

Secure Parameter Sharing in Federated Learning via Over-the-Air Computing

Xinyu Cao⁺, Shangqing Zhao⁺, Yanjun Pan^{*}, Yuchen Liu[§]



NC STATE

⁺University of Oklahoma,

^{*}University of Arkansas,

[§]North Carolina State University



UNIVERSITY OF ARKANSAS

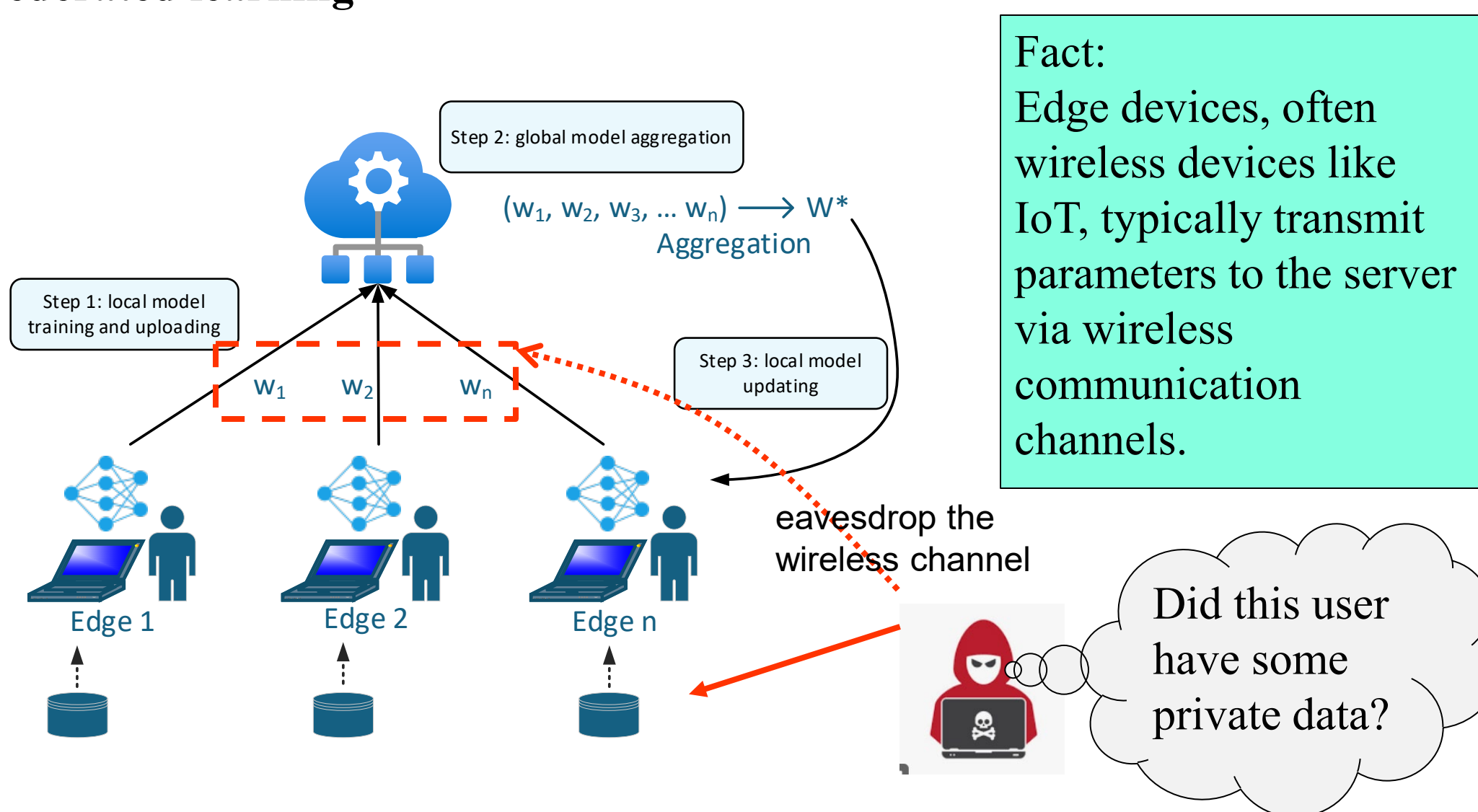
Abstract

Federated learning has gained significant popularity, particularly with the rise of edge devices such as IoT systems. However, it remains vulnerable to inference attacks, where adversaries can intercept shared model parameters and infer sensitive training data. Traditional encryption methods, though effective, impose computational complexity, making them unsuitable for resource-constrained IoT devices that often rely on battery power.

