Francesco Cerasuolo

Continuous and Adaptive Learning for Traffic Analysis in the New Internet Era

Tutor: Prof. Antonio Pescapè

Cycle: XXXVIII Year: First

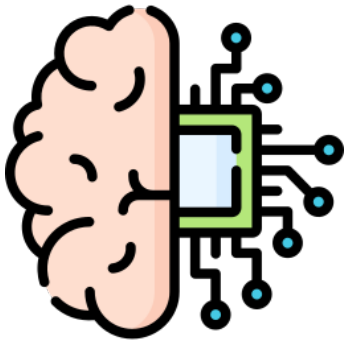
My background

- **MSc degree:** MSc degree in Computer Engineering from University of Naples Federico II
- **Research group/laboratory:** Traffic Group/ARCLab
- **PhD start date:** 01/11/2022
- **Scholarship type:** Unina
- **Collaboration:** Huawei

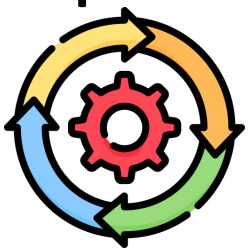
Research field of interest

- **Network Traffic Analysis (NTA)**
  - Collecting and inspecting network data
  - Understand and enhance performance

The increasing **network traffic** requires efficient management to ensure security and QoS. This task is primarily executed using **ML/DL methods** but the traffic is *dynamic* and *constantly evolving*…



- **Lifelong Learning:**
  - Allows the model **to learn and continuously adapt to new information** while **retaining old knowledge**
  - **Time and resource saving**



Summary of study activities

- **Ad hoc PhD courses / schools**
  - Statistical data analysis for science and engineering research
  - On the challenges and impact of Artificial Intelligence in the Insurance domain
  - IoT Data Analysis
  - Using Deep Learning properly
- **Courses borrowed from MSc curricula**
  - Data Analytics
- **PhD School**
  - TMA PhD School, Università degli Studi di Napoli Federico II

Summary of study activities

- **16 seminars**

- **Conferences**
  - Italian Conference on CyberSecurity (ITASEC) Conference, 2-5 May 2023, Bari

    Presentation of the Paper: *A Comparison of Machine and Deep Learning Models for Detection and Classification of Android Malware Traffic*
  - Network Traffic Measurement and Analysis (TMA) Conference, University of Napoli Federico II, 28-29 June 2023

    Presentation of the Poster: *Class Incremental Learning for Mobile Traffic Classification*

Research Question

Mobile-App Traffic Classification Challenges:

- ***Number of new apps constantly rising***
  - 4.67 million apps during Q3 2021

- ***Traffic Classification Systems outdated***
  - ML/DL models must be re-trained to classify the newly published apps

Research Question: *How to update a model with new information, without retraining from scratch each time a new app is released?*

