Federated Selective State-Space Learning for Measurement-Based False Data Injection Attack Detection in Islanded Microgrids

Mahmuda Akter, Zhifang Wang

Electrical and Computer Engineering
College of Engineering

Contributions

- Proposed a federated selective state-space learning framework for FDIA detection in islanded microgrids.
- Developed FDIA dataset using injection and line-flow measurements under weak, medium, and strong attacks.
- Designed a five-client regional learning setup where each client trains locally without sharing raw microgrid measurements.
- Validated the proposed method on an IEEE 13-node islanded microgrid and compared it with the FL-BiLSTM baseline.

FDIA Formulation

- State-measurement model: $z(t) = h\big(x(t)\big) + e(t)$ ……(1)
- FDIA-corrupted measurement: $z^a(t) = z(t) + a(t)$ ……(2)
- Stealthy attack vector: $a(t) = Hc(t)$ ……(3)

Proposed FL-Mamba Framework

- Each client keeps its own local measurement windows and trains a Mamba-based FDIA detector without sharing raw data.

$$X_i \in R^{F_i \times T} \text{ ……(4)}$$

where X_i is the local input window of client i, F_i is the number of measurement features, and T is the sequence length.

- The Mamba encoder learns temporal attack patterns from local measurement sequences by selectively retaining important time-dependent information.
- During FL training, only model parameters are returned to the server:

$$w^{r+1} = \sum_{i=1}^{M} \frac{n_i}{n} w_i^{r+1} \text{ ……(5)}$$

- During inference, client attack probabilities are fused:

$$p_{global} = \frac{1}{M} \sum_{i=1}^{M} p_i \text{ ……(6)}$$

$p_{global} \geq \tau \rightarrow$ FDIA, $p_{global} < \tau \rightarrow$ Normal. p_i is the local attack probability from client i, and τ is the detection threshold.

Case Studies

- The proposed FL-Mamba detector is compared with FL-Bi-LSTM under the same five-client federated learning setup.
- Detection performance is evaluated using accuracy, precision, attack recall, F1-score, and confusion matrices across different attack strengths.

TABLE I. FEDERATED CLIENT REGIONS

Client	Representative Nodes
C1	650, 632
C2	633, 634
C3	645, 646
C4	670, 671, 692, 675, 680
C5	684, 611, 652

