IEEE Future NETWORKS™

IEEE Future Networks™ WORLD FORUM • 2023

Elevating 5G Network Security: A Profound Examination of Federated Learning Aggregation Strategies for Attack Detection

Ioannis Makris, Nikolaos Ntampakis, Thomas Lagkas, Panagiotis Radoglou-Grammatikis, Sotirios K. Goudos, Vasileios Argyriou, Eleftherios Fountoukidis, Antonio F. Skarmeta, Pablo Fernandez Saura, Panagiotis Sarigiannidis

Co-funded by the European Union

6GSNS

NANCY

NANCY project has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101096456.

Ioannis Makris	MetaMinds Innovations - Kozani, Greece
Nikolaos Ntampakis	MetaMinds Innovations - Kozani, Greece
Thomas Lagkas	International Hellenic University - Kavala, Greece
Panagiotis Radoglou-Grammatikis	University of Western Macedonia - Kozani, Greece
Sotirios K. Goudos	Aristotle University of Thessaloniki - Thessaloniki, Greece
Vasileios Argyriou	Kingston University London - London, UK
Eleftherios Fountoukidis	Sidroco Holdings LTD - Nicosia, Cyprus
Antonio F. Skarmeta	University of Murcia - Murcia, Spain
Pablo Fernadez Saura	University of Murcia - Murcia, Spain
Panagiotis Sarigiannidis	University of Western Macedonia - Kozani, Greece

Overview

- Motivation
- Aim and Contribution
- System Architecture
- Federated Learning
  - Model Architecture
  - FL strategies
- Dataset
  - Description
  - Preprocessing
- Results
  - Evaluation Metrics
  - Experiments Outcomes
- Conclusion and Future Work

Motivation

- **Rapid Growth of 5G Networks**: Significant advancements in connectivity, speed, and reliability.
- **Security Challenges**: Increased security and privacy concerns in distributed, dynamic 5G networks.
- **Dynamic and Complex Nature**: Difficulty of traditional Intrusion Detection Systems (IDS) to handle 5G's diverse devices.
- **Privacy and Data Exchange Issues**: Limitations in data sharing among devices due to privacy concerns.
- **Need for Effective IDS**: Critical for detecting cyber threats, with the balance of accuracy and privacy.

