel inversion is performed to achieve amplitude alignment as required for AirComp. We consider block fading channels such that the channel state is constant in each round. To avoid deep fading, device $k$ is inverted only if its gain exceeds a given threshold, denoted as $G_{th}$, or otherwise device $k$ is absent in this round by setting its power as zero. Mathematically,

$$p_k(n) = \begin{cases} \frac{P_0}{|h_k(n)|^2}, & |h_k(n)|^2 \geq G_{th} \\ 0, & |h_k(n)|^2 < G_{th}, \end{cases}$$ \hspace{1cm} (13)

where $P_0$ is the signal-magnitude-alignment factor. Transmission of each device is subject to a long-term power constraint over $N$ rounds:

Fig. 2. Transceiver of the spectrum breathing system.
where the expectation is taken over the randomness of channel coefficients and transmitted symbols. Given (5), $P_0$ determines the receive SIR of the model-update from each device [19].

The probability that device $k$ avoids truncation, called activation probability, is denoted by $\xi_a$ and obtained as

$$\xi_a = \Pr(|h_k(n)|^2 \geq G_{th}) = e^{-G_{th}}.$$  \hfill (15)

Due to random truncation, the random set of active devices of round $n$ is denoted as $K(n)$, which varies over rounds.

3) Spectrum Spreading: For interference suppression, spectrum spreading [30] is performed to expand the data bandwidth, denoted as $B_s(n)$, into the whole available bandwidth, denoted as $B_c$, using PN sequences. Let $T_s(n) = \frac{1}{B_s(n)}$ and $T_c = \frac{1}{B_c}$ denote the duration of one gradient symbol and one chip of PN sequences, respectively. Then a PN sequence comprises $G_n = T_s(n)/T_c$ chips, when $G_n$ is called the processing gain. The key operation of the spreader is to upsample and scramble the input elements by the corresponding PN sequences to realize spectrum expansion.

Given the $s$-th input element of the spreader, say $[\hat{g}_{co_k(n)}]_s$, the corresponding PN sequence is represented as $C_{s}(n) \in \mathbb{R}^{G_n}$ wherein $[C_s(n)]_{\ell} \in \{+1,-1\}$, $s \in \{1,2,\ldots,S_n\}$, $\ell \in \{1,2,\ldots,G_n\}$ is the $\ell$-th chip and is generated at the server through Bernoulli trails with the probability 0.5. The set of PN sequences, denoted as $C(n) \triangleq \{C_{1}(n),\ldots,C_{S_n}(n)\}$, is broadcast to all devices. For device $k$, the output of the spreader is represented by a $G_nS_n \times 1$ vector, say $\tilde{g}_k(n) = [[\tilde{g}_{k,1}(n)]^T,\ldots,[\tilde{g}_{k,s}(n)]^T,\ldots,[\tilde{g}_{k,S_n}(n)]^T]^T$, where $\tilde{g}_{k,s}(n) \in \mathbb{R}^G$ is a $G_n$-entry vector representing the spreading chips of $[\hat{g}_{co_k(n)}]_s$, given as

$$\tilde{g}_{k,s}(n) = [\hat{g}_{co_k(n)}]_s C_s(n), \ \forall(s,k).$$  \hfill (16)

Note that for all $s \in \{1,2,\ldots,S_n\}$, $\frac{1}{G_n} \sum_{\ell=1}^{G_n} [C_s(n)]_{\ell}^2 = 1$ holds.

B. Receiver Design

The receiver design is illustrated in Fig. 2(b) comprising three cascaded operations, i.e., spectrum de-spreading, signal de-normalization and zero padding.

1) Spectrum De-spreading: The operation targets mining the desired gradient symbols hidden in the interference using the de-spreader to be elaborated in the following. Perfect synchroniza-
tion between transmitters and receiver is assumed such that chip-level operations of spectrum de-spreading can be realized. Considering round \( n \), the received signals at the server are the superimposed waveform due to the simultaneous transmission of devices. Let \( \tilde{y}(n) \in \mathbb{R}^{S_n} \) denote the output vector of spectrum de-spreading. By introducing the truncated channel inversion in (13), the \( s \)-th output element, say \( [\tilde{y}(n)]_s \), is given as

\[
[\tilde{y}(n)]_s = \frac{1}{G_n} \sum_{\ell=1}^{G_n} [C_s(n)]_\ell [y_s(n)]_\ell = \sum_{k \in K(n)} \sqrt{\frac{P_0}{G_n}} \sum_{\ell=1}^{G_n} [C_s(n)]_\ell [G_k^{co}]_s + [\tilde{z}(n)]_s,
\]

where \( [\tilde{z}(n)]_s \sim \mathcal{N}(0, \frac{P_0}{G_n} I_D) \) is zero-mean Gaussian interference, whose power is inversely proportional to \( G_n \).  

2) Signal De-normalization: This operation is performed to eliminate the impact of normalization and channel inversion to obtain the noisy averaged gradient symbols, denoted as \( \hat{y}(n) \in \mathbb{R}^{S_n} \), given as

\[
\hat{y}(n) = \frac{V(n)}{\sqrt{P_0} |K(n)|} [\tilde{y}(n) + |K(n)| M(n) 1]
= \frac{1}{|K(n)|} \sum_{k \in K(n)} g_k^{co}(n) + \frac{V(n)}{\sqrt{P_0} |K(n)|} \tilde{z}(n). 
\]

3) Gradient Zero-padding: To facilitate global-model updating, zero padding executes the inverse of pruning \( \Psi^{-1}(\cdot) : \mathbb{R}^{S_n} \rightarrow \mathbb{R}^D \) to restore the \( D \)-dimensional update by inserting zeros into the punctured dimensions. The zero-padded gradient, denoted as \( y'(n) \), is represented as

\[
y'(n) = R \left( \frac{1}{|K(n)|} \sum_{k \in K(n)} g_k(n) + \tilde{z}(n) \right),
\]

where \( \tilde{z}(n) \in \mathbb{R}^D \) represents the interference vector distributed as \( \mathcal{N}(0, \frac{V^2(n)P_t}{P_0|K(n)|^2 G_n} I_D) \), and \( R(\cdot) : \mathbb{R}^D \times \Omega_n \rightarrow \mathbb{R}^D \) is the zero-padding operation; Finally, devices update the global model using the gradient \( y'(n) \) after its broadcasting from the server.

