

# A Federated Continual Learning Framework for Sustainable Network Anomaly Detection in O-RAN

Chafika Benzaid\*, Fahim Muhtasim Hossain\*, Tarik Taleb\*\*, Pedro Merino Gomez<sup>§</sup>, Michael Dieudonne<sup>§</sup>

\*University of Oulu, \*\*Ruhr University Bochum, <sup>§</sup>Universidad de Malaga, <sup>§</sup>Keysight Technologies

[chafika.Benzaid@oulu.fi](mailto:chafika.Benzaid@oulu.fi), [fahimtonmoy108@gmail.com](mailto:fahimtonmoy108@gmail.com), [tarik.taleb@rub.de](mailto:tarik.taleb@rub.de), [pmerino@uma.es](mailto:pmerino@uma.es), [Michael\\_dieudonne@keysight.com](mailto:Michael_dieudonne@keysight.com)

IEEE WCNC 2024, 21-24 April 2024, Dubai, United Arab Emirates

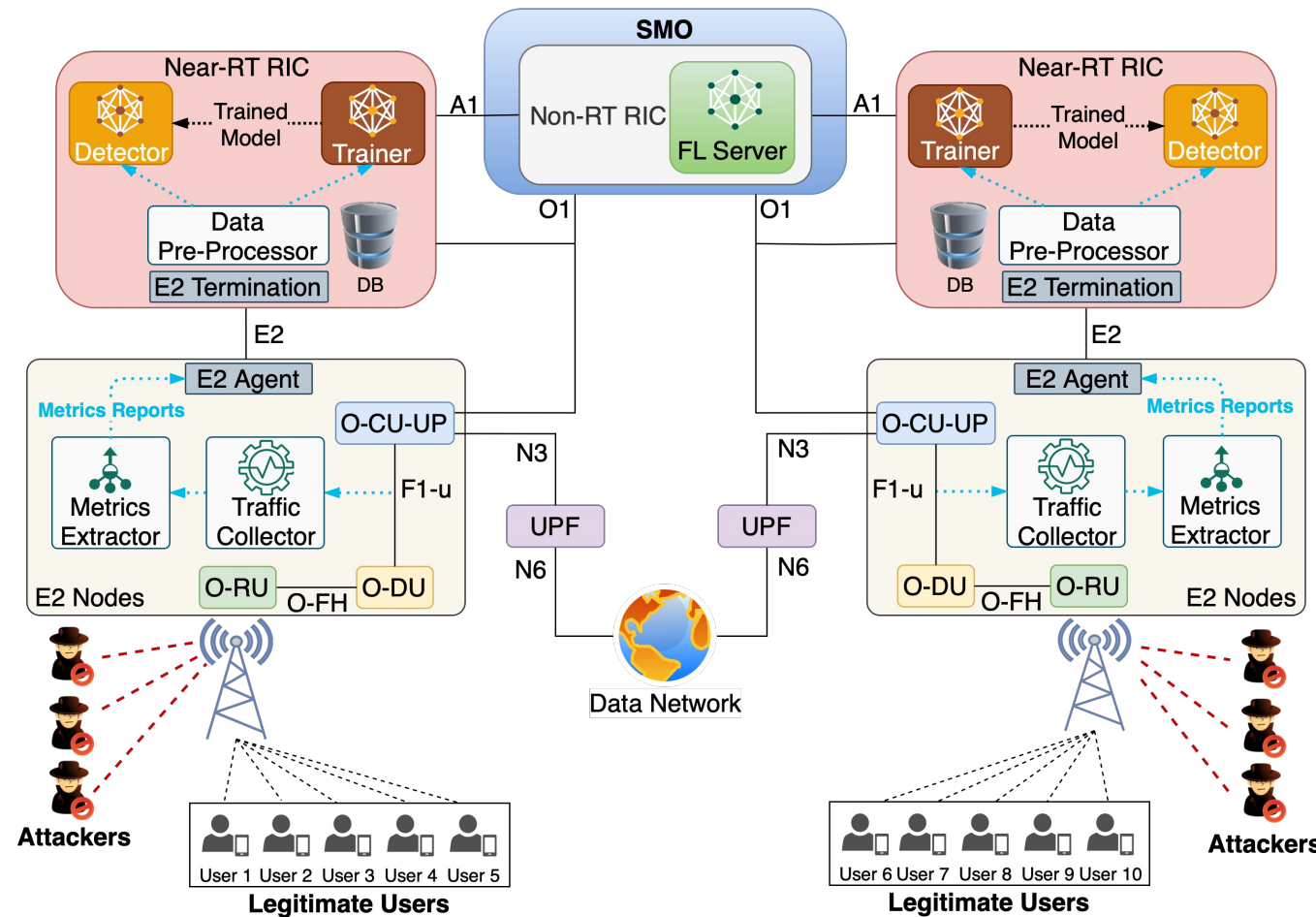
# Network Slicing – Opportunities & Challenges



