Robust Over-the-Air Computation with Type-Based Multiple Access

Marc Martinez-Gost*†, Ana Pérez-Neira*†‡, Miguel Ángel Lagunas†
*Centre Tecnològic de Telecomunicacions de Catalunya, Spain
†Dept. of Signal Theory and Communications, Universitat Politècnica de Catalunya, Spain
‡ICREA Acadèmia, Spain
{mmartinez, aperez}@cttc.es

***Abstract*—This paper utilizes the properties of type-based multiple access (TBMA) to investigate its effectiveness as a robust approach for over-the-air computation (AirComp) in the presence of Byzantine attacks, this is, adversarial strategies where malicious nodes intentionally distort their transmissions to corrupt the aggregated result. Unlike classical direct aggregation (DA) AirComp, which aggregates data in the amplitude of the signals and are highly vulnerable to attacks, TBMA distributes data over multiple radio resources, enabling the receiver to construct a histogram representation of the transmitted data. This structure allows the integration of classical robust estimators and supports the computation of diverse functions beyond the arithmetic mean, which is not feasible with DA. Through extensive simulations, we demonstrate that robust TBMA significantly outperforms DA, maintaining high accuracy even under adversarial conditions, and showcases its applicability in federated learning (FEEL) scenarios. Additionally, TBMA reduces channel state information (CSI) requirements, lowers energy consumption, and enhances resiliency by leveraging the diversity of the transmitted data. These results establish TBMA as a scalable and robust solution for AirComp, paving the way for secure and efficient aggregation in next-generation networks.**

I. Introduction

The advent of highly complex and heterogeneous networks has created an urgent need for high-speed data transfer protocols capable of handling massive data volumes while enabling real-time processing and data-driven decision-making. To address these demands, future communication networks must integrate distributed computation directly into the communication process, as seen in applications like Artificial Intelligence (AI), which require continuous aggregation of vast data from distributed devices to train and update models. These massive data flows call for efficient and scalable techniques, such as over-the-air computation (AirComp), which leverages the waveform superposition property of wireless channels to aggregate data directly over the air. By aligning simultaneous transmissions to compute a desired function of the transmitted signals, AirComp minimizes latency and radio resource usage, making it particularly relevant for large-scale distributed systems like wireless sensor networks and federated learning (FEEL), where high-speed data aggregation is crucial.

While AirComp offers significant advantages in terms of efficiency and scalability, it also introduces critical security concerns [1]. Since the receiver does not access individual device transmissions, AirComp inherently preserves privacy, which is a desirable feature in many applications. However, this same characteristic makes it challenging to identify malicious behavior, as the aggregated result conceals individual contributions. Consequently, AirComp is particularly vulnerable to Byzantine attacks, where adversaries deliberately manipulate their transmissions to corrupt the aggregated outcome. Addressing these vulnerabilities is essential to ensure the robustness and reliability of AirComp in adversarial environments.

The existing literature on Byzantine attacks and outlier detection in distributed computing has largely focused on general frameworks [2], with limited attention to their application in AirComp. The only proposed solution under the AirComp framework is presented in [3], where the authors introduce an algorithm operating between the physical and link layers. Specifically, devices are divided into subsets, which transmit data concurrently within each group. Then, the geometric median across groups is computed as a robust estimate of the mean. However, this approach is limited to FEEL scenarios and only considers the computation of the arithmetic mean. Additionally, the algorithm is not fully in the physical layer, as it requires scheduling transmissions among users. Another line of research explores robust precoders for AirComp [4]–[7], addressing channel imperfections by accounting for channel uncertainty in a probabilistic sense. However, these works do not address resiliency to adversarial attacks, leaving a critical gap in the robustness of AirComp.

All previous works on AirComp operate under a direct aggregation (DA) framework, where the additive property of the wireless channel is used to achieve superposition, resulting in the receiver obtaining a single aggregated signal. To achieve resiliency against attacks with DA in the physical layer, the function estimate has to be robust. However, the performance is heavily dependent on the data distribution and the nature of the attacks, limiting their effectiveness.