Aim and Contribution

Research Aim

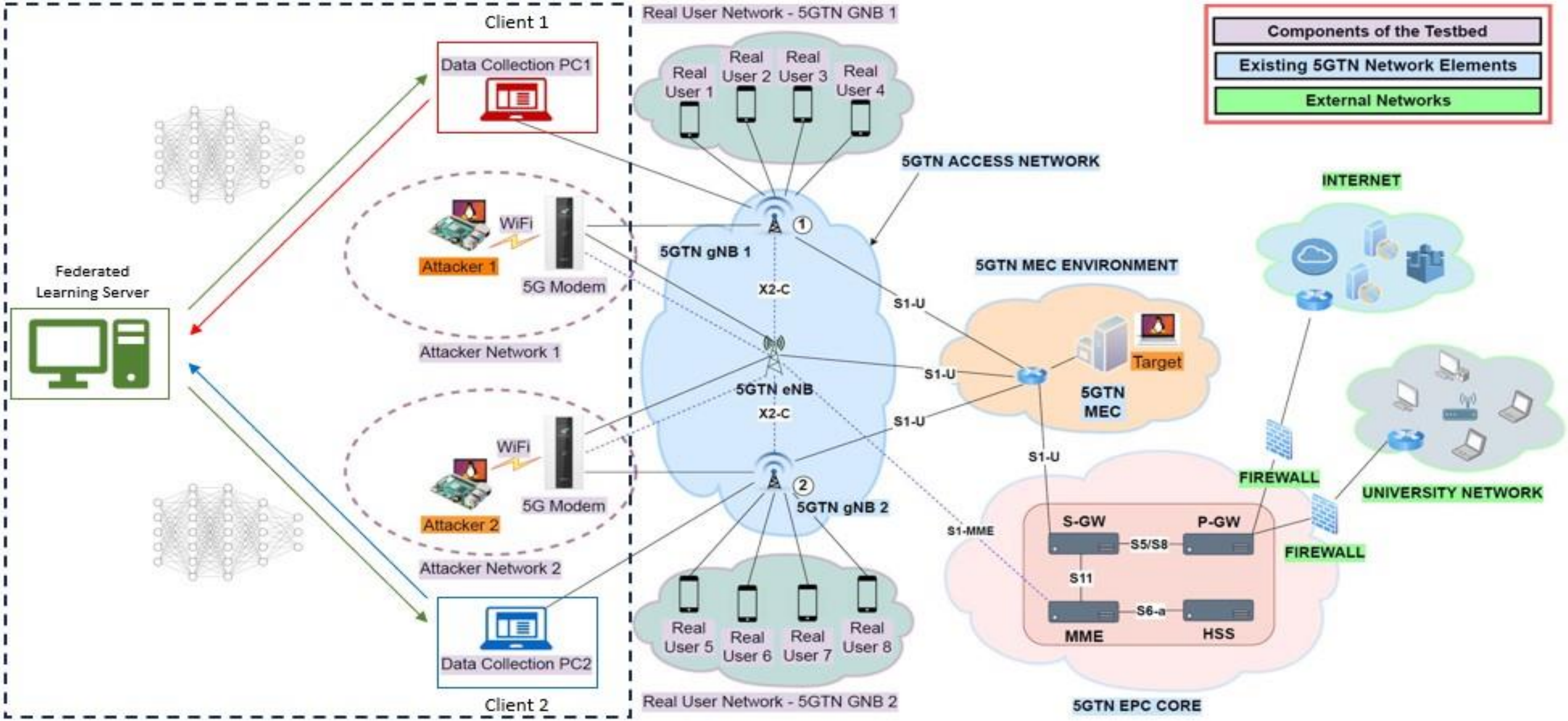
Explore the use of Federated Learning (FL)-based Intrusion Detection Systems (IDS) in 5G networks to detect 9 different types of intrusions while upholding user privacy.

Innovative Approach: Utilization of FL to train an IDS across different nodes without direct data exchange.

Contributions

- Demonstrated higher effectiveness and privacy preservation of FL-based IDS.
- Provided insights into the impact of FL aggregation strategies on IDS performance.
- Offered a scalable, adaptable solution for securing 5G networks against cyber threats.

System Architecture



S. Samarakoon, Y. Siriwardhana, P. Porambage, M. Liyanage, S.-Y. Chang, J. Kim, J. Kim, and M. Ylianttila, "5g-nidd: A comprehensive network intrusion detection dataset generated over 5g wireless network," arXiv preprint arXiv:2212.01298, 2022

Federated Learning: Model Architecture

AI/ML Model: Multi-Layer Perceptron (MLP)

- Hidden layers: 5
- Neurons/layer: 150 → 100 → 75 → 50 → 25
- Output layer's neurons: 9
- Output's layer activation function: Softmax