- **Network anomaly detection** systems are crucial for protecting B5G networks against emerging cyberthreats
- The highly distributed and disaggregated nature of B5G networks has spurred interest in **Federated Learning (FL)** for empowering **collaborative** network anomaly detection at the edge
  - Improving the effectiveness and timeliness of anomaly detection
  - Fostering data privacy preservation
- FL is prone to **catastrophic forgetting (CF)**
  - Prior knowledge is forgotten while sequentially learning new attack patterns from a stream of data
    - Undermine the attack detection effectiveness
- **Few studies addressed CF** issue in network anomaly detection using **Continual Learning (CL)**
  - Focusing on centralized models rather than FL
  - Overlooking integration in B5G

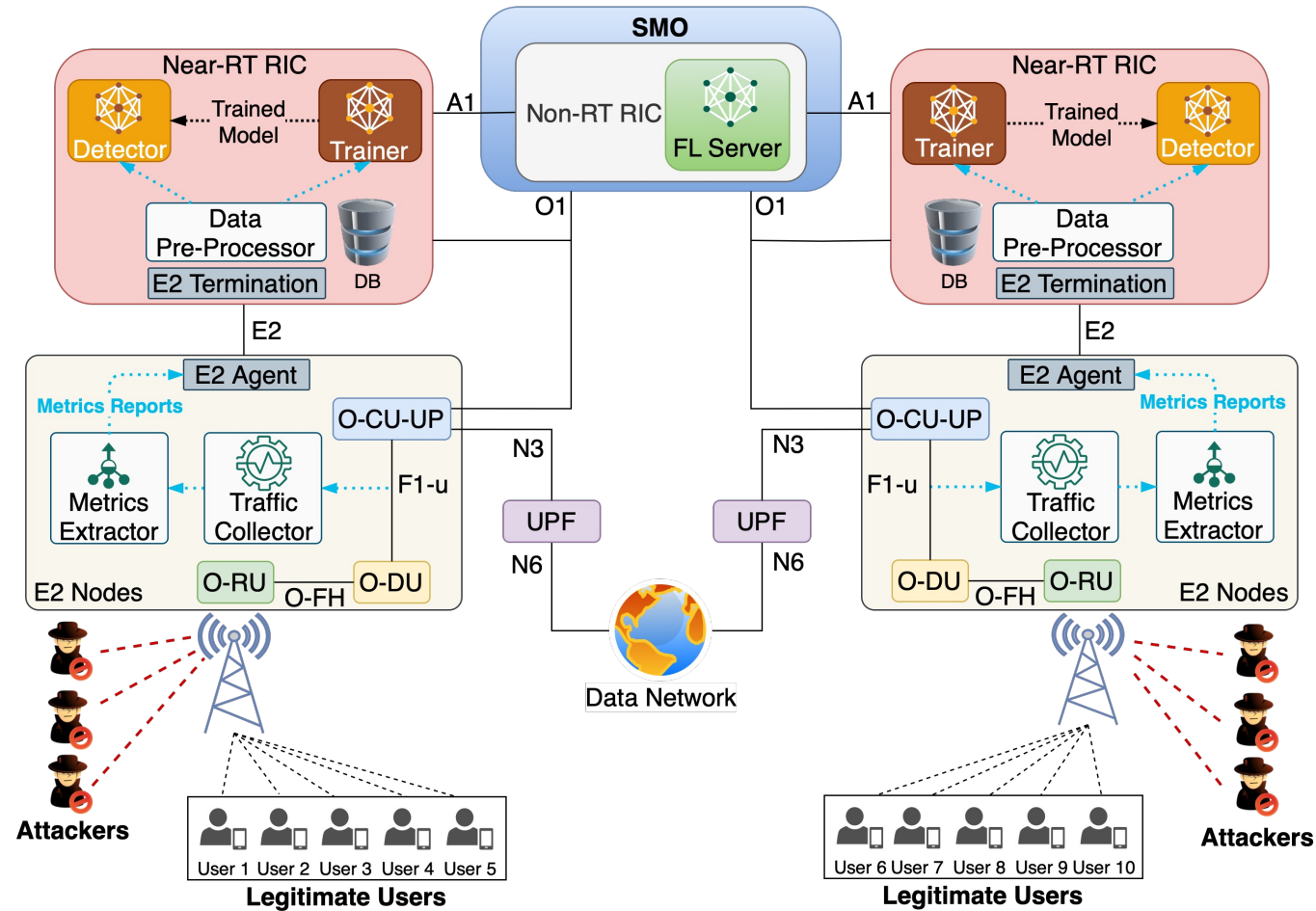
# TenaxDoS – A FCL-based DDoS Detection Framework (1/6)