In this work, we propose leveraging a type-based multiple access (TBMA) for AirComp instead. In TBMA, devices transmit in a single radio resource (i.e., time, frequency or code) according to their data, allowing the receiver to construct a histogram representation of the transmitted data. It has been previously shown the benefits of TBMA over DA in terms of power consumption and channel state information (CSI) [1].

This work is part of the project SOFIA PID2023-147305OB-C32 funded by MICIU/AEI/10.13039/501100011033 and FEDER/UE.

In this work we show that the diversity provided by multiple radio resources can be exploited at the receiver to identify and isolate attacks targeting specific resources. Moreover, TBMA supports a broader range of function computations compared to DA, as it decouples the attack detection and compensation from the function computation.

The contributions of this work are as follows:

1) We propose a novel physical-layer framework for robust aggregation in TBMA-based AirComp, enhancing resilience against adversarial attacks.
2) TBMA enables the integration of both parametric and non-parametric estimators, providing flexibility and generality.
3) Unlike most works that assume the sample average, our scheme allows the computation of robust estimates for a variety of functions, which we evaluate.
4) We compare TBMA with DA and demonstrate the effectiveness of robust aggregation with TBMA in a FEEL use case, highlighting its practical applicability.

The remaining part of the paper proceeds as follows: Section II introduces aggregation techniques for AirComp and presents the system model. Section III introduces robust techniques for TBMA and section IV assesses their performance in different scenarios. Section V concludes the paper.

II. System Model

Consider a wireless network with K distributed devices (i.e., transmitters) and a single server (i.e., receiver). Each device $k \in \mathcal{K}$ has local data s_k (e.g., sensor measurements or local computations) and the goal of the network is to compute a function of the data $f(s_1, \dots, s_K)$. For this purpose, AirComp is exploited to efficiently use the communication resources.

The traditional approach for AirComp is encoding the information in the amplitude of the transmitted waveform. Assuming perfect synchronization and channel compensation, the additive nature of the wireless channel aggregates the signals at the input of the receiver. To compute the sample average, the receiver only needs to divide the amplitude of the received waveform by the number of transmitters. To compute other functions, the transmitters and receiver need to process the transmitted and received signals, respectively, a procedure termed nomographic function representation [8]. These techniques, either analog or digital, fall under the umbrella of DA, as the aggregation occurs over a single communication resource. Alternatively, for robust AirComp we propose using TBMA.

A. Type-based multiple access

In TBMA [9] there is a one-to-one mapping between L different measurements and L orthogonal radio resources. For the sake of simplicity we assume that $s_k \in [1, \dots, L]$, which can be achieved via linear or nonlinear mappings (e.g., quantization). Thus, in TBMA, radio resources are allocated according to data, not users, enabling superposition when users have the same measurement. The signal transmitted by user k is $\varphi(s_k)$. For instance, in (1), TBMA can be implemented with M-ary frequency shift keying (FSK) when there is a bijective mapping between data and frequency resources; alternatively, TBMA can be implemented with pulse position modulation (PPM), where there is a bijective mapping between the data and the time shifts of a pulse.

$$\varphi(s_k) = \begin{cases} a_k e^{j2\pi s_k n/T} & \text{for } M\text{-FSK} \\ a_k e^{j2\pi (n-s_k)/T} & \text{for PPM} \end{cases} \tag{1}$$

In (1), T is the duration of the signal and $n = 0, \dots, N-1$ is the discrete time index. The amplitude $a_k \in \mathcal{C}$ is used to compensate channel imperfections. Although these are two examples of how TBMA can be implemented, this technique always requires an orthogonal support of signals. Furthermore, notice that each user uses a single from the L available radio resource.

At the receiver side, the signal at resource $\ell \in [1, \dots, L]$ is

$$y_\ell = \sum_{k \in \mathcal{K}} h_{k\ell} \varphi(s_k) + w_\ell, \tag{2}$$

where $h_{k\ell} \in \mathcal{C}$ is the channel between user k and the receiver at resource ℓ, and w_ℓ is the additive white Gaussian noise (AWGN) sample at resource ℓ with power σ^2. Notice that $\varphi(s_k) \neq 0$ only when $s_k = \ell$. We assume perfect CSI, which can be achieved via channel inversion as $a_k = h_k^*/|h_k|^2$. We refer the reader to [9] for the consideration of channel knowledge and effects on error estimation, as the purpose of this paper is to show how TBMA provides robustness towards Byzantine attacks. Additional techniques for channel compensation can be designed on top of the proposed design.