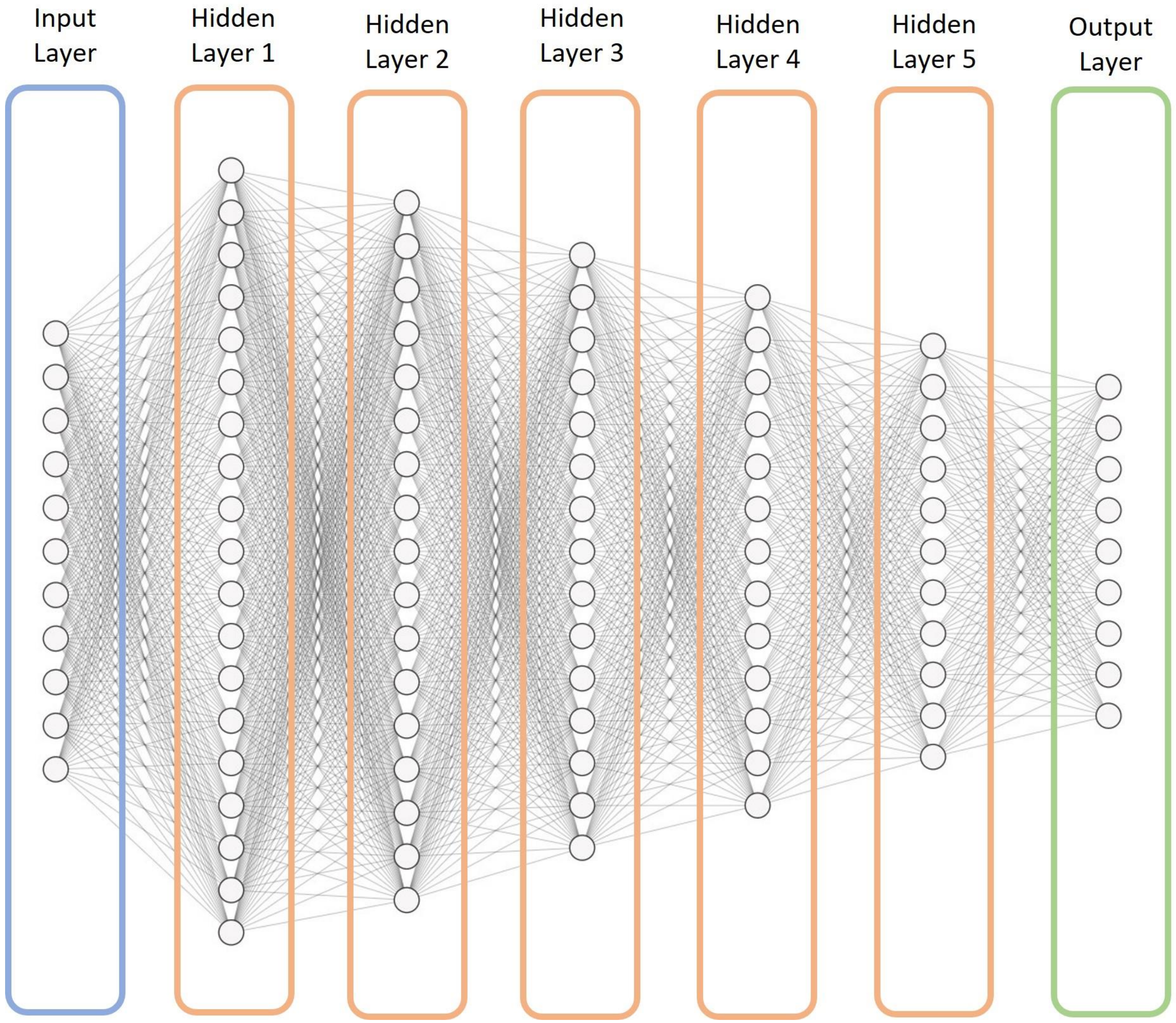
$$Softmax(x) = [e\hat{}x\_1 / sum(e\hat{}x), e\hat{}x\_2 / sum(e\hat{}x), \ldots, e\hat{}x\_9 / sum(e\hat{}x)]$$

- Optimizer: Adam

$$Adam\_update = \mathrm{lr} * \hat{m} / \mathrm{np.sqrt}(\hat{v} + 1\mathrm{e}\text{-}8)$$

- Loss function: Sparse Categorical Crossentropy

$$Sparse\_categorical\_crossentropy(y\_true, y\_pred) = \text{-sum}(\text{y\_true} * \log(\text{y\_pred}))$$



Federated Learning: FL Strategies

Aggregation

- *FedAvg*: Weighted average of local model updates. → $w_{global} = \frac{n_1}{n_1+n_2} w_1 + \frac{n_2}{n_1+n_2} w_2$
- *FedProx*: Generalization of FedAvg introducing a proximal term. Aims to reduce the impact of variable local updates. → $w_{global} = \frac{n_1}{n_1+n_2} w_1 + \frac{n_2}{n_1+n_2} w_2 + \lambda(\|w_1 - w_{prev}\|^2 + \|w_2 - w_{prev}\|^2)$