V. CONVERGENCE ANALYSIS OF AIRBREATHING FEDERATED LEARNING

In this section, we analyze the convergence of AirBreathing FL. The results are useful for optimizing the spectrum breathing in the next section.
A. Assumptions, Definitions, and Known Results

For tractable analysis, some commonly used assumptions, definitions, and known results are provided below. First, we consider a strongly-convex loss function with bounded gradient estimates. These assumptions are commonly used in the literature (see, e.g., [36], [39], [40]).

**Assumption 1.** The differentiable loss function $F(\cdot)$ is $c$-strongly convex, i.e., $\forall w_1, w_2 \in \mathbb{R}^D$, $F(w_1) - F(w_2) \geq \nabla F(w_1)^T (w_2 - w_1) + \frac{c}{2} \|w_2 - w_1\|^2$. \hfill (20)

**Assumption 2.** Let $w^* \in \mathbb{R}^D$ denote the optimality point of $F(\cdot)$. For $\varepsilon > 0$, there exists a success region indicating the convergence, defined as $S = \{w | \|w - w^*\|^2 \leq \varepsilon\}$.

**Assumption 3.** Local gradients $g_k(n)$ are i.i.d. over devices $k \in \{1, 2, \ldots, K\}$ with unbiased estimate of the ground truth $g(n)$ and bounded variance, i.e.,

$\mathbb{E}[g_k(n)] = g(n), \quad \mathbb{E}[\|g_k(n) - g(n)\|^2] \leq \sigma_g^2, \quad \mathbb{E}[\|g(n)\|^2] \leq \zeta^2$, \hfill (21)

for all $(n, k)$, where $\sigma_g^2$ and $\zeta^2$ are constants.

Next, we adopt the method of martingale-based convergence analysis in [39]. To this end, a useful definition and some known results from [39] are provided below.

**Definition 1 ( [39]).** A non-negative process $W_n(w(n), w(n-1), \ldots, w(0)) : \mathbb{R}^{D \times (n+1)} \rightarrow \mathbb{R}$ is defined as a rate supermartingale with a scalar parameter $A$, called the horizon, if the following conditions hold.

1) It must be a supermartingale [41], i.e., for any sequence $w(n), w(n-1), \ldots, w(0)$ and $\forall n \leq A$,

$$\mathbb{E}[W_{n+1}(w(n+1), w(n), \ldots, w(0))] \leq W_n(w(n), \ldots, w(0)).$$ \hfill (22)

2) For all rounds $N \leq A$ and for any sequence $w(n), w(n-1), \ldots, w(0)$, if the algorithm has not converged into the success region by $N$ (i.e., $w(n) \notin S, \forall n \leq N$),

$$W_N(w(N), w(N-1), \ldots, w(0)) \geq N.$$ \hfill (23)

**Lemma 1 ( [39], Lemma 1).** Consider an FL system updating as in (4) with a learning rate $\eta < 2c\varepsilon\mathbb{E}G^2$. If the algorithm has not converged by round $n$, the process defined as
\[ W_n(w(n), \ldots, w(0)) \triangleq \frac{\varepsilon}{2\eta c \varepsilon - \eta^2 G^2} \log \left( \frac{e \| w(n) - w^* \|^2}{\varepsilon} \right) + n, \]  

is a rate supermartingale with horizon \( A = \infty \), where \( G^2 \geq \zeta^2 + \sigma_g^2 \) is the upper bound of the squared norm of aggregated gradients. Under Assumptions 1-2, \( W_n(w(n), \ldots, w(0)) \) is also \( H \)-Lipschitz smooth in the first coordinate, with \( H = 2\sqrt{\varepsilon(2\eta c \varepsilon - \eta^2 G^2)^{-1}} \). In other words, for any \( n \geq 1, w_1, w_2 \in \mathbb{R}^D \) and any sequence \( w(n-1), \ldots, w(0) \), it satisfies

\[ \| W_n(w_1, w(n-1), \ldots, w(0)) - W_n(w_2, w(n-1), \ldots, w(0)) \| \leq H \| w_1 - w_2 \|. \]  

Intuitively, the rate supermartingale represents the level of satisfaction for model weights \( w(n), w(n-1), \ldots, w(0) \) over \( n + 1 \) rounds. Some intuition into the preceding assumptions are as follows. First, (22) reflects the fact that obtained model weights are more satisfactory as they approach the optimality point. Second, as specified in (23), the satisfaction is reduced if the algorithm is executed for many rounds without convergence. FL updating as in (4) is considered as the vanilla SGD satisfying the properties of rate supermartingale. It is a commonly used analytical method in the convergence analysis of SGD [36], [39], [40].

**B. Convergence Analysis**

Based on the preceding assumptions, we further develop the mentioned rate-supermartingale approach to study the convergence of AirBreathing FL. The new approach is able to account for channel fading, and the system operations such as AirComp and spread spectrum. Specifically, several useful intermediate results are obtained as shown in the following lemmas.