- A novel framework that leverages and **combines** the potential of **CL** and **FL** to empower **sustainable and cooperative** network attack detection in **O-RAN**



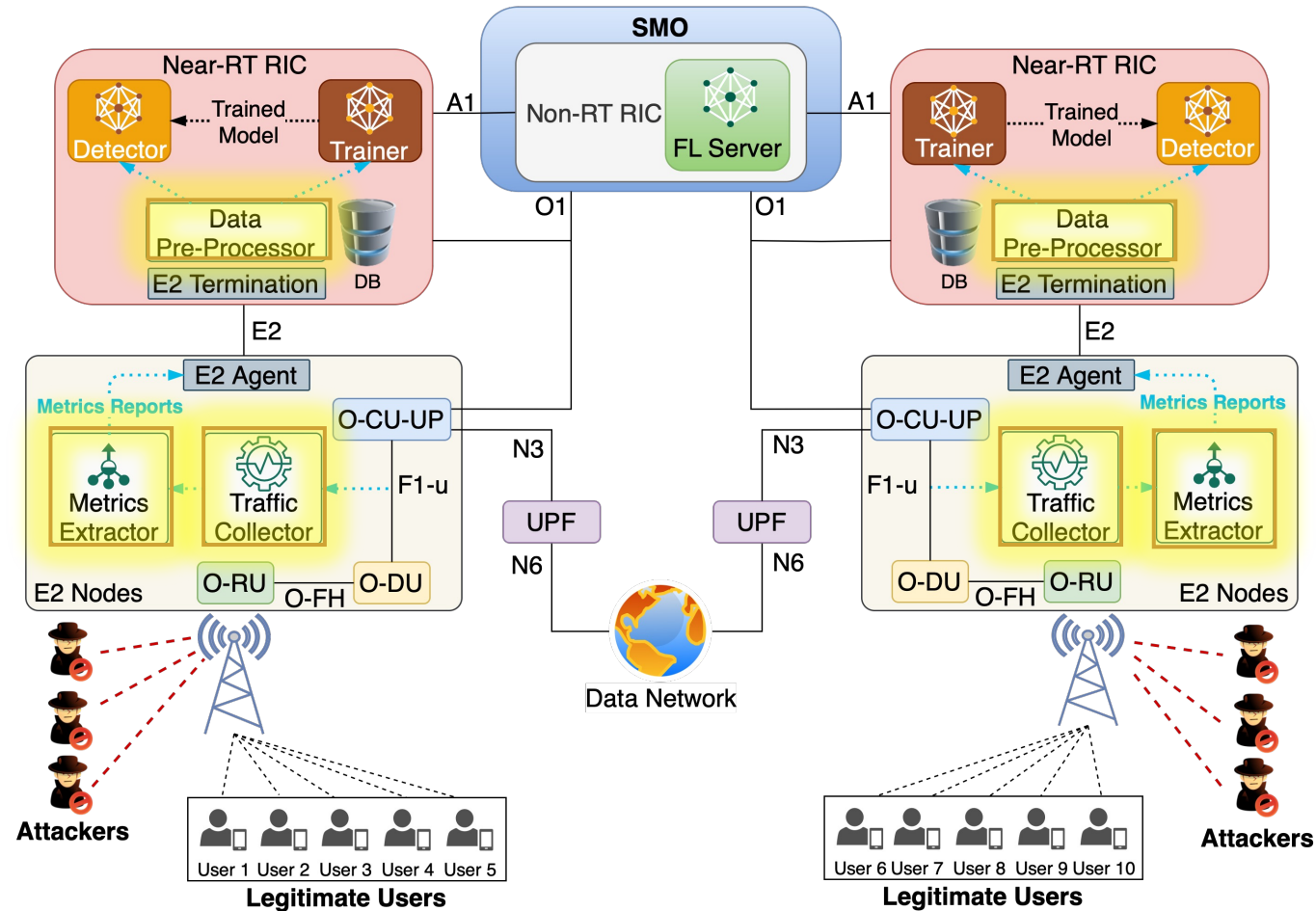
# TenaxDoS – A FCL-based DDoS Detection Framework (2/6)

- Attack detection is powered by a DL model trained following **Federated Continual Learning (FCL)** approach
  - Facilitate knowledge sharing
  - Avoid the sharing of local data
  - Address the CF concern