Computing the matched filter for the set of y_ℓ and normalizing by K results in

$$\mathbf{r} = \frac{1}{K}[K_1, \dots, K_L]^T + [\tilde{w}_1, \dots, \tilde{w}_L]^T = \mathbf{p} + \tilde{\mathbf{w}}, \tag{3}$$

where the ℓ-th entry in $\mathbf{p}$ corresponds to the fraction of devices K_ℓ/K that transmitted at resource ℓ (i.e., $s_k = \ell$) and $\tilde{w}_\ell$ is Gaussian noise with power $\tilde{\sigma}^2 = \sigma^2/K^2$. Provided that $K > L$, which is reasonable in AirComp scenarios, $\mathbf{r}$ corresponds to a nosy version of the empirical measure $\mathbf{p}$, this is, a histogram or type of the distributed data s_k.

From the noisy type $\mathbf{r}$, many of the functions of interest can be computed by aggregating the L signals with an aggregation function Ψ. For instance,

$$\Psi(\mathbf{r}) = \begin{cases} \frac{1}{K}\sum_{\ell=1}^{L} \ell r_\ell & \text{for arithmetic mean} \\ \exp\left(\frac{1}{K}\sum_{\ell=1}^{L} r_\ell \ln \ell\right) & \text{for geometric mean} \end{cases} \tag{4}$$

As mentioned previously, amplitude-based AirComp requires non-linear pre-processing and post-processing to compute functions beyond the arithmetic mean. Conversely, TBMA computes the function over the type $\mathbf{r}$. Besides (4), other functions such as the minimum or maximum reduce to classical detection problems for TBMA. Furthermore, from the communication perspective, one of the most relevant benefits of TBMA over DA is the saving in energy consumption. For instance, to compute the geometric mean with DA, each device transmits $\ln(s_k)$, which may have a large impact in the transmitted power. Conversely, as shown in (4), TBMA only chooses the radio resource and the transmitted power is independent of the function.

The figure of merit is the normalized mean squared error (NMSE) between the distributed data and the function estimated at the receiver side:

$$\text{NMSE} = \frac{|f(s_1, \dots, s_K) - \Psi(r_1, \dots, r_L)|^2}{f(s_1, \dots, s_K)^2} \tag{5}$$

B. Byzantine attacks

In a Byzantine attack there is a set of users that try to corrupt the aggregation by sending malicious data. In the context of AirComp and, particularly, in TBMA we define a set of users $\mathcal{M}$ that attack a specific radio resource to alter the distribution of $\mathbf{p}$. We assume that the attackers are coordinated to attack the same radio resource $\tilde{\ell}$, which represents the worst case scenario in terms of (5). We define the received signal in the presence of attackers as

$$\tilde{y}_\ell = \sum_{k \in \mathcal{K}} h_{k\ell} \varphi(s_k) + \sum_{m \in \mathcal{M}} h_{m\ell} \varphi(\ell) + w_\ell, \tag{6}$$

and the corrupted type as

$$\tilde{\mathbf{r}} = \frac{1}{K}[K_0, \dots, K_{L-1}]^T + \frac{1}{K}[0, \dots, M_{\tilde{\ell}}, \dots, 0]^T + \tilde{\mathbf{w}}, \tag{7}$$

where $M_{\tilde{\ell}}$ is the number of attackers at resource $\tilde{\ell}$. Without loss of generality we assume that $M \leq K$, as allowing the number of attackers to exceed the number of legitimate devices would result in most of the data being controlled by attackers, leading to a completely compromised system. Although not considered in this work, attackers can be more severe if they adjust the transmission power (e.g., $|a_m|^2 = P_{max}$, this is, transmitting at maximum power).