We first upper bound the gap between the vanilla SGD and AirBreathing FL using the results on the AirComp error (see Lemmas 2 and 3). Next, based on Lemma 3, a supermartingale for AirBreathing FL is constructed in Lemma 4. Furthermore, the upper bound of the convergence rate is derived using the theory of martingale as shown in Lemma 5.

**Lemma 2.** The AirComp error defined in (6) for round \( n \), can be expressed as the sum of the gradient-pruning error and interference-induced error:

\[ \text{MSE}(n) = (1 - \gamma_n) \mathbb{E}[\alpha^2(n)] + \frac{\gamma_n D P_t}{G_n P_0} \mathbb{E} \left[ \frac{V^2(n)}{|K(n)|^2} \right], \]  

where \( \gamma_n = \frac{S_n}{D} \) represents the pruning ratio in round \( n \), and \( \alpha^2(n) \) is defined as
\[ \alpha^2(n) = \left\| \frac{1}{|\mathcal{K}(n)|} \sum_{k \in \mathcal{K}(n)} g_k(n) \right\|^2. \]  

\[(27)\]

**Proof.** See Appendix A.

**Lemma 3.** Considering round \( n \), the gap between vanilla SGD and AirBreathing FL is defined as the expected difference between the update of vanilla SGD, namely \( \frac{1}{K} \sum_{k=1}^{K} g_k(n) \), and spectrum breathing, namely \( y'(n) \). The gap can be bounded as

\[ \mathbb{E} \left[ \left\| \frac{1}{K} \sum_{k=1}^{K} g_k(n) - y'(n) \right\| \right] \leq u(n), \]

\[(28)\]

where \( u(n) \) is defined as

\[ u(n) = \frac{2 - \xi_a \sigma_g^2}{K \xi_a} + \sqrt{\text{MSE}(n)}, \]

\[(29)\]

where \( \xi_a \) and \( \sigma_g^2 \) is the activation probability in (15) and gradient variance in (21), respectively. The first and second terms of the bound result from 1) the fading channel and gradient randomness and 2) the AirComp error in (26), respectively.

**Proof.** See Appendix B.

The process defined in Lamma 3, \( \{u(n)\} \), serves as indicators of performance loss caused by the air interface and is hence termed *propagation-loss process*. To this end, we use the result in Lemma 3 to define a new stochastic process pertaining to spectrum breathing and show it to be a supermartingale. The details are as follows.

**Lemma 4.** Define a stochastic process, \( \{U_n\} \), as

\[ U_n(w(n), \ldots, w(0)) \triangleq W_n(w(n), \ldots, w(0)) - \eta H \sum_{i=0}^{n-1} u(i), \]

\[(30)\]

for \( \forall i \leq n \) and \( w(i) \notin S \), \( \{U_n\} \) is a supermartingale process.

**Proof.** See Appendix C.

Note that, \( U_n \) has a negative term, which is a function of the propagation-loss process, removes from the model under training the effect of the air interface. Thereby, the result in Lemma 4 facilitates the use of supermartingale theory to quantify the convergence probability.
of AirBreathing FL as shown below.

**Lemma 5.** Consider $N$ rounds and AirBreathing FL for minimizing the loss function $F(w)$. If the learning rate satisfies

$$\eta < \frac{2\sqrt{\varepsilon} \left( c\sqrt{\varepsilon}N - \sum_{n=0}^{N-1} u(n) \right)}{N G^2},$$

(31)

the event of failing to converge to the success region, denoted as $F_N$, has a probability bounded as

$$\Pr\{F_N\} \leq \varepsilon \log \left( \frac{e\|w(0) - w^*\|^2\varepsilon^{-1}}{(2\eta c\varepsilon - \eta^2 G^2) N - 2\eta \sqrt{\varepsilon} \sum_{n=0}^{N-1} u(n)} \right).$$

(32)

where $G^2$ is the upper bound of aggregated gradient defined in Lemma 1.

*Proof:* See Appendix D.

**Definition 2 (Breathing Depth).** In the considered scenario of constrained bandwidth-and-latency, it is necessary to fix the product of processing gain and pruning ratio: $G_n \gamma_n = 1$. Under this constraint, the tradeoff between spread spectrum and gradient pruning can be regulated by the processing gain $G_n = \frac{1}{\gamma_n}$. To be more instructive, it is renamed the *Breathing Depth*, that is the most important control variable of spectrum breathing.

Substituting $G_n = \frac{1}{\gamma_n}$ into the result in Lemma 5 yields the following main result.

**Theorem 1.** Consider AirBreathing FL with breathing depths $\{G_n\}$ and $N$ rounds. If the learning rate satisfies (31), the probability of failing to converge to the success region is bounded as

$$\Pr\{F_N\} \leq \frac{\varepsilon \log \left( e\|w(0) - w^*\|^2\varepsilon^{-1} \right)}{(2\eta c\varepsilon - \eta^2 G^2) N - 2\eta \sqrt{\varepsilon} \sum_{n=0}^{N-1} u(n)}.$$  

(33)

Here $\beta_\Sigma = \sum_{n=0}^{N-1} \sqrt{\beta_n(G_n)}$ is a sum of error terms where each term $\beta_n(G_n)$ represents the air-interface error in round $n$, given as

$$\beta_n(G_n) = \left( 1 - \frac{1}{G_n} \right) \mathbb{E}[\alpha^2(n)] + \frac{DP_t}{G_n P_0} \mathbb{E} \left[ \frac{V^2(n)}{|K(n)|^2} \right].$$

(34)

Consider the air-interface error term in (34). One can see that increasing the breathing depth, $G_n$, corresponds to decreasing the pruning ratio and thus causes the pruning error to grow. On the
other hand, increasing $G_n$ enhances the process gain and thereby reduces interference perturbation (and its corresponding error term). The above tradeoff suggests the need of optimizing $\{G_n\}$, which is the topic of the next section.