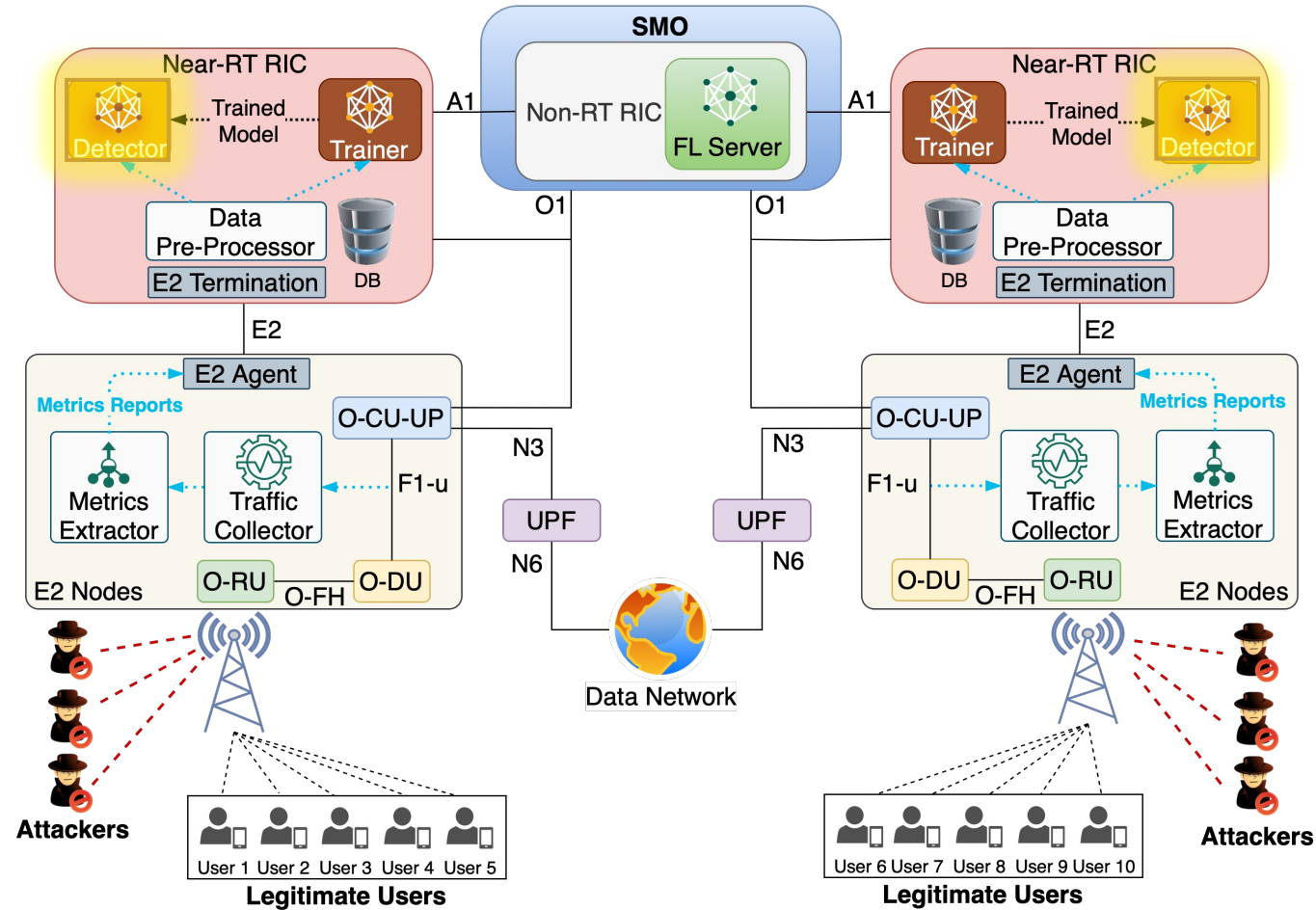
# TenaxDoS – A FCL-based DDoS Detection Framework (3/6)

- TenaxDoS encompasses six core components
  - **Traffic Collector** – continuously captures the user plane traffic over the F1-u interface
  - **Metrics Extractor** – extracts the network flow's features (from the collected traffic) pertinent to identify malicious patterns caused by DDoS attacks
    - Extracted features are streamed to the near-RT RIC in the form of metrics reports via the E2 interface
  - **Data Pre-Processor xApp** – transforms the raw data in the metrics reports into appropriate format to fit for the DL model