III. Robust techniques for TBMA

The additional consumption of wireless resources of TBMA with respect to DA —in fact, by a factor of L— provides more information at the receiver side. According to (7), when the number of attackers is small, we have $\tilde{\mathbf{r}} \approx \mathbf{r}$ and the NMSE is mostly affected by channel noise. Conversely, when the number of attackers is large, radio resource $\tilde{\ell}$ can be easily spotted due to the structure imposed by TBMA. We will use this information to provide detection and compensation techniques against Byzantine attacks. Notice that this robustness is not only limited to attacks, but also to any abnormal alternation in the amplitude of the received type, such as channel fading. We leave the extension beyond attacks for future work.

Assume, without loss of generality, f to be the arithmetic mean. Given $\mathbf{p}$ with an arbitrary distribution, attackers need to select an adequate resource $\tilde{\ell}$ to displace the mean. This implies that $\tilde{\ell} \leq \min s_k$ or $\tilde{\ell} \geq \max s_k$ are suitable candidates. However, in TBMA, these attacks are very easy to detect over $\tilde{\mathbf{r}}$ because they represent outliers in the data distribution. Thus, robust estimation over TBMA reduces to the classical signal processing problem of outlier detection and robust estimation over data distributions. Many off-the-shelf techniques can be used to provide robustness. In the following we list a few:

- *Robust estimators*: for instance, the median is a non-parametric robust estimator of the arithmetic mean.
- *Percentile truncation*: keeping only the data in a certain percentile range removes extreme outliers.
- *Resampling techniques*: methods like bootstrapping or RANSAC [10] resample the data several times to robustly estimate the underlying distribution.

The purpose of this paper is not to provide a superior robust algorithm for TBMA, but to show that classical techniques can be implemented over TBMA. We define $\hat{\mathbf{r}}$ as the corrected type and we present an approach for robust estimation over TBMA that integrates several techniques in Algorithm 1. First, we threshold the type below the noise level (e.g., $\theta_1 = 3\sigma^2$); then, percentile truncation is designed to remove extreme outliers that lie far outside the main distribution of the data. We define P_1 and P_2 as the low and high percentiles of $\tilde{\mathbf{r}}$, respectively. The last step targets outliers that are not far from the overall data range but deviate significantly from their local context (i.e., their immediate neighbors). Under the assumption that a single resource is attacked, we identify values that are much larger than both their preceding and succeeding neighbors. Instead of removing these points, we compensate for their effect by replacing them with the average of their adjacent values. This ensures smoother transitions in the data while preserving the overall structure of the distribution. These operations can be executed in parallel across the L radio resources, ensuring an efficient scaling with the number of resources.

From the corrected type $\hat{\mathbf{r}}$, the desired function can be estimated using the aggregation function $f \approx \Psi(\hat{\mathbf{r}})$. However, note that some information from non-attackers transmitting on resource $\tilde{\ell}$ may be lost from the non-attackers that were transmitting at the attacked resource. Unlike DA, where the design of robust estimation is inherently coupled with the specific function being computed, TBMA decouples attack detection and compensation from function computation. For instance, with DA, a robust estimator for the arithmetic mean might be the median, requiring pre-processing and post-processing steps that are tightly linked to the mean computation. In contrast, TBMA makes the outlier removal independent from the function estimation. This decoupling enables TBMA to support the computation of multiple functions from a single transmission, offering greater flexibility compared to DA methods.

It is critical to emphasize that the design of this algorithm and the corresponding parameters must be tailored to the specific distribution of $\mathbf{p}$. Additionally, the algorithm must account for the nature of potential attacks on the aggregation process. For example, if the attack strategy injects subtle but coordinated outliers within the main distribution, step 3 (local outlier compensation) becomes vital. Conversely, if the attack introduces extreme values far from the distribution, step 2 (percentile truncation) is more critical. By adapting the algorithm to both the data distribution and the anticipated attack strategies, it can robustly ensure the integrity of the aggregated results.