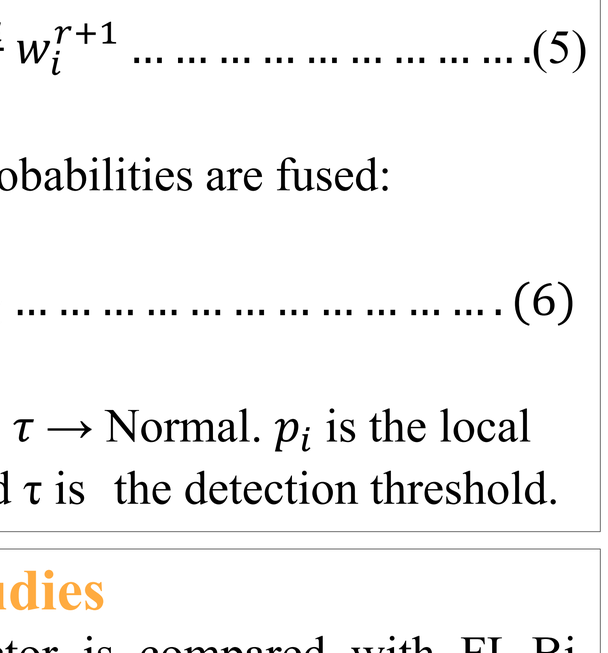

Fig. 1. One-Line Diagram of Islanded IEEE 13 Node Microgrid

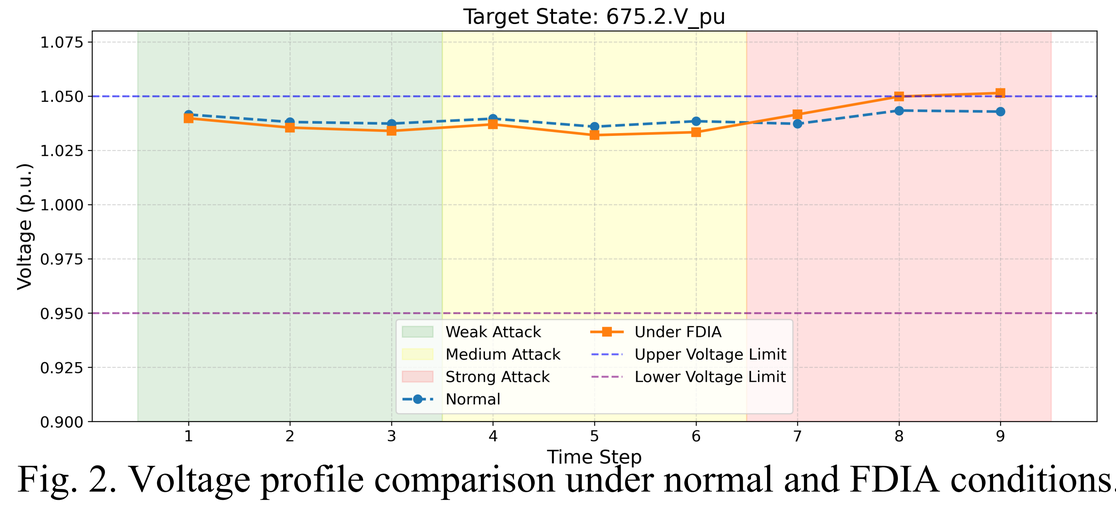

Fig. 2. Voltage profile comparison under normal and FDIA conditions.

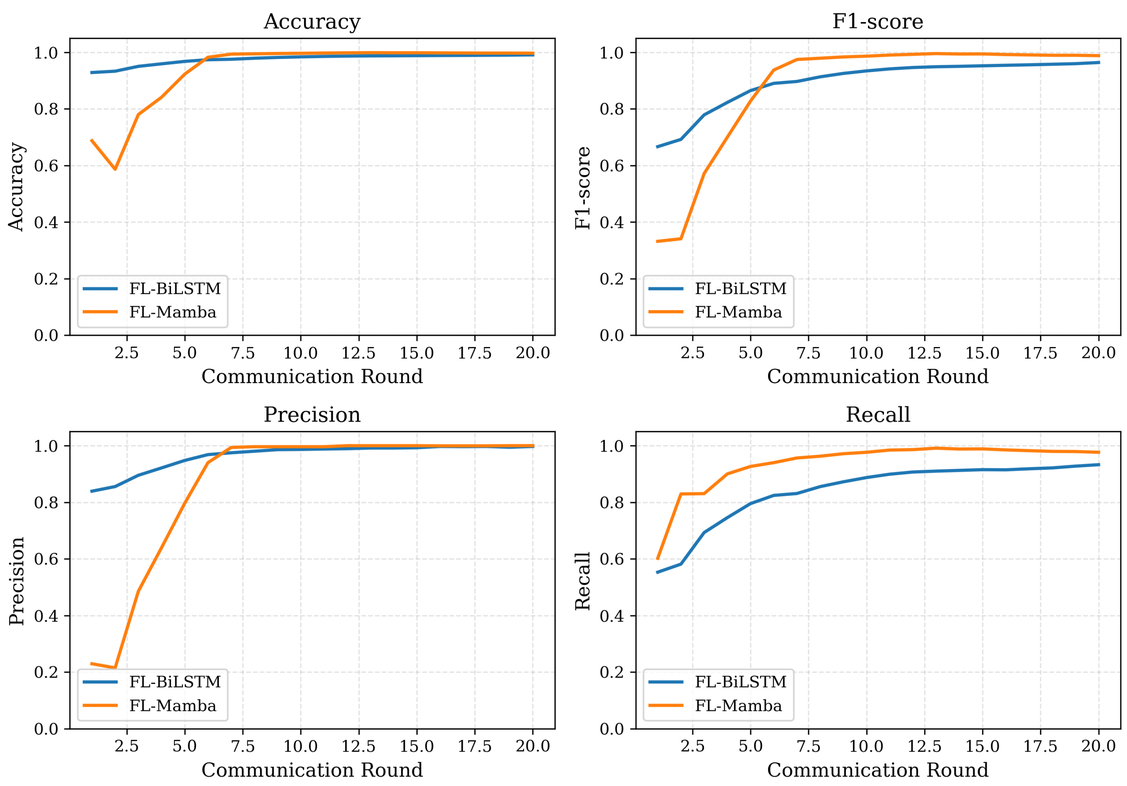

Fig. 3. Training performance comparison of FL-BiLSTM and FL-Mamba over communication rounds.