Comparing Theorem 1 to the convergence analysis in related works [25], [36], our results have two main differences: First, our results reflect the effect of spectrum breathing depth, $G_n$, in (34), which does not exist in prior work. When $G_n = 1$ (no breathing, pruning), (34) reduces to the mean squared norm of the introduced noise in [25] (18). Second, the effect of fading channels on convergence is characterized in (34) by the term $\frac{1}{|\mathcal{K}(n)|^2}$, while the $|\mathcal{K}(n)|$ in [36] is assumed to be constant.

VI. OPTIMIZATION OF SPECTRUM BREATHING

In this section, the results from the preceding convergence analysis are applied to the optimization of the breathing depth of AirBreathing FL. To enhance convergence, Theorem 1 imposes the need of minimizing (34). Before that, the assumptions on known and unknown parameters are specified as follows. The predefined parameters, i.e., model size $D$ and receive SIR $\frac{P_0}{P_I}$, are assumed to be known. Let Gradient State Information (GSI) refer to the statistical parameters of the stochastic gradient in the current round, namely $\alpha(n)$ and $V(n)$ in (34), which are not accessible but can be estimated at each round using local gradients. Moreover, let CSI refer to the channel-dependent number of active devices in the current round, namely $|\mathcal{K}(n)|$. It is known to the server by assuming perfect channel estimation over rounds. Then we consider the optimization in two cases: (1) without GSI and CSI, and (2) with GSI and CSI at the server.

A. Breathing Depth Optimization without GSI and CSI Feedback

Without GSI and CSI feedback, we deploy fixed breathing depth for all rounds, i.e., $G_n = G, \forall n$. Consider the term $\beta_\Sigma$ in Theorem 1 which is the only term related to the breathing depth, $G$. Then $G$ is optimized to minimize $\beta_\Sigma$, thereby accelerating convergence. The difficulty of such optimization lies in the lack of the required GSI and CSI. To address the issue, we resort to minimizing an upper bound on $\beta_\Sigma$ that requires no such information.

Lemma 6. Consider gradient $g_k(n), k \in \mathcal{K}(n)$. There exists a positive constant $\Gamma(n)$, satisfying $\Gamma(n) \geq \frac{1}{D}(\|g(n)\|^2 + \sigma_g^2)$, such that $\beta_\Sigma$ is upper bounded as

$$\beta_\Sigma \leq \beta_F(G) \sum_{n=0}^{N-1} \sqrt{DG(n)},$$

(35)
where $\beta_F(G)$ is a function of $G$, given as

$$
\beta_F(G) = \sqrt{1 - \frac{1}{G} + \frac{6P_I}{G^2K^2\xi^2aP_0}}.
$$

(36)

Proof. See Appendix E

We next formulate the optimization problem

$$
\min_G \beta_F(G)
$$

s.t. $G \in \{1, 2, \ldots, D\}$.

(37)

Problem (37) can be solved by integer relaxation as follows. Given a continuous variable $x > 0$, setting $\nabla_x \beta_F(x) = 0$ yields the optimal solution $x^* = \frac{12P_I}{P_0K^2\xi^2a}$. Thus, for the discrete function $\beta_F(G), \forall G \in \{1, 2, \ldots, D\}$, the fixed breathing depth, denoted $G^*$, can be obtained approximately by

$$
G^* = \begin{cases} 
1, & x^* < 1, \\
\lfloor x^* \rfloor_{\beta_F(G)}, & 1 \leq x^* \leq D, \\
D, & x^* > D,
\end{cases}
$$

(38)

where $\lfloor \hat{x} \rfloor_{\beta_F(x)}$ is equal to $\lfloor \hat{x} \rfloor$ if $\beta_F(\lfloor \hat{x} \rfloor) \leq \beta_F(\lceil \hat{x} \rceil)$, and is otherwise equal to $\lceil \hat{x} \rceil$.

In the above results, $G^*$ is a monotonous decreasing function of the receive SIR $\frac{P_0}{P_I}$. It implies that for a low receive SIR, we allocate more bandwidth resources for interference suppression to guarantee convergence at cost of more aggressive gradient compression. On the other hand, for a high receive SIR, the spectrum-breathing control favours uploading as many gradient dimensions as possible to attain faster convergence. Increasing the expected number of active devices $K\xi_a$ directly enhances the received signal power, which suppresses the interference by aggregation gain and hence reduces the need of interference suppression via spectrum spreading.

B. Breathing Depth Optimization with GSI and CSI Feedback

Given GSI and CSI feedback, the breathing depth can be adapted over rounds and hence re-denoted as $G_n$ for round $n$. The optimization criteria is to minimize the estimate of the relevant term, $\beta_n(G_n)$, of the successful convergence probability in the Theorem 1. Let the estimate be denoted as $\hat{\beta}_n(G_n)$:

$$
\hat{\beta}_n(G_n) = \left(1 - \frac{1}{G_n}\right)\hat{\alpha}^2(n) + \frac{DP_I\hat{V}^2(n)}{G_n^2P_0|\mathcal{K}(n)|^2}.
$$