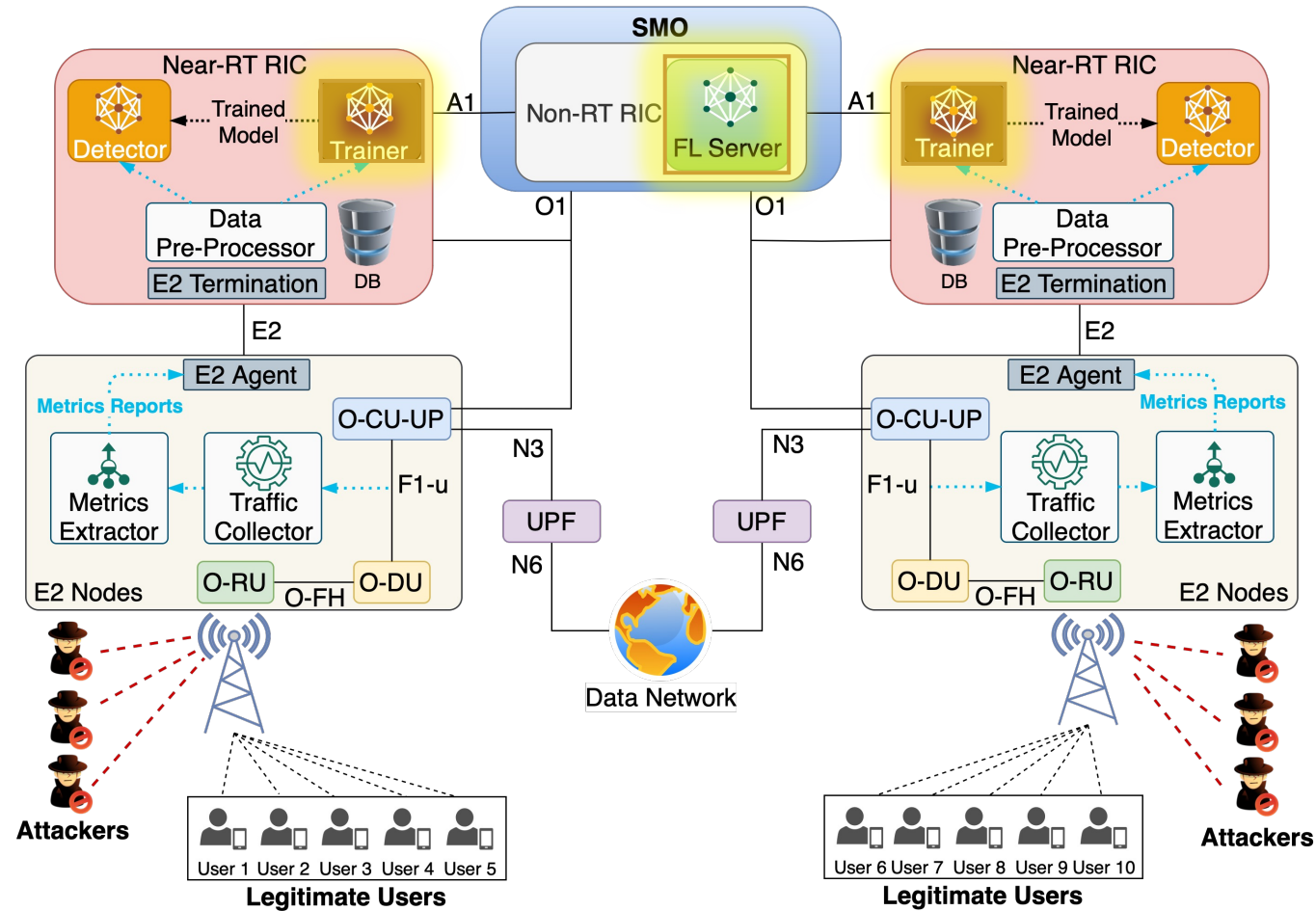
# TenaxDoS – A FCL-based DDoS Detection Framework (4/6)

- TenaxDoS encompasses six core components
  - **Detector xApp** – incorporates a DL-powered DDoS detection model trained following an FCL approach
    - Analyses the pre-processed network flow's features to decide on the legitimacy or maliciousness of the received traffic
    - Issues a security policy for enforcement on E2 Nodes to mitigate the DDoS attack
      - Blocking the F1-u GTP tunnel of UE's PDU session source of the malicious traffic