The authors in [3] tackle the problem of robust aggre-

Algorithm 1: Robust estimation over TBMA

Input: $\tilde{\mathbf{r}}$, θ_1, θ_2, P_1 and P_2

Output: $\Psi(\hat{\mathbf{r}})$

1. Threshold the noise:
$$\hat{r}_\ell = \begin{cases} \tilde{r}_\ell & \text{if } |\tilde{r}_\ell| \geq \theta_1 \\ 0 & \text{if } |\tilde{r}_\ell| < \theta_1 \end{cases}$$
2. Percentile truncation:
$$\hat{r}_\ell = \begin{cases} \tilde{r}_\ell & \text{if } P_1 \leq \tilde{r}_\ell \leq P_2 \\ 0 & \text{otherwise} \end{cases}$$
3. Outlier detection:
$$\hat{r}_\ell = \begin{cases} \tilde{r}_\ell & \text{if } |\tilde{r}_\ell - \tilde{r}_{\ell-1}| \leq \theta_2 \\ & \text{and } |\tilde{r}_\ell - \tilde{r}_{\ell+1}| \leq \theta_2, \\ \frac{\tilde{r}_{\ell-1}+\tilde{r}_{\ell+1}}{2} & \text{otherwise.} \end{cases}$$
4. Function estimation: $f \approx \Psi(\hat{\mathbf{r}})$

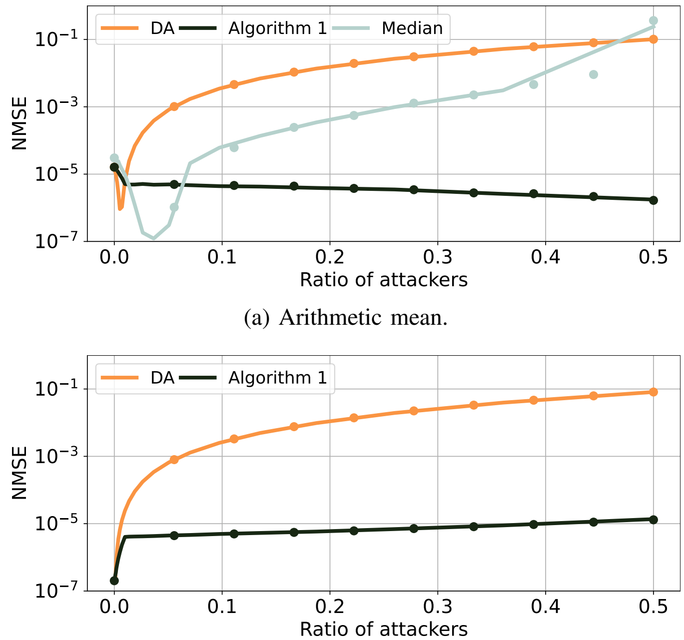
gation in amplitude-based AirComp, which aligns with the general framework of TBMA. In their approach, devices are grouped into clusters to disperse the attackers, with each group transmitting concurrently using DA at different time steps. The resulting aggregations are robustly averaged using the geometric median. Notice that assigning different transmission times to groups is simply an orthogonal radio allocation, similar to what is done in TBMA. The key distinction lies in how radio resources are assigned: in [3], this is done randomly, whereas in TBMA, it is based on the data. Moreover, the structure set by TBMA allows compensating a greater number of attackers.

IV. Results

A. Comparison of TBMA with DA

In Figure 1 we evaluate different AirComp techniques for different functions and data distributions under the influence of Byzantine attacks. We focus on the arithmetic mean, which serves as the classical function in AirComp and is widely used in aggregation tasks. Additionally, we compute the geometric mean as an example of an alternative function that is not present in the literature. To ensure adequate density for TBMA to represent data distributions effectively, the setup includes $K = 10^4$ devices and $L = 256$. In the succeeding section we will showcase TBMA in a low density scenario. Different ratios of attackers are tested, and results are averaged over 10^3 independent experiments.

Three methods are compared in the evaluation. The first is DA, which aggregates all received signals without applying any robust estimation, making it highly vulnerable to attacker influence. We do not include any robust variations of DA because no physical layer technique exists that can inherently provide robustness, even for the arithmetic mean. The second approach is the robust TBMA of Algorithm 1, for which we set $\theta_1 = 3\sigma^2, \theta_2 = 5, P_1 = 0.01$ and $P_2 = 0.99$. The third



(a) Arithmetic mean.

(b) Geometric mean.

