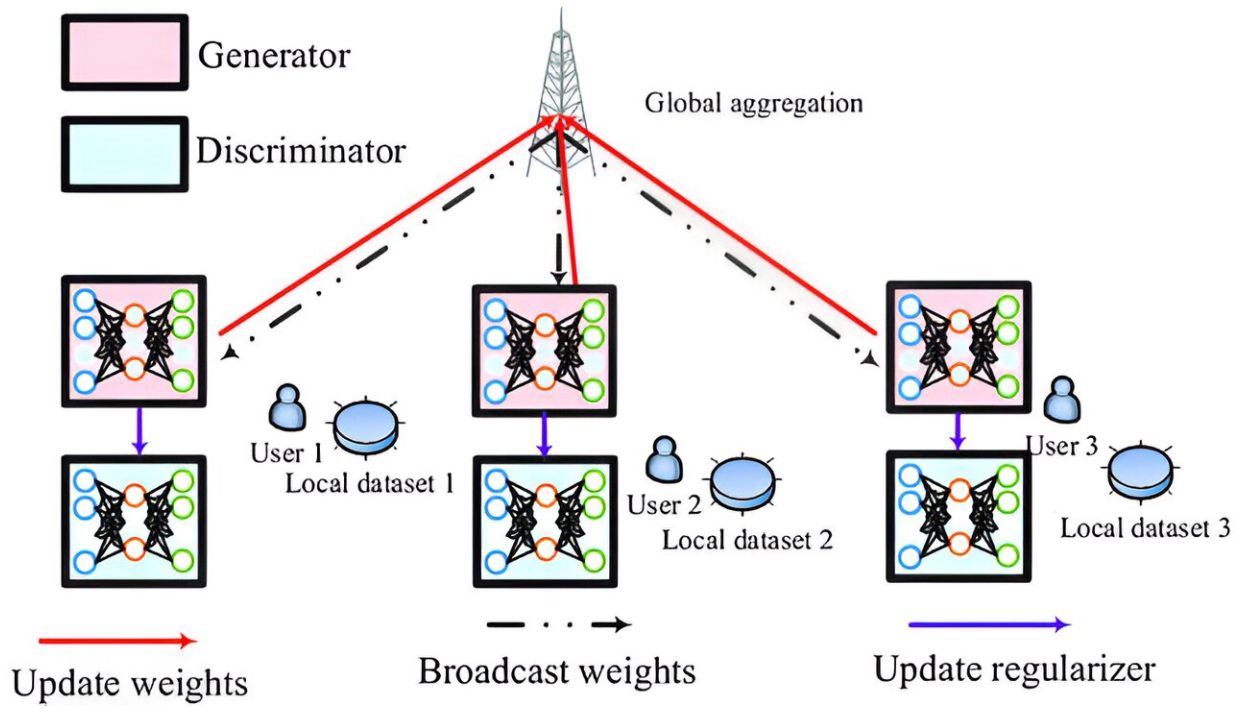
Research team designs privacy-protecting algorithm for better wireless communication

January 18 2024



During training, only the parameters of the generator are transmitted between the central server and local devices. The discriminators on the local devices update their regularization terms based on the parameters received from the server. Credit: YIYU GUO ET AL.

In today's increasingly interconnected world, high-quality communication has become more vital than ever. Accurately estimating the dynamic status of communication channels is a key factor in

achieving this. Recently, a joint research team designed a new algorithm that offers high-level estimation accuracy and privacy protection with low computational and communication costs. This research was published in Intelligent Computing.

This new algorithm uses a specially designed deep learning model for precise estimation and a federated learning framework for training the model while keeping user data secure and overhead low. It also includes a user motivation scheme to get the most out of computing resources.

The team tested the algorithm in a wireless communication network using local user datasets and realistic environment datasets. The test on local user datasets demonstrated that their method is more accurate in estimating channel state information compared with some traditional and deep learning algorithms under different signal-to-noise ratios, pilot frequencies and other conditions.

The realistic environment test further proved the effectiveness of the algorithm. The channel data used in the test are from a mobile communication open dataset and include sparse and dense scenarios; the sparse scenario contains 10,000 maps, each containing five base station locations and 30 user locations, and the dense scenario contains 100 maps, each containing one base station location and 10,000 user locations. All users are assumed to be stationary throughout the process.

The results show that the algorithm outperforms three state-of-the-art models in both sparse and dense scenarios, and the performance gap is wider in the sparse scenario where conditions are more variable and complex. That means the model trained through federated learning and with a higher level of user participation is more robust, adaptable, and scalable than the benchmark models, which were trained in a centralized way.

In a federated learning framework, the resources used for training are those of the local devices, which exchange parameters instead of raw data with the central server. This reduces computational and communication costs, protects user data privacy, and suits large complex communication networks, and thus perfectly complements accuracy-first, less flexible deep learning models, such as, in this case, a generative adversarial network.

A typical generative adversarial network consists of a generator and a discriminator: the former creates samples to approximate real-world data, and the latter challenges the samples to push for better results. The team designed their version into a dual-U-shaped network to avoid information loss during sampling and added a regularization function at the discriminator for higher consistency and stability.

The team pointed out that their algorithm has certain limitations, including numerous model parameters and reliance on labeled data. Compressing the model and training it with unsupervised approaches are possible directions for future work. In the future, they plan to explore federated learning in dynamic, diverse networks where each device possesses different resources to perform onboard verification and client selection.

More information: Yiyu Guo et al, Federated Generative-Adversarial-Network-Enabled Channel Estimation, *Intelligent Computing* (2023). DOI: 10.34133/icomputing.0066

Provided by Intelligent Computing

privacy-algorithm-wireless-communication.html