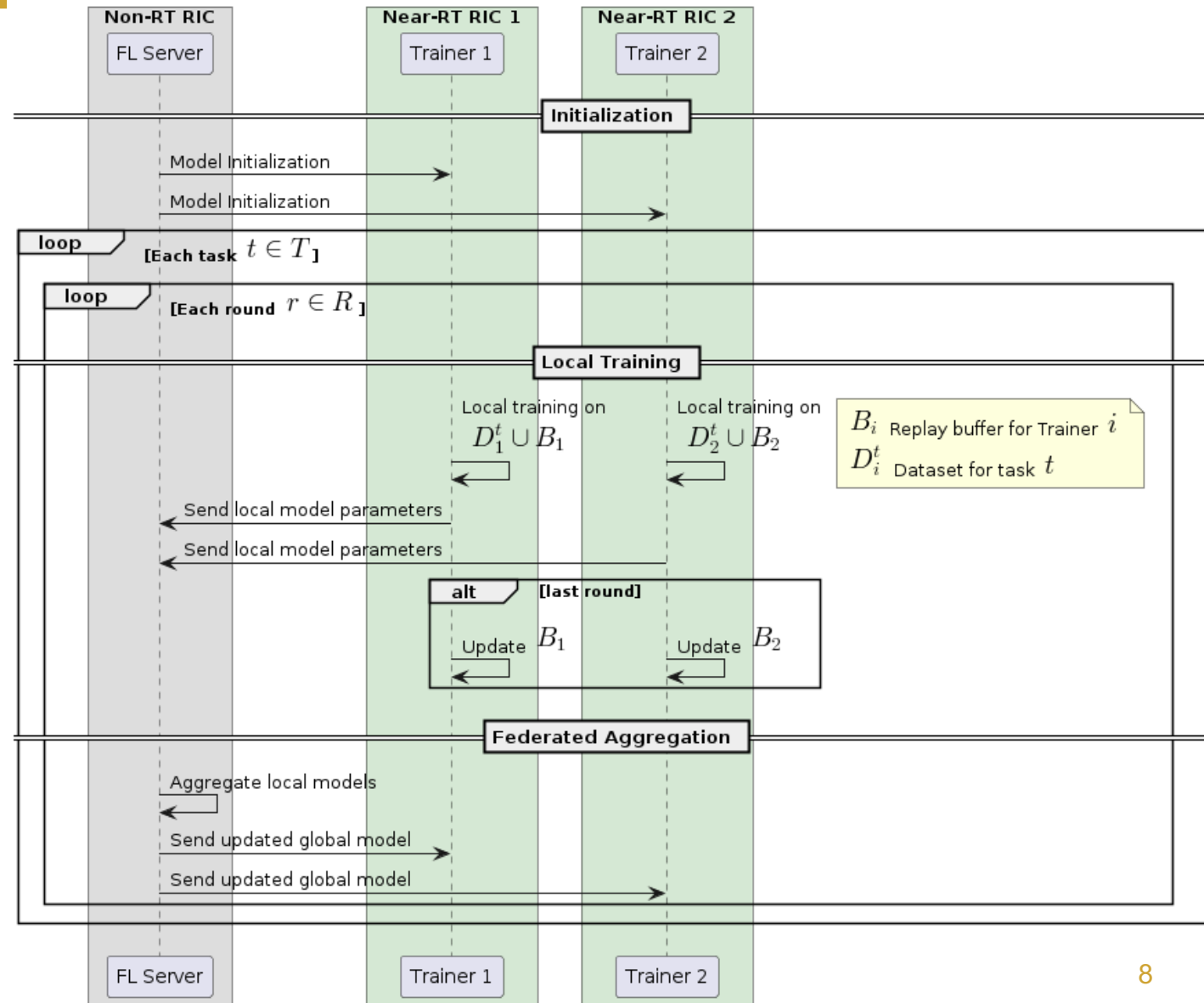
# TenaxDoS – A FCL-based DDoS Detection Framework (5/6)

- TenaxDoS encompasses six core components
  - **Trainer xApps** – perform local training of the local DL-powered DDoS detection model
  - **FL Server rApp** – acts as the central server in charge of training the global model by aggregating the local models' updates