In this work, we explore AirComp (Over-the-Air Computing) as a lightweight solution to secure federated learning against inference attacks. AirComp leverages the superposition property of wireless channels to enable simultaneous transmissions from multiple users, allowing the computation of specific functions directly over the air, thus eliminating the need for complex encryption on edge devices. By introducing inherent noise and randomness during the transmission process, AirComp reduces the risk of parameter leakage without adding computational overhead. This poster presents our conceptual framework and initial findings, demonstrating the potential of AirComp to safeguard federated learning while maintaining efficiency in resource-limited environments.

Background

Federated learning



Fact: Edge devices, often wireless devices like IoT, typically transmit parameters to the server via wireless communication channels.

Vulnerability

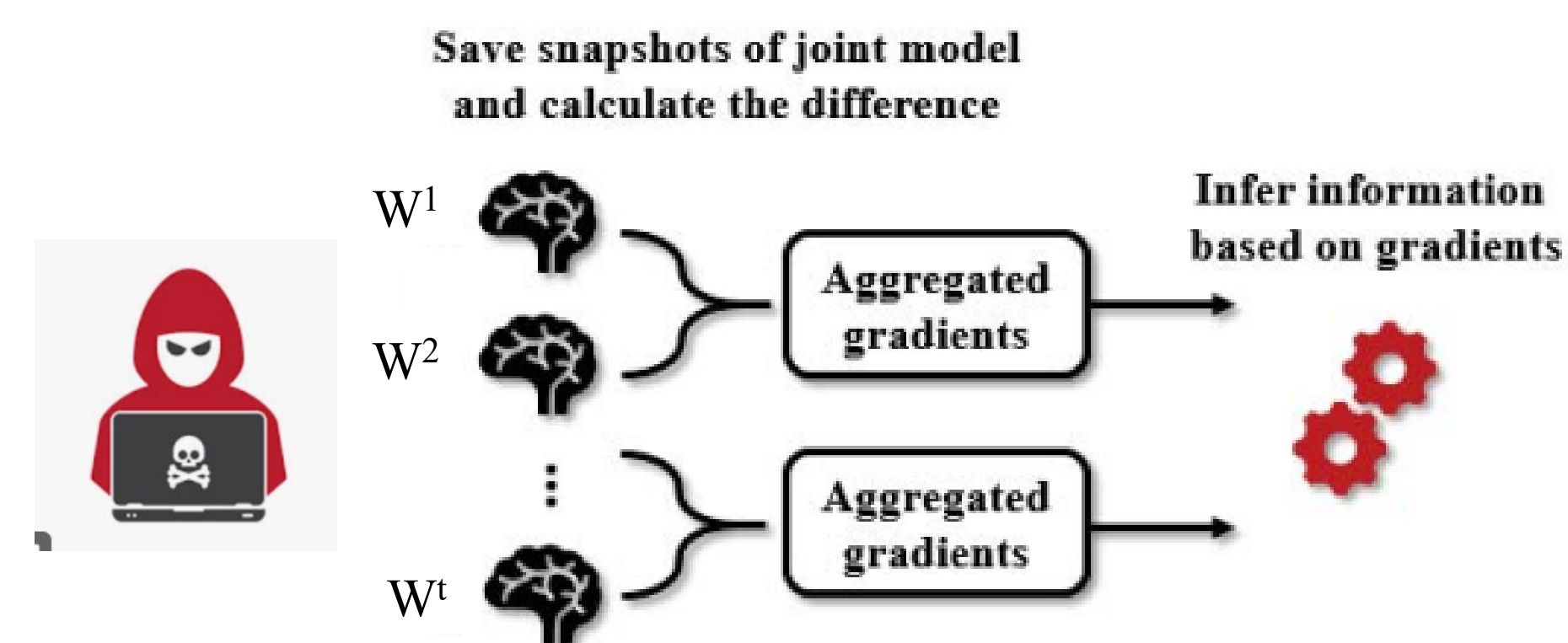
Attackers can eavesdrop on the wireless transmission, intercepting these parameters and launching inference attacks to extract sensitive information from the dataset.

Motivation

Existing Attacks

Membership inference attacks aim to identify whether a data record was part of the target model's training dataset or not.

An adversary can tell whether a data record has been used to train a classifier or not, solely based on the prediction vector of the data record.



White Box attack: the attacker can obtain all the parameters as well as the models and aggregation function used in the system.

Black Box attack: the attacker can obtain the updating parameters of both uplink and downlink.