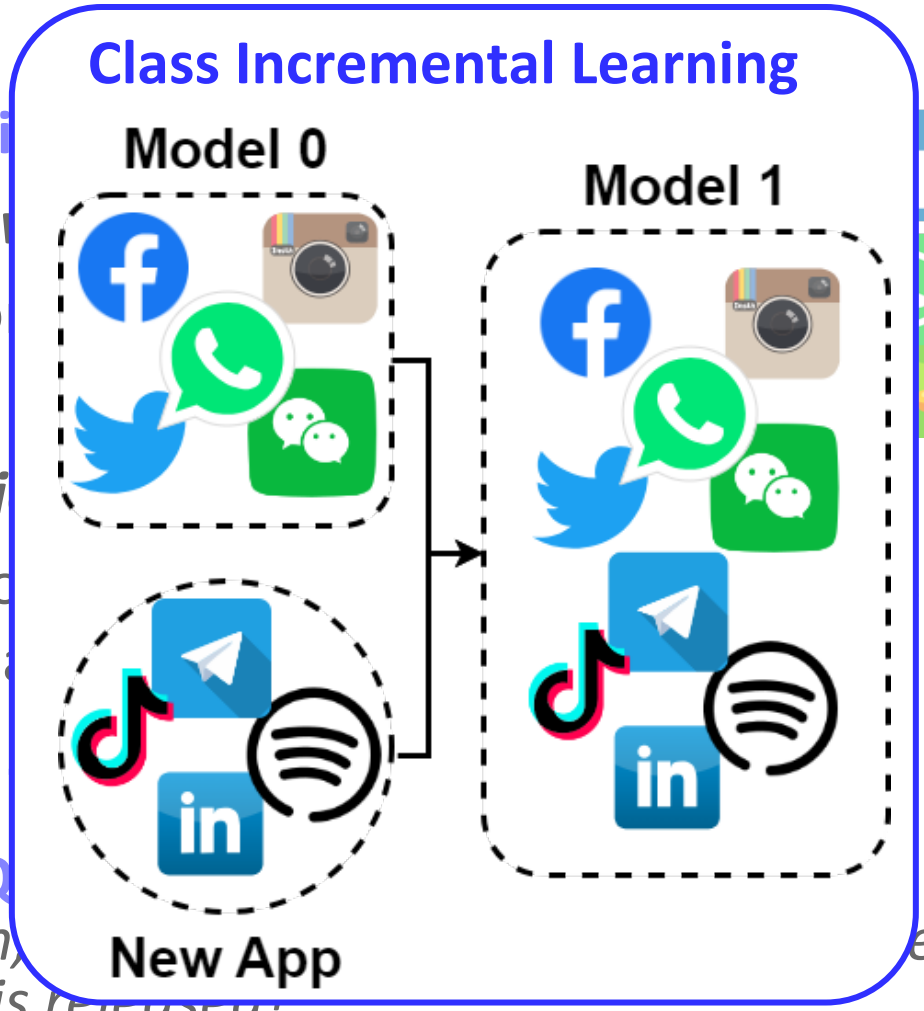
Research Question

Mobile-App Traffi

- ***Number of ne***
  - 4.67 millio

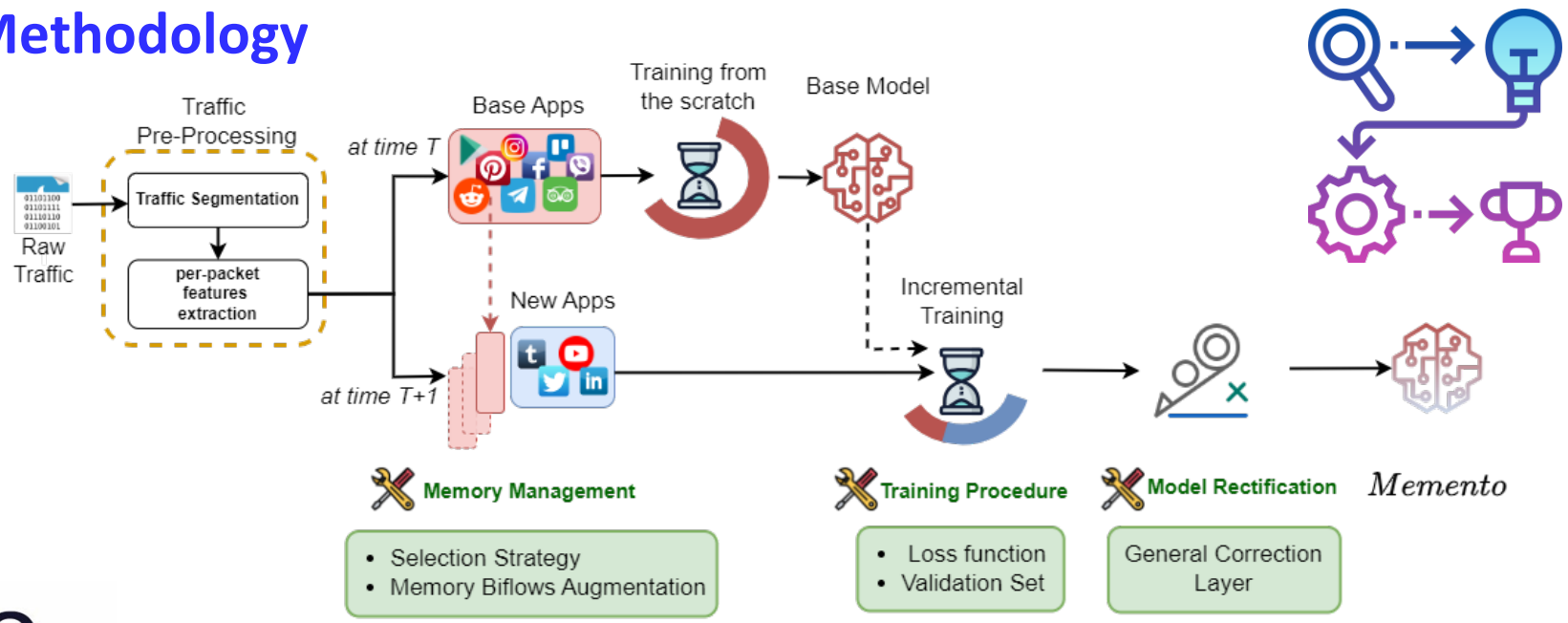
- ***Traffic Classifi***
  - ML/DL mo ify the newly published