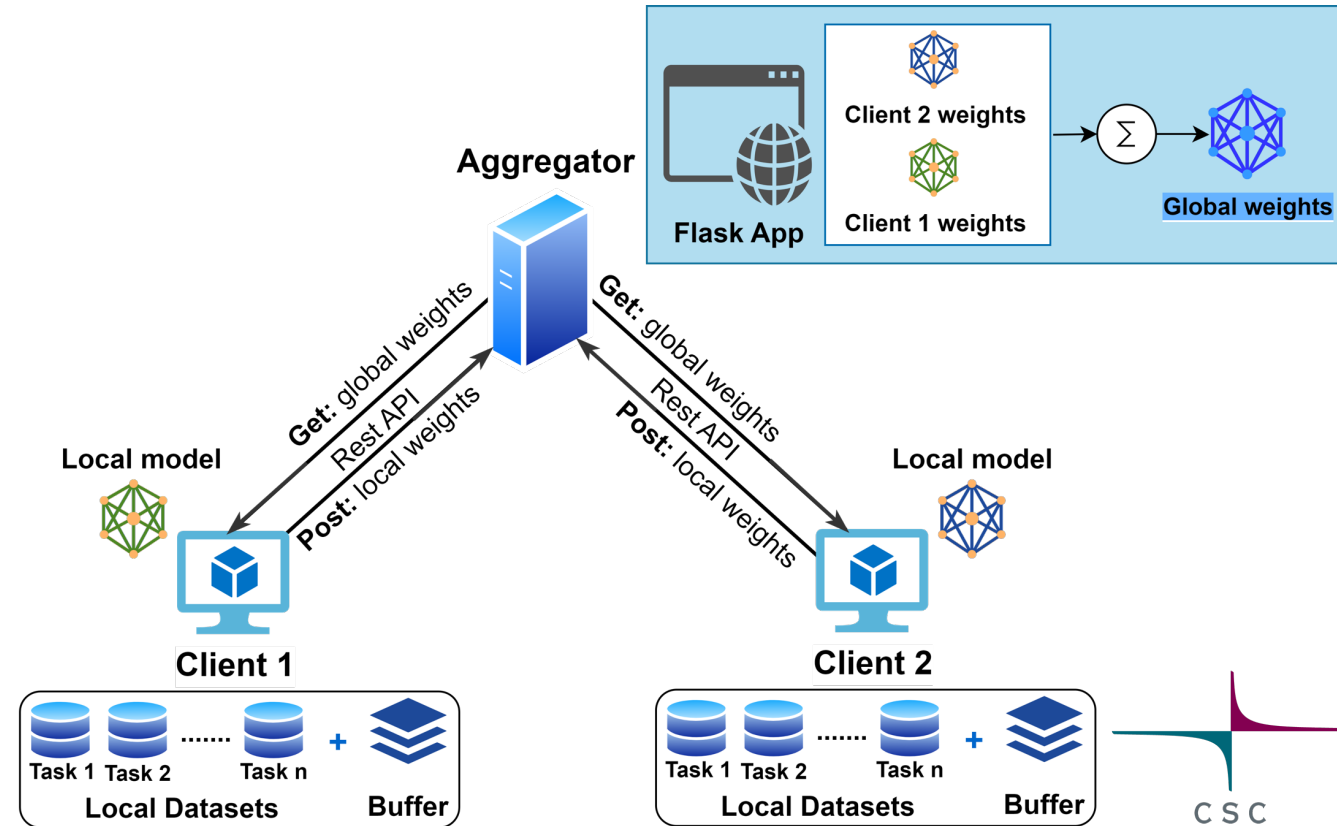
# TenaxDoS – A FCL-based DDoS Detection Framework (6/6)

- **Rehearsal-based strategy** with **reservoir sampling** adopted to tackle CF
- Each **Trainer** maintains a **fixed-size buffer memory**
  - to **store** representative network flow **samples** from **past tasks**
  - the buffer content is replayed when learning new tasks
  - **Reservoir sampling** technique decides whether to keep or reject a new sample based on a given probability



# Performance Evaluation Results

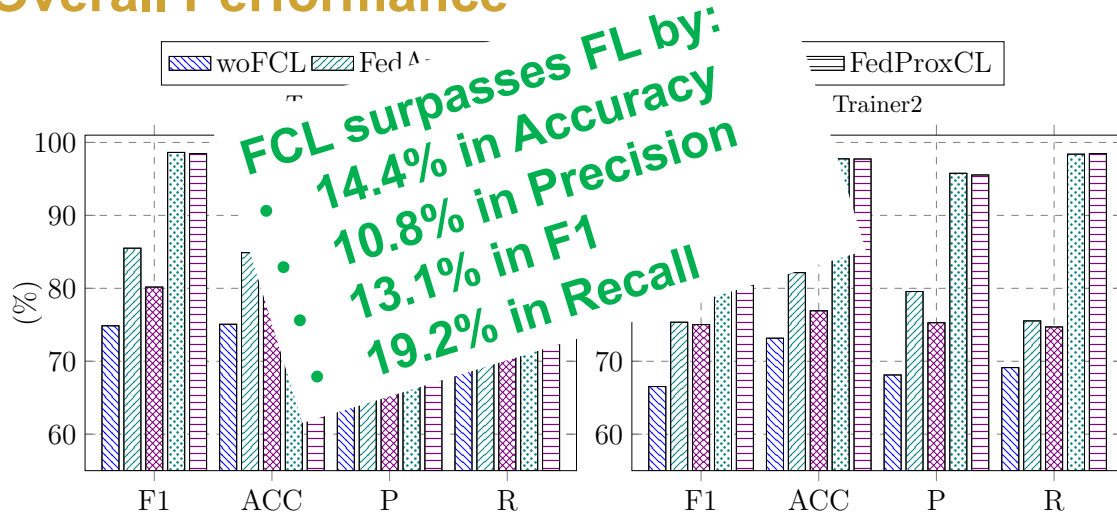
- 5G-NIDD dataset – a dataset for network intrusion detection generated using 5GTN testbed in Oulu through 2 bases stations
- Tasks** – different attack classes (9 classes of DDoS attack)
- Evaluation metrics
  - Average Performance Metrics**
    - Accuracy (ACC),
    - Precision (P),
    - F1-Score (F1),
    - Recall (R)
  - Backward Transfer (BWT)**
    - Degree of forgetting older tasks after training on a new task
  - Forward Transfer (FWT)**
    - Ability to generalize to future tasks