(39)
where \( \hat{\alpha}(n) \) and \( \hat{V}(n) \) are estimates of \( \alpha(n) \) and \( V(n) \), respectively, while the number of active devices, \( |K(n)| \), is perfectly known at the server from CSI. Based on feedback statistics of local gradients, the estimation is similar to that in [12] given as

\[
\hat{\alpha}^2(n) = \frac{1}{|K(n)|} \sum_{k \in K(n)} \|\mathbf{g}_k(n)\|^2, \quad \hat{V}^2(n) = \frac{1}{|K(n)|} \sum_{k \in K(n)} \hat{V}_k^2(n), \tag{40}
\]

where \( \hat{V}_k^2(n) \) is the local gradient variance:

\[
\hat{V}_k^2(n) = \frac{1}{D} \sum_{d=1}^{D} \left( [\mathbf{g}_k(n)]_d - \frac{1}{D} \sum_{d=1}^{D} [\mathbf{g}_k(n)]_d \right)^2. \tag{41}
\]

Consider an arbitrary round \( n \) of AirBreathing FL. Based on (39) and (40), the problem of optimizing the breathing depth can be formulated as

\[
\min_{G_n} \quad \hat{\beta}_n(G_n)
\]

s.t. \( G_n \in \{1, 2, \ldots, D\} \),

\[
\forall n \in \{0, 1, \ldots, N - 1\}. \tag{42}
\]

Again, by integer relaxation of \( G_n \) into \( x > 0 \), \( \nabla_x \hat{\beta}_n(x) = 0 \) yields the optimal solution \( x^*_n = \frac{2P_0D\hat{V}^2(n)}{P_I|K(n)|^2\hat{\alpha}^2(n)} \) such that \( \hat{\beta}_n(x^*_n) \) is the minimum. Then an approximate of the adaptive breathing depth is given as

\[
G^*_n = \begin{cases} 
1, & x^*_n < 1, \\
[x^*_n]_{\hat{\beta}_n(G_n)}, & 1 \leq x^*_n \leq D, \\
D, & x^*_n \geq D.
\end{cases} \tag{43}
\]

Note that the adaptive breathing depth is a clipping function of \( x^*_n \), truncated by the smallest and largest achievable value. For the general case, \( 1 \leq x^*_n \leq D \), \( G^*_n \) is found to be inversely proportional to the receive SIR \( \frac{P_0}{P_I} \), number of active devices \( |K(n)|^2 \) and estimate of gradient squared norm \( \hat{\alpha}^2(n) \). Enlarging these parameters reduces the impact of interference on convergence so that breathing depth decreases accordingly. On the other hand, the breathing depth increases with the rise of gradient-variance estimate due to the scaling of interference in de-normalization. The resultant protocol for adaptive spectrum breathing is summarized in Algorithm 1.
Algorithm 1: Adaptive Breathing Depth Protocol

**Input:** Receive SIR $P_0/P_I$, Model size $D$;

1. Initialisation: $w(0)$ in all devices;
2. for Round: $n = 0$ to $N$ do
3. for each device $k \in \mathcal{K}(n)$ in parallel do
4. Computes $g_k(n)$ via (2);
5. Computes $\|g_k(n)\|^2$ ;
6. Computes $\hat{V}_k^2(n)$ via (41);
7. Uploads $\|g_k(n)\|^2$ and $\hat{V}_k^2(n)$ to server;
8. end for
9. Server estimates $\hat{\alpha}^2(n)$ and $\hat{V}^2(n)$ via (40);
10. Server computes adaptive breathing depth $G^*_n$ via (43);
11. Server generates selected index set $\psi_n$ and set of PN sequence $\mathcal{C}(n)$ w.r.t. $G^*_n$;
12. Server broadcasts $\psi_n$ and $\mathcal{C}(n)$ to all devices;
13. **Spectrum Breathing Process** returns $w(n + 1)$
14. end for
15. return $w(n + 1)$

VII. EXPERIMENTAL RESULTS

In this section, the preceding fixed and adaptive breathing depth protocols are simulated. Based on this, we evaluate the performance of AirBreathing FL by comparing it with six benchmarks to be specified below.

A. Experimental Settings

The default experimental settings are as follows unless specified otherwise.

- **Communication Settings:** We consider an AirBreathing FL system comprising one server and 10 devices. In each round, the PN sequence shared by devices is generated by having i.i.d. chips following the unbiased Bernoulli distribution; the sequence is varied over rounds. Each chip spans unit time and a transmitted gradient coefficient occupies $G_n$ chips with $G_n$ being the breathing depth. The interference at the server’s receiver is modelled as a sequence of i.i.d Gaussian symbols. Assuming Rayleigh fading, all channel coefficients are modelled as $\mathcal{CN}(0, 1)$ random variables. Consider the scenario of strong interference. The devices’ fixed transmission power and the interference power are set such the expected receive SIR is $-23$ dB, which can be enhanced by aggregation and spectrum de-spreading in AirBreathing. Finally, the threshold of truncated channel inversion is set as $G_{th} = 0.2$ and the resultant activation probability of each device is $\xi_a = 0.82$. 

May 11, 2023 DRAFT
• **Learning Settings:** We consider the learning task of handwritten digit classification using the popular MNIST dataset. To model non-i.i.d data at devices, each of which comprises 3000 randomly drawn samples of one class. Two randomly chosen shards with different labels are assigned to each device. The task is to train a CNN model having 21,840 parameters. The model consists of two $5 \times 5$ convolutional layers with ReLU activation (with 10, 20 channels, respectively), and the ensuing $2 \times 2$ max pooling, a fully connected layer with 50 units and ReLU activation, and a final softmax output layer. Furthermore, the pruning for spectrum contraction is executed on model weights (99.8% of all parameters) but not bias to avoid divergence.

Six benchmarking schemes with their legends in brackets are described below.

• **Ideal Case:** The ideal FL system without pruning and channel distortion.