Existing Defense

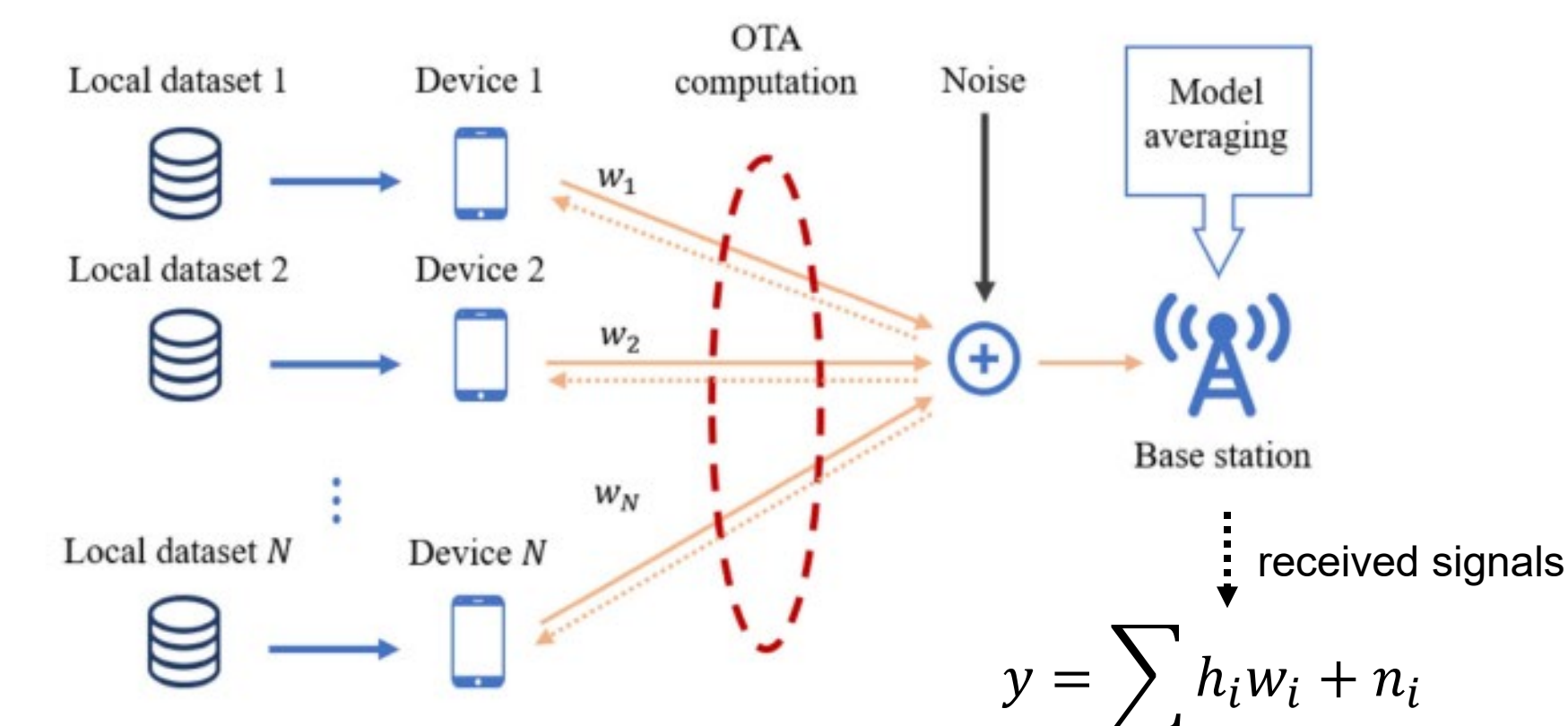
1. Differential privacy: adding random noise to the model updates shared by clients before they are sent to the server, which helps obscure individual data points and ensures privacy.
2. Homomorphic Encryption: allows computations to be performed directly on encrypted data without needing to decrypt it. In federated learning

Open problem:

- Impaired Updating Performance: The noise injected to guarantee privacy can degrade model accuracy.
- High Computational Cost: HE is computationally expensive, especially for resource-constrained IoT devices.

Over the Air Computing

AirComp works by exploiting the fact that wireless signals naturally add up in the air due to the superposition property of electromagnetic waves. Rather than treating this signal superposition as interference, AirComp turns it into a computational advantage



Advantage:

This approach bypasses the need for traditional techniques like time-division or frequency-division multiplexing, significantly improving spectrum efficiency and reducing communication delays.

AirComp for Data Privacy

Due to the concurrent transmission from multiple clients, the signals are aggregated over the air, making it difficult for the central fusion center or any potential eavesdropper to distinguish the individual up-dates from each client.

This inherent characteristic of AirComp can serve as a form of privacy protection, as the superimposed signals obscure the contribution of each client. As a result, adversaries attempting to launch inference attacks to extract sensitive information from the updates would face significant challenges, since the individual updates are masked by the aggregation process.

Open Research Questions

- handling channel variability h_i : Could employ advanced channel estimation and pre-coding techniques to manage variability in wireless channels.
- Synchronization: Slotted synchronization protocols could be implemented to handle the timing differences across clients, allowing signals to be superimposed effectively in real-time without distortion.
- Mitigate noise accumulation: noise reduction filters or denoising algorithms.