Fig. 1: NMSE for different AirComp techniques at SNR = 30 dB (lines) and 5 dB (markers).

method computes the median from the TBMA type, which serves as a robust estimate of the arithmetic mean. However, this approach is specific to the arithmetic mean and cannot be easily generalized to other functions. Notably, computing the median with DA is not straightforward. The underlying modulation for DA is double sideband (DSB) modulation, while for TBMA is PPM, and we consider an AWGN channel.

As shown in Figure 1, the results are consistent across different signal-to-noise ratio (SNR) regimes, as the large number of signal aggregations provides robustness against channel noise. Regarding the attacks, DA is not robust, and the error increases with the number of attackers for all functions. TBMA with the median function is more robust than DA, but the NMSE still increases with the number of attackers. This emphasizes the need for robust AirComp techniques, not just robust function estimates. In this respect, Algorithm 1 is resilient to attacks, and the error does not increase significantly with the ratio of attackers. For the arithmetic mean, the NMSE even decreases because it is easier to detect outliers in the type. This effect is not observed in the geometric mean, as it involves nonlinear transformations.

B. FEEL use case

FEEL is a distributed approach where multiple devices collaboratively train a global model by sharing model updates (e.g., gradients in a neural network), instead of raw data. AirComp complements FEEL by using the superposition property of the wireless channel to perform aggregation directly during transmission. This eliminates the need for separate aggregation at the receiver, reducing communication overhead and latency.

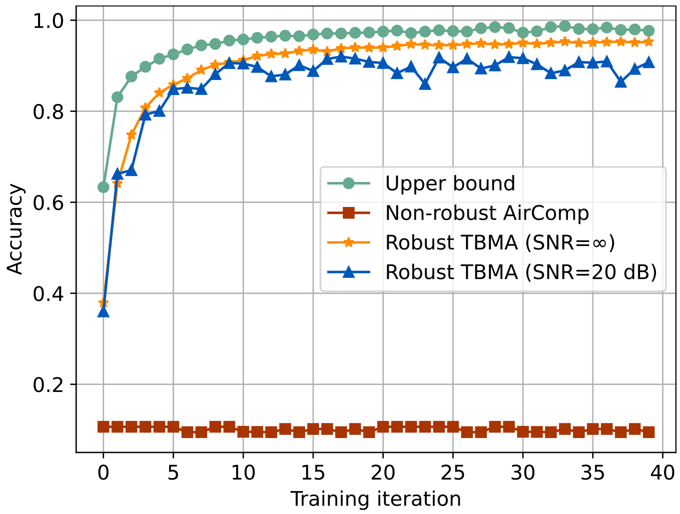


Fig. 2: Test accuracy across training for an AirComp-based FEEL system under Byzantine attacks.

We consider the deployment of a FEEL system in which a server coordinates the learning process of $K = 50$ devices. The task is image classification using the MNIST dataset [11], consisting in images of handwritten digits ranging from 0 to 9. The learning model consists in a classical convolutional neural network (CNN) (see [12]) and deployed with the Flower framework [13]. Each device trains a local CNN with a portion of the data and sends the parameters after each epoch. For transmission, each parameter is quantized, modulated with M-FSK and transmitted in a TBMA fashion. The receiver receives a type for each parameter and computes the arithmetic mean. Notice that an orthogonal set of resources is required for every parameter. We consider 6% of the devices ($M = 3$) to generate Byzantine attacks and the figure of merit is the accuracy, this is, the number of correctly classified samples.

Figure 2 shows the convergence of the AirComp-assisted FEEL system. The upper bound represents the system trained in a noiseless channel and without attacks. In practice, even a small number of attackers is enough to corrupt the system and prevent convergence. DA (i.e., non-robust AirComp) achieves only 10% accuracy, equivalent to random guessing given 10 classes. In contrast, robust TBMA performs almost as good as the non-attacked system in the noiseless scenario. The performance is slightly below the baseline due to information loss from devices sharing resources with attackers. At high SNR, robust TBMA maintains strong performance, as M-FSK proves more resilient than PPM, thanks to the frequency-based nature of the modulation.