• **No Spectrum Breathing (No SB):** This is equivalent to AirBreathing FL with $G_n = 1, \forall n$. The resultant system is exposed to strong interference.

• **Pruning without Spectrum Spreading:** Gradients are pruned randomly with a fixed ratio, $\gamma$, and uploaded without spread spectrum. This results in the exposure of pruned gradients to strong interference.

• **Convergent OTA FL (COTAF) [25]:** Given the same power constraint and interference, time-varying scalar precoding (equivalent to power control) with full-dimensional gradient uploading is simulated by accounting for the gradually decreasing squared norm of gradient over rounds. Note that COTAF requires offline simulation to estimate the scalar precoder, while AirBreathing FL does not need this as a result of online estimation from GSI feedback with negligible communication overhead.

• **Optimal Fixed Breathing Depth (Optimal fixed BD):** The optimal fixed breathing depth is obtained using an exhaustive search, as opposed to using the closed-form result in (38).

• **AirBreathing with Importance-aware Pruning (AirBreathing with IP):** Random pruning is replaced with importance-aware pruning, namely pruning gradient coefficients with the smallest magnitudes. The difficulty in its implementation is overcome by alternating rounds of 1) full-gradient uploading to allow the devices to select from aggregated gradient coefficients an index subset to prune in the next round and 2) using the subset to perform importance-aware pruning at devices assuming temporal correlation in gradients [32].
B. Performance of AirBreathing FL

The learning performance of AirBreathing FL is compared with the benchmarking schemes. For spectrum breathing, both the schemes of fixed and adaptive breathing depth are considered. The curves of validation accuracy versus communication time are plotted in Fig. 3 (a). Several observations can be made. First, AirBreathing in both the cases of fixed and adaptive breathing depth achieves convergence. This demonstrates its effectiveness in coping with strong interference. On the contrary, FL without spectrum breathing, which suffers from strong interference, fails to converge. Second, there exists a substantial performance gap between the scheme of fixed breathing depth from the ideal case due to approximation in the former design to obtain the closed-form result. Thus the gap is largely removed using the proposed scheme of adaptive breathing depth. Finally, AirBreathing with adaptive depth is observed to approach the ideal case within a reasonable performance gap. In particular, the converged accuracy for the former is 96.2% and 94.6% for the latter.

Fig. 3 (b) compares the performance of pruning without spectrum spreading and AirBreathing FL. One can see the former has a rapid increase in accuracy at the beginning, as a result from a higher communication rate in the absence of spectrum spreading. However, the corruption of gradients by interference eventually takes its toll and leads to unsuccessful learning. In contrast, despite a slower learning speed initially, AirBreathing FL ensures steady increase in accuracy to achieve convergence.

Fig. 4 (a) compares the performance between COTAF and adaptive AirBreathing FL in coping...
with strong interference. Several observations can be made. When subjected to the same power constraints, COTAF avoids divergence by gradually increasing transmit power. Despite this, COTAF still struggles to achieve a high accuracy due to the discussed limitation of power control in suppressing interference. In contrast, adaptive AirBreathing FL achieves a significantly higher accuracy after convergence, albeit with a slower learning speed at the beginning, thanks to its interference-suppression capability.

C. Random Pruning versus Importance-aware Pruning

In Fig. 4 (b), we compare the learning performance of AirBreathing FL using the proposed random pruning with that of the benchmarking scheme using importance-aware pruning. The main observation is that the latter does not yield any performance gain over the proposed scheme. The reasons are two drawbacks of the importance-aware scheme. First, the full-gradient uploading in every other round in the benchmarking scheme increases communication overhead. Second, the pruned gradient coefficients in a round are selected based on those in the preceding round, resulting in inaccurate choices as gradients vary over rounds.

D. Effects of Network Parameters

We study the effects of two key network parameters, namely the number of devices and the receive SIR per device, on the learning performance of AirBreathing FL for a given communication time of $7 \times 10^6$ chips. To this end, the curves of validation accuracy versus varying network parameters are plotted in Fig. 5.
Fig. 5. The effects of (a) number of devices and (b) receive SIR on the learning performance for given communication time of $7 \times 10^6$ chips.

From Fig. 5(a), one can see the continuous performance improvement as the number of devices increases, as the AirComp’s aggregation over devices suppresses interference by averaging. Note that AirBreathing realizes interference suppression using a different mechanism of spread spectrum. On the other hand, as expected, the AirBreathing FL with either fixed or adaptive breathing depth sees growing performance improvement as the receive SIR per device (before aggregation) becomes larger.

VIII. CONCLUSION

In this work, we presented a spectrum-efficient method, called spectrum breathing. Leveraging the graceful degradation of learning performance due to pruning, the method exploits signal spectrum contraction via pruning to enable interference suppression via spread spectrum without requiring extra bandwidth. The breathing depth that controls spectrum contraction level is optimized and adapted to both the states of gradient descent and channels to amplify the learning performance gain.

This work establishes a new principle of designing robust AirFL by integrating gradient pruning and interference suppression. Beyond spread spectrum, this principle can be applied to other interference management techniques such as adaptive coding and modulation, MIMO beamforming, and cooperative transmission. The current AirBreathing FL method can also be generalized to more complex systems such as multi-cell or distributed AirFL. Practical issues such as synchronization errors and security warrant further investigation.
APPENDIX

A. Proof of Lemma 2

In this section, the AirComp error of AirBreathing FL using random pruning is derived as below. For the expression brevity, the round index $n$ is omitted in the following equations.