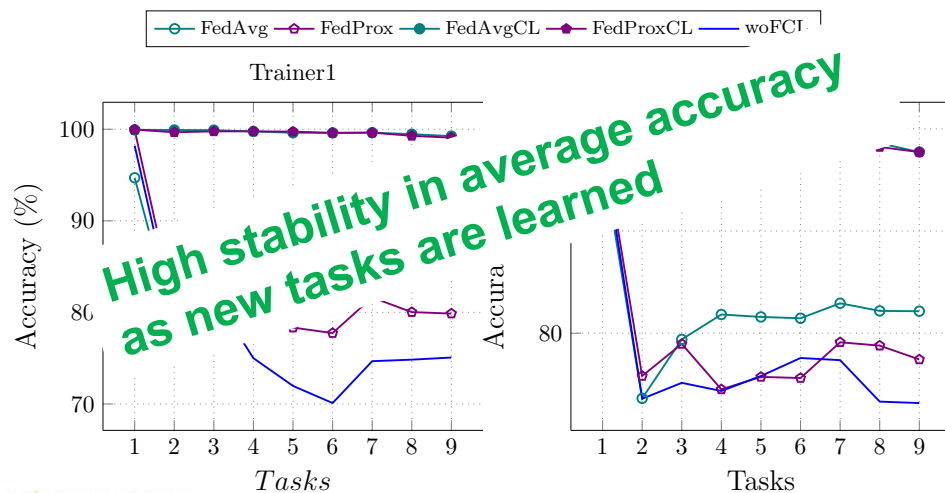
Experimental Setup

# Performance Evaluation Results

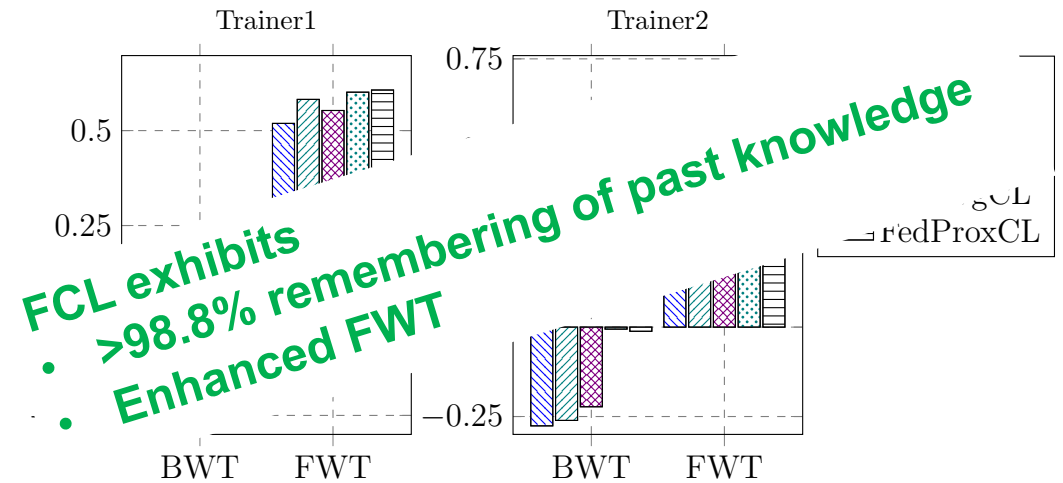
## Overall Performance



## Average Accuracy



## Catastrophic Forgetting



# Conclusion & Future Work

- We proposed **TenaxDoS**, a novel **FCL-based cooperative network anomaly detection** framework in an O-RAN environment
  - **Timely** and **continuous** detection of network anomalies **at the edge**
  - fosters **multi-operator collaboration** in a **privacy-preserving** way
- Future Work
  - Extend TenaxDoS to support fully decentralized asynchronous FCL
  - Handling more realistic scenarios where DDoS attacks arrive to base stations with different orderings

**MOSA!C LAB**

Mobile Network Softwarization & Service Customization



For further updates, visit us at

**[www.mosaic-lab.org](http://www.mosaic-lab.org)**

More than wireless.

---



**FLAGSHIP**  
UNIVERSITY  
OF OULU

6GFLAGSHIP.COM • #6GFLAGSHIP