V. Conclusion

This paper presents the first physical-layer robust aggregation method for AirComp under Byzantine attacks. Unlike classical DA techniques, which aggregate data in the amplitude domain, we propose using TBMA, where orthogonal radio resources are allocated to different data, not transmitters. With TBMA, the receiver obtains a histogram of the transmitted data, enabling straightforward detection of attacks. TBMA allows the integration of classical robust estimators and outlier detection methods, extending beyond the sample average to support robust estimation of diverse functions that cannot be computed with DA. Through simulations, we demonstrated that robust TBMA significantly outperforms DA in the presence of Byzantine attacks, maintaining high performance even with a substantial number of attackers. Additionally, we showcased its practical applicability in a FEEL use case, highlighting its resilience and adaptability. These results establish TBMA as a robust and general solution for AirComp in adversarial settings. Future work will explore extending robust TBMA to address other amplitude-related challenges, such as channel alterations.

References

[1] Ana Pérez-Neira, Marc Martinez-Gost, Alphan Şahin, Saeed Razavikia, Carlo Fischione, and Kaibin Huang, "Waveforms for computing over the air," *arXiv preprint arXiv:2405.17007*, 2024.

[2] Aditya Vempaty, Lang Tong, and Pramod K. Varshney, "Distributed inference with byzantine data: State-of-the-art review on data falsification attacks," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 65–75, 2013.

[3] Houssem Sifaou and Geoffrey Ye Li, "Robust federated learning via over-the-air computation," in *2022 IEEE 32nd International Workshop on Machine Learning for Signal Processing (MLSP)*. IEEE, 2022, pp. 1–6.

[4] Changjie Hu, Quanzhong Li, Qi Zhang, and Qiang Li, "Robust design for multi-carrier multi-relay assisted over-the-air computation networks with bounded channel uncertainties," *IEEE Wireless Communications Letters*, vol. 13, no. 8, pp. 2290–2294, 2024.

[5] Hongrui Zhang, Xiao Tang, Ruonan Zhang, Turlykozhayeva Dana, Nurzhan Ussipov, and Zhu Han, "Distributionally robust over-the-air computation in presence of channel uncertainties," in *2024 IEEE Wireless Communications and Networking Conference (WCNC)*, 2024, pp. 1–6.

[6] Dongkai Zhou, Jing Guo, Siqiang Wang, Zhong Zheng, Zesong Fei, Weijie Yuan, and Xinyi Wang, "Otfs-based robust mmse precoding design in over-the-air computation," *IEEE Transactions on Vehicular Technology*, 2024.

[7] Qiaochu An, Yong Zhou, and Yuanming Shi, "Robust design for reconfigurable intelligent surface assisted over-the-air computation," in *2021 IEEE Wireless Communications and Networking Conference (WCNC)*, 2021, pp. 1–6.

[8] Mario Goldenbaum, Holger Boche, and Sławomir Stanczak, "Harnessing interference for analog function computation in wireless sensor networks," *IEEE Transactions on Signal Processing*, vol. 61, no. 20, pp. 4893–4906, 2013.

[9] G. Mergen and L. Tong, "Type based estimation over multiaccess channels," *IEEE Transactions on Signal Processing*, vol. 54, no. 2, pp. 613–626, 2006.

[10] Martin A Fischler and Robert C Bolles, "Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography," *Communications of the ACM*, vol. 24, no. 6, pp. 381–395, 1981.

[11] Li Deng, "The MNIST database of handwritten digit images for machine learning research," *IEEE Signal Processing Magazine*, vol. 29, no. 6, pp. 141–142, 2012.

[12] Marc Martinez-Gost, Ana Pérez-Neira, and Miguel Ángel Lagunas, "Frequency modulation aggregation for federated learning," in *GLOBECOM 2023 - 2023 IEEE Global Communications Conference*, 2023, pp. 1878–1883.

[13] Daniel J. Beutel, Taner Topal, Akhil Mathur, Xinchi Qiu, Javier Fernandez-Marques, Yan Gao, Lorenzo Sani, Kwing Hei Li, Titouan Parcollet, Pedro Porto Buarque de Gusmão, and Nicholas D. Lane, "Flower: A friendly federated learning framework," Open-Source, mobile-friendly Federated Learning framework, Mar. 2022.