First, the AirComp error of AirBreathing FL, denoted as $\text{MSE}(n)$, is the MSE between received signal $y'(n)$ and the ideal version $\frac{1}{|K(n)|} \sum_{k \in K(n)} g_k(n)$, given as

$$\text{MSE}(n) = \mathbb{E} \left[ \left\| \frac{1}{|K|} \sum_{k \in K} g_k - y' \right\|^2 \right]$$

$$= \mathbb{E}_{\psi_n} \left[ \left\| \frac{1}{|K|} \sum_{k \in K} g_k - R \left( \frac{1}{|K|} \sum_{k \in K} g_k \right) \right\|^2 \right] + \mathbb{E}_{\tilde{z}} \left[ \left\| R(\tilde{z}) \right\|^2 \right]$$

$$(a) = \mathbb{E}_{\psi_n} \left[ \left\| \frac{1}{|K|} \sum_{k \in K} g_k - R \left( \frac{1}{|K|} \sum_{k \in K} g_k \right) \right\|^2 \right] + \frac{S_n P_I}{G_n P_0} \mathbb{E} \left[ \frac{V^2}{|K|^2} \right]$$

$$(b) = \left(1 - \frac{S_n}{D}\right) \mathbb{E} \left[ \left\| \frac{1}{|K|} \sum_{k \in K} g_k \right\|^2 \right] + \frac{S_n P_I}{G_n P_0} \mathbb{E} \left[ \frac{V^2}{|K|^2} \right]$$

$$= (1 - \gamma_n) \mathbb{E}[\alpha^2(n)] + \frac{\gamma_n D P_I}{G_n P_0} \mathbb{E} \left[ \frac{V^2}{|K|^2} \right],$$

where the expectation is taken over $\psi_n$ and $\tilde{z}(n)$. (a) is derived from the sum power of $S_n$ i.i.d zero mean Gaussian random variables. (b) is derived from the expectation of $\psi_n$ that is chosen at random from $\Omega_n$. That is, for a generic vector $x \in \mathbb{R}^D$, the MSE between $x$ and $R(x)$ over $\psi_n$ can be represented as [42],

$$\mathbb{E}_{\psi_n}[\|x - R(x)\|^2] = \frac{1}{|\Omega_n|} \sum_{\psi_n \in \Omega_n} \sum_{d=1}^D |x|^2 \mathbb{I}\{d \notin \psi_n\} = \sum_{d=1}^D |x|^2 \sum_{\psi_n \in \Omega_n} \frac{\mathbb{I}\{d \notin \psi_n\}}{|\Omega_n|}$$

$$= \sum_{d=1}^D |x|^2 \frac{(D-1)}{S_n} = (1 - \frac{S_n}{D}) \|x\|^2 = (1 - \gamma_n) \|x\|^2. \tag{45}$$

(b) trivially holds by replacing $x$ of (45) with $\frac{1}{|K|} \sum_{k \in K} g_k$.

The proof of Lemma 2 is completed.
Consider round \( n \), the gap between vanilla SGD and AirBreathing FL is upper bounded as

\[
\mathbb{E} \left[ \left\| \frac{1}{K} \sum_{k=1}^{K} g_k(n) - y'(n) \right\| \right] = \mathbb{E} \left[ \left\| \frac{1}{K} \sum_{k=1}^{K} g_k - \frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} g_k + \frac{1}{|\mathcal{K}|} \sum_{k \not\in \mathcal{K}} g_k - y' \right\| \right]
\]

\[
\leq \mathbb{E} \left[ \left\| \frac{1}{K} \sum_{k=1}^{K} g_k - \frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} g_k \right\| \right] + \mathbb{E} \left[ \left\| \frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} g_k - y' \right\| \right]
\]

\[
\leq \mathbb{E} \left[ \left\| \frac{1}{K} \sum_{k=1}^{K} g_k - \frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} g_k \right\| \right] + \sqrt{\text{MSE}(n)},
\]

where \((c)\) comes from Jensen’s inequality on concave function \(\sqrt{\cdot} \); \(\nu(n)\) is upper bounded as

\[
\nu(n) \leq \mathbb{E} \left[ \left\| \frac{1}{K} \sum_{k=1}^{K} g_k - \frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} g_k \right\| \right] = \mathbb{E} \left[ \left\| \frac{|\mathcal{K}| - K}{K|\mathcal{K}|} \sum_{k \in \mathcal{K}} g_k + \frac{1}{K} \sum_{k \not\in \mathcal{K}} g_k \right\| \right]
\]

\[
\leq \sqrt{\mathbb{E}_g \left[ \left\| \frac{|\mathcal{K}| - K}{K|\mathcal{K}|} \sum_{k \in \mathcal{K}} g_k + \frac{1}{K} \sum_{k \not\in \mathcal{K}} g_k \right\|^2 \right]} \leq \sqrt{\text{MSE}(n)},
\]

where \((d)\) is due to that \(|\mathcal{K}|\) subjects to binomial distribution \(B(K, \xi_a)\) such that the inequality below holds \([43]\):

\[
\mathbb{E} \left[ \frac{1}{|\mathcal{K}|} \right] \leq \frac{2}{K \xi_a}, \quad \mathbb{E} \left[ \frac{1}{|\mathcal{K}|^2} \right] \leq \frac{6}{K^2 \xi_a^2}.
\]

The proof of Lemma is completed.

