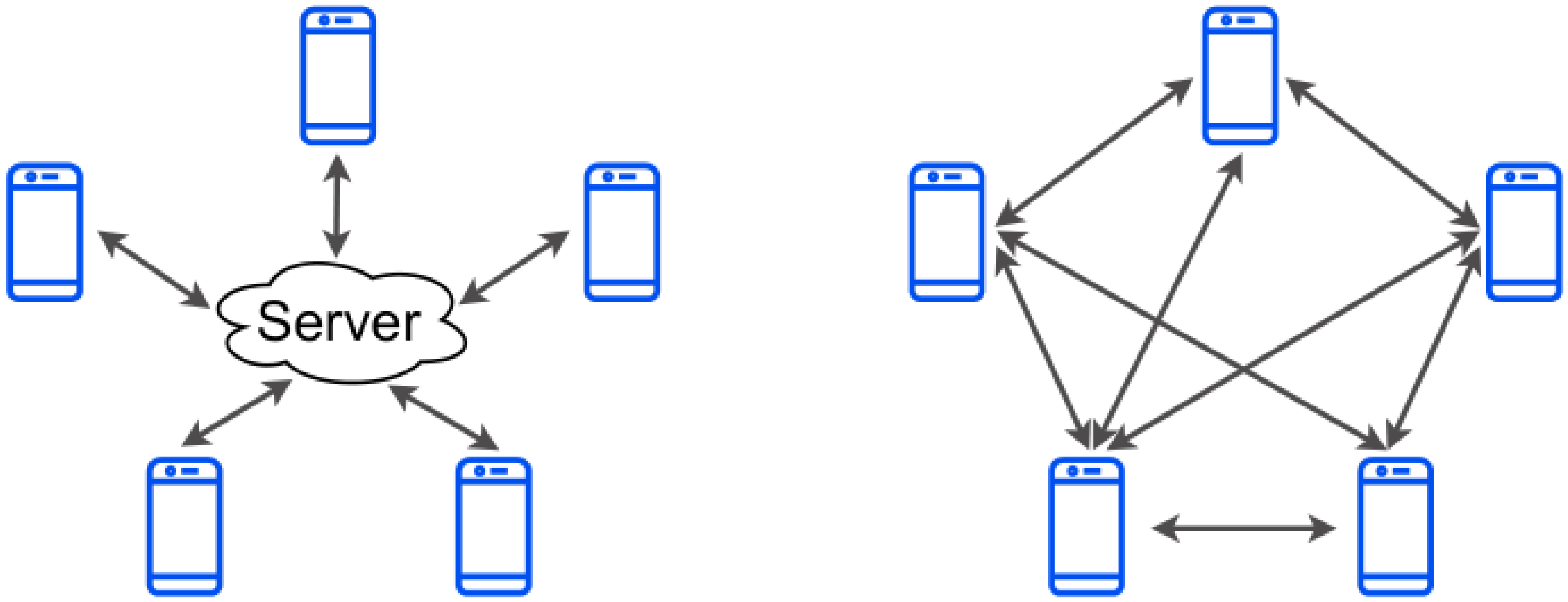
FL Security

Meeting

02-21-2025



(a) Server-assisted FL (b) DFL

Figure 1: Server-assisted FL vs. DFL.

Server-assisted FL or DFL (our proposed aggregation rule):

Given a total of *n* clients, the server first calculates the coordinate-wise median across all clients' local model updates. Then, for each dimension, it selects the top (*n*-*b*) values that are closest to the median and computes either their average or a weighted average. Here, *b* represents the estimated number of malicious clients.

Based on their distance to median

We can use clustering approach or other methods to estimate the number of malicious clients

To do (we need GPU to run the experiments. Focus on server-assisted FL first):

1) Familiar with the code

2) Implement our aggregation rule (in page three)