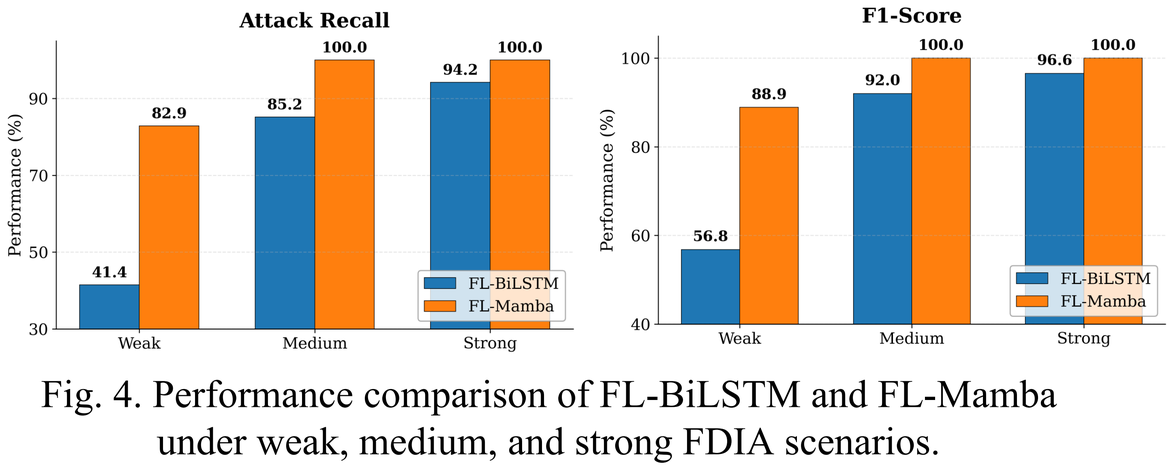

Fig. 4. Performance comparison of FL-BiLSTM and FL-Mamba under weak, medium, and strong FDIA scenarios.

$$\textbf{Recall} = \frac{\textbf{TP}}{\textbf{TP} + \textbf{FN}} \qquad \textbf{F1} = \frac{\textbf{2(Precision} \times \textbf{Recall)}}{\textbf{Precision} + \textbf{Recall}}$$

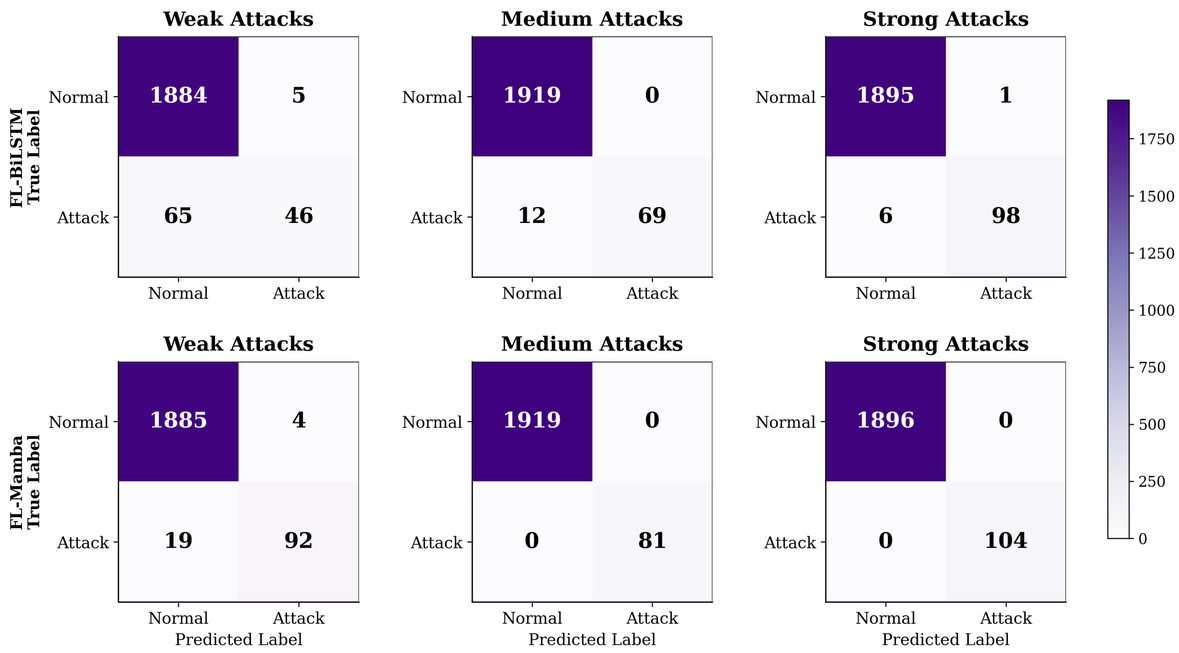

Fig. 5. Confusion matrices for FL-BiLSTM and FL-Mamba under weak, medium, and strong FDIA scenarios.

Conclusion & Future Work

- FL-Mamba improves weak-attack detection over FL-Bi-LSTM, increasing recall from 41.4% to 82.9% and F1-score from 56.8% to 88.9%.
- Future work will focus on attack localization and additional cyberattack scenarios.