Optimization

- *FedAdam*: Introduces two decay parameters controlling historical and current model update importance. → $m_t = \beta_1 m_{t-1} + (1-\beta_1) g_t$, $u_t = \beta_2 u_{t-1} + (1-\beta_2)\, g_t{}^2$
- *FedAdagrad*: Aggregates based on the difference between client and server models. → $g_{t,i} = \frac{1}{\eta}(\sqrt{\sum_{T=11} t\, g_{T,i}^2})$
- *FedYogi*: Considers distance from server model, direction of difference, and a decay parameter. → $g_{t,i} = g_{t-1,i} a \|\nabla F_i(w_{t-1}) - g_{t-1,i}\|$

Dataset: Description

- *Origin and Data Collection:* Generated for 5G-NIDD at University of Oulu's 5G Test Network, focusing on intrusion detection in 5G; data from Raspberry Pi attackers and live mobile traffic saved independently across two base stations.

- *Data Format and Structure:* Data collected in packet and flow formats, saved in PCAPNG, Argus, and CSV file formats, divided by base station and attack session.

- *Dataset Composition:* Focuses on BTS_1.csv (*728,316 rows*) and BTS_2.csv (*487,574 rows*), each featuring 52 features such as network packet flags, sequence numbers, runtimes, statistical measures, and TCP details.

- *Primary Study Variable:* "Attack Type" highlighted as the pivotal feature, encompassing 9 distinct categories: 1 benign and 8 varied attack types.

Dataset: Preprocessing

Consistent modifications applied to both BTS_1 and BTS_2 datasets.

- Managed missing values through sample removal or imputation.
- Eliminated duplicates.
- Applied one-hot encoding for categorical attributes.
- Stratified train-test split was done with an 80/20 ratio to maintain representation of all classes.
- Standard scaling was employed to ensure all features had consistent scale and distribution.
- SMOTE oversampling technique was implemented to address class imbalances in the "Attack Type" column, creating synthetic samples for minority classes.

Results: Evaluation Metrics

Confusion Matrix:

True label \ Predicted label		
	TP: Model correctly identifies an attack.	**FP**: Model incorrectly identifies an attack.
	FN: Model fails to identify an actual attack.	**TN**: Model correctly identifies no attack.

Predicted label

Accuracy:

$$\frac{TP+TN}{TP+TN+FP+FN}$$

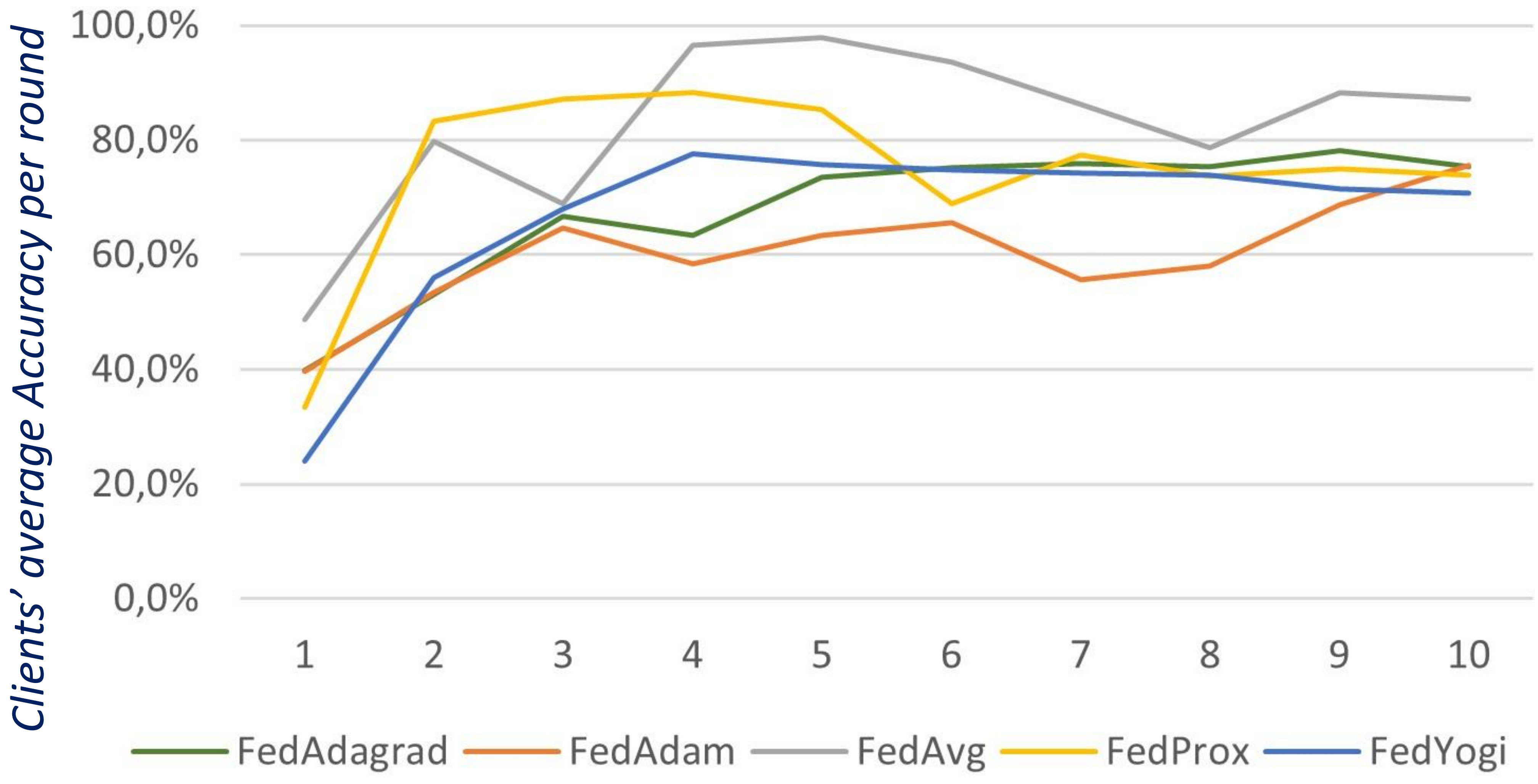
F1 Score:

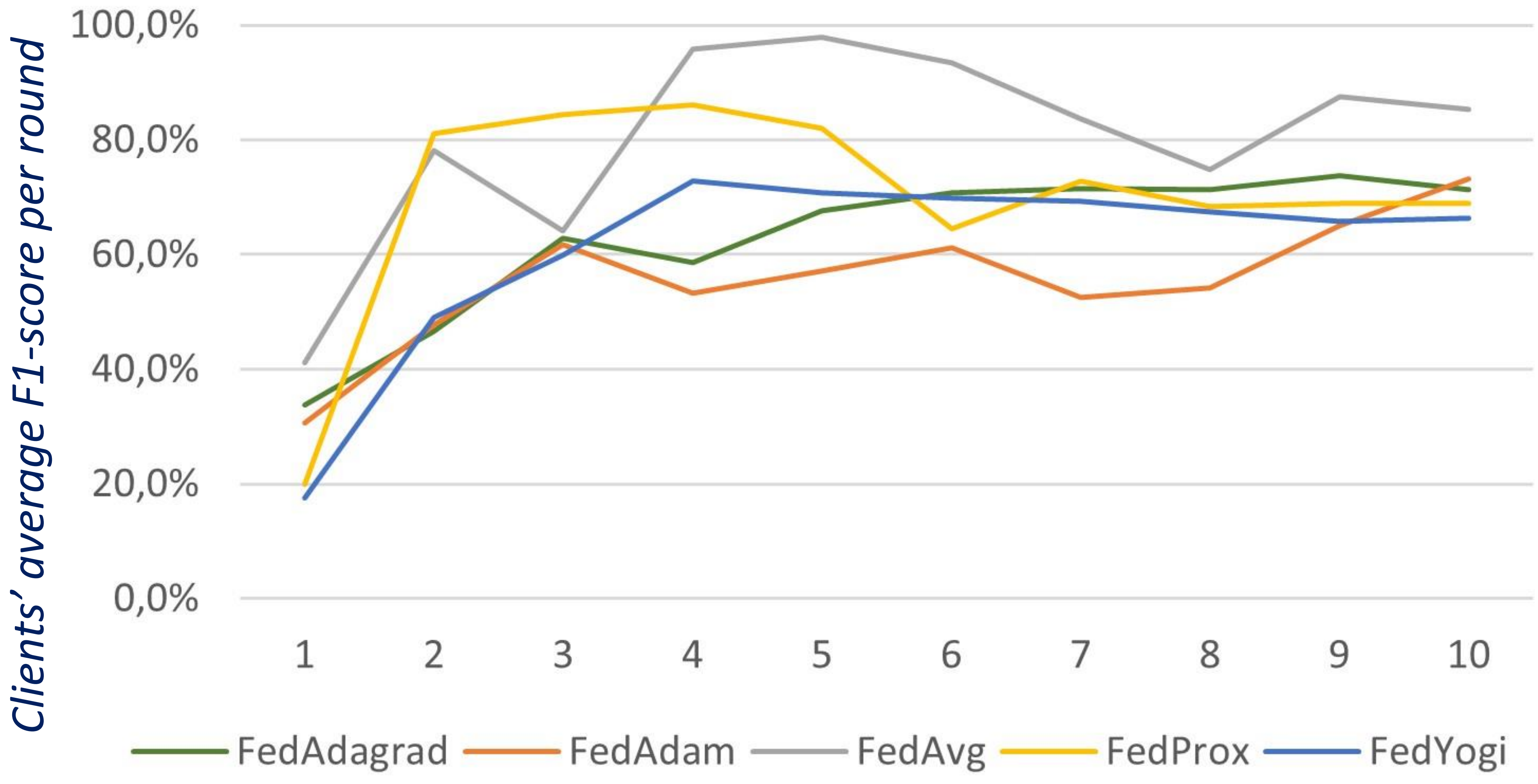
$$\frac{2\times \mathrm{TP}}{2\times \mathrm{TP}+\mathrm{FP}+\mathrm{FN}}$$

The evaluation metrics were weighted based on each client's data sample size to ensure a fair assessment.

Results: Experiments Outcomes

Strategy	Evaluation Metric	Client 1	Client 2	Average
FedAvg	Accuracy	99.45%	95.64%	**97.89%**
	F1-score	99.45%	95.55%	**97.85%**
FedProx	Accuracy	82.22%	97.18%	88.35%
	F1-score	79.01%	96.33%	86.11%
FedAdam	Accuracy	76.05%	75.12%	75.67%
	F1-score	73.47%	72.97%	73.27%
FedAdagrad	Accuracy	78.35%	77.87%	78.15%
	F1-score	73.22%	74.76%	73.85%
FedYogi	Accuracy	79.18%	75.49%	77.67%
	F1-score	74.00%	71.01%	72.77%