We consider the process defined as follows

\[
U_n(w(n), \ldots, w(0)) \triangleq W_n(w(n), \ldots, w(0)) - \eta H \sum_{i=0}^{n-1} u(i),
\]
where \( u(i) \) is given in Lemma 3 and global model is updated using (19). When the algorithm has not entered the success region at round \( n \), we have \( \forall n \geq 0, \)

\[
U_{n+1}(w(n+1), \ldots, w(0)) = W_{n+1}(w(n) - \eta y'(n), w(n), \ldots, w(0)) - \eta H \sum_{i=0}^{n} u(i)
\]

\[
\leq W_{n+1} \left( w(n) - \eta \frac{1}{K} \sum_{k=1}^{K} g_k(n), w(n), \ldots, w(0) \right)
\]

\[
+ \eta H \left\| \frac{1}{K} \sum_{k=1}^{K} g_k(n) - y'(n) \right\| - \eta H \sum_{i=0}^{n} u(i),
\]

where the scaling up results from the \( H \)-Lipschitz smooth in the first coordinate given in (25).

Then we take the expectation for both sides of the inequality and use the supermartingale property of \( W_n \). The expectation of \( U_{n+1} \) is bounded by

\[
\mathbb{E}[U_{n+1}(w(n+1), \ldots, w(0))] 
\]

\[
\leq \mathbb{E} \left[ W_{n+1} \left( w(n) - \eta \frac{1}{K} \sum_{k=1}^{K} g_k(n), w(n), \ldots, w(0) \right) \right]
\]

\[
+ \eta H \mathbb{E} \left[ \left\| \frac{1}{K} \sum_{k=1}^{K} g_k(n) - y'(n) \right\| \right] - \eta H \sum_{i=0}^{n} \mathbb{E}[u(i)]
\]

\[
\leq W_n(w(n), \ldots, w(0)) + \eta H u(n) - \eta H \sum_{i=0}^{n} u(i) = U_n(w(n), \ldots, w(0)).
\]

The inequality above still holds in the case when the algorithm has succeeded at round \( n \). Thus, \( U_n \) is a supermartingale process for AirBreathing FL.

Proof of Lemma 4 is completed.

**D. Proof of Theorem 5**

We denote the failure to enter the success region by \( N \) as \( F_N \), otherwise, the success as \( \neg F_N \).

Consider the same model initialization \( w(0) \) for \( U_n \) and \( W_n \), we have

\[
\mathbb{E}[W_0] = \mathbb{E}[U_0] \geq \mathbb{E}[U_n] = \mathbb{E}[U_n|F_N] \Pr\{F_N\} + \mathbb{E}[U_n|\neg F_N] \Pr\{\neg F_N\}
\]

\[
\geq \mathbb{E}[U_n|F_N] \Pr\{F_N\} = \left( \mathbb{E}[W_N|F_N] - \eta H \sum_{n=0}^{N-1} u(n) \right) \Pr\{F_N\}
\]

\[
\geq \left( N - \eta H \sum_{n=0}^{N-1} u(n) \right) \Pr\{F_N\}.
\]

May 11, 2023 DRAFT
Hence, we obtain

$$\Pr\{F_N\} \leq \frac{\mathbb{E}[W_0]}{N - \eta H \sum_{n=0}^{N-1} u(n)},$$

where $\mathbb{E}[W_0]$ can be obtained by setting $n = 0$ in (24) and taking expectation.

Proof of theorem 5 is completed.

E. Proof of Lemma 6

The round index is omitted for expression brevity. By taking the expectation over the gradient and number of active devices, the upper bound of $\mathbb{E}[\alpha^2(n)]$ is given as

$$\mathbb{E}[\alpha^2(n)] = \mathbb{E}\left[\left\| \frac{1}{|K|} \sum_{k \in K} g_k \right\|^2 \right] \leq \mathbb{E}\left[ \left\| g \right\|^2 + \frac{\sigma_g^2}{|K|} \right] \leq \mathbb{E}\left[ \left\| g \right\|^2 + \frac{2\sigma_g^2}{K \xi_a} \right] \leq \left\| g \right\|^2 + \sigma_g^2,$$

where $(e)$ trivially holds when no less than 2 devices are expected to be active at each round such that $K \xi_a \geq 2$. By taking the expectation over selected element set $\psi_n$, $\mathbb{E}[V^2(n)]$ is upper bounded as below:

$$\mathbb{E}[V^2(n)] = \mathbb{E}\left[ \frac{1}{|K|} \sum_{k \in K} V_k^2 \right] = \mathbb{E}[V_k] = \mathbb{E}\left[ \frac{1}{S_n} \sum_{s=1}^{S_n} (|g^c|_s - M_k)^2 \right]$$

$$= \mathbb{E}\left[ \frac{1}{S_n} \sum_{s=1}^{S_n} |g^c|_s^2 - M_k^2 \right] \leq \mathbb{E}\left[ \frac{1}{S_n} \sum_{s=1}^{S_n} |g^c|_s^2 \right]$$

$$= \frac{1}{D} \sum_{d=1}^{D} (g_k)_d^2 \frac{D}{S_n} \sum_{\psi_n \in \Omega_n} \frac{I\{d \in \psi_n\}}{|\Omega_n|} = \frac{1}{D} \left\| g_k \right\|^2 \frac{D}{S_n} \left( \frac{D-1}{S_n} \right) = \frac{1}{D} \left\| g_k \right\|^2 \leq \frac{1}{D} (\left\| g \right\|^2 + \sigma_g^2),$$

where $M_k = \frac{1}{S_n} \sum_{s=1}^{S_n} |g^c|_s^2$ is the mean of local sparse gradient. Building on the analysis above, $\mathbb{E}[\alpha^2(n)] \leq D \Gamma(n)$ and $\mathbb{E}[V^2(n)] \leq \Gamma(n)$ holds if the upper bound of GSI is chosen as $\Gamma(n) \geq \frac{1}{D} (\left\| g \right\|^2 + \sigma_g^2)$. Last, the upper bound for CSI can be simply obtained by (48).

Proof of Lemma 6 is completed.

REFERENCES