Research Q *with new information each time a new app is released?*



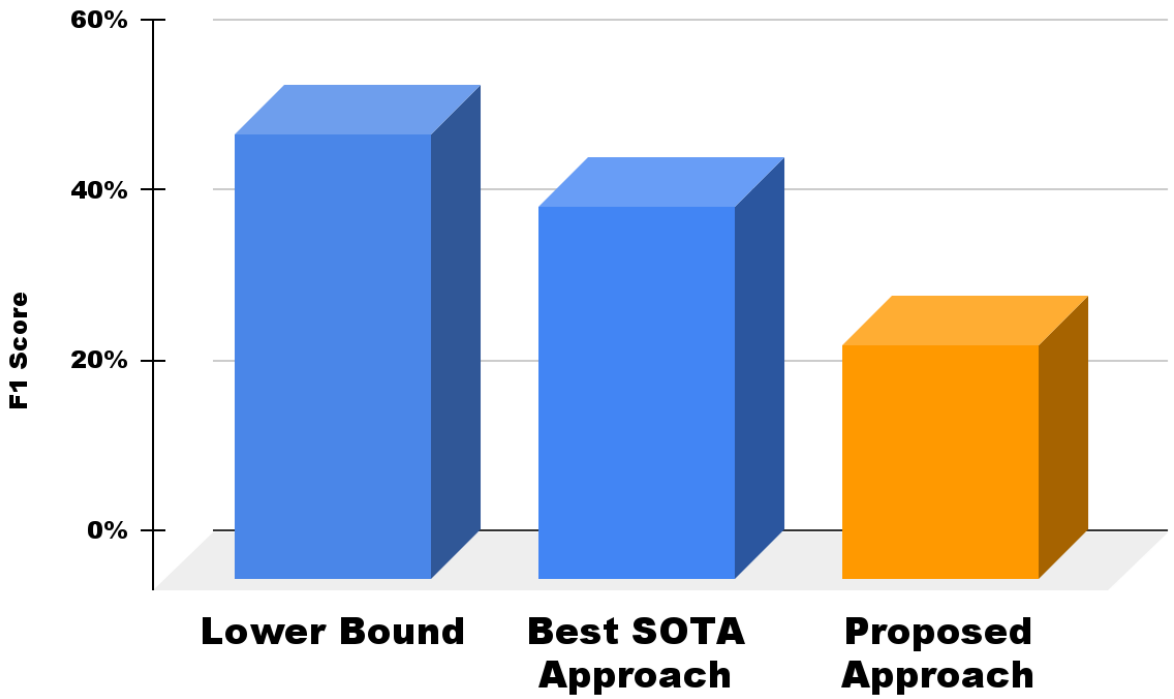
Class Incremental Learning

- **Objective**
  - Design of a new and more efficient **Incremental Classifier** for **Encrypted Network Traffic**
  - Improve state-of-the-art performance in classifying new added apps without **forgetting** already-acquired knowledge
- **Methodology**



Class Incremental Learning

Performance difference for a new app w.r.t. ideal model



- Selection Strategy
- Memory Biflows Augmentation

- Loss function
- Validation Set

General Correction Layer