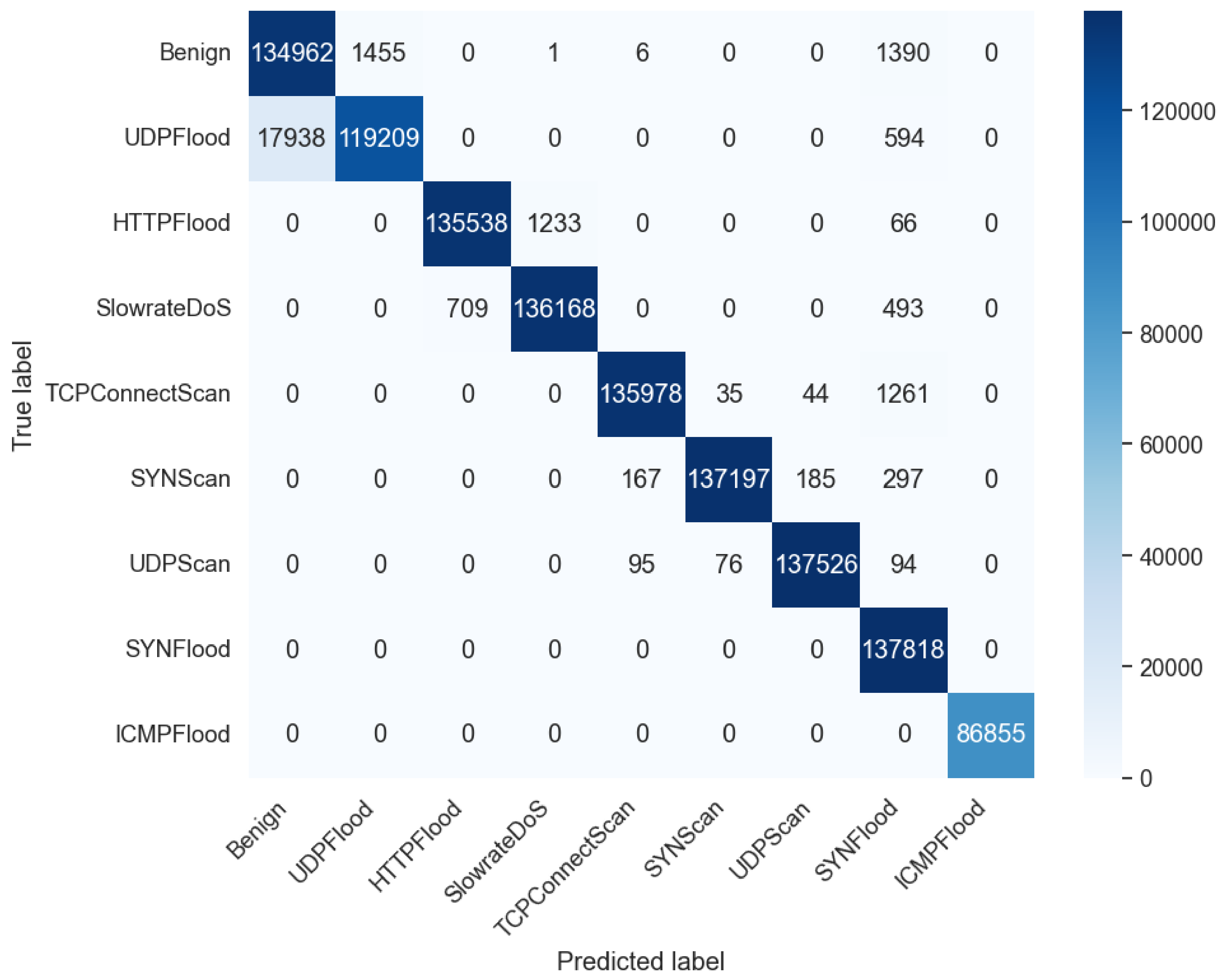




Results: Experiments Outcomes

Strategy	Evaluation Metric	Client 1	Client 2	Average
FedAvg	Accuracy	99.45%	95.64%	**97.89%**
	F1-score	99.45%	95.55%	**97.85%**
FedProx	Accuracy	82.22%	97.18%	88.35%
	F1-score	79.01%	96.33%	86.11%
FedAdam	Accuracy	76.05%	75.12%	75.67%
	F1-score	73.47%	72.97%	73.27%
FedAdagrad	Accuracy	78.35%	77.87%	78.15%
	F1-score	73.22%	74.76%	73.85%
FedYogi	Accuracy	79.18%	75.49%	77.67%
	F1-score	74.00%	71.01%	72.77%

FedAvg Confusion Matrix



Conclusion and Future Work

Conclusion

- *Concluding Insight:* Federated Learning, particularly using the FedAvg aggregation strategy, proves effective for enhancing privacy and security in 5G networks by enabling base stations to collaboratively train a deep ANN for reliable intrusion detection.

Future Work

- *Aggregation Strategies:* Development of innovative, intrusion-specific federated aggregation strategies to enhance both communication and computational efficiency.

- *Real-World Testing:* Extensive testing in practical, large-scale scenarios to validate the approach's feasibility and identify any potential limitations.

Thank you for your attention!

Questions?

Co-funded by the European Union

NANCY project has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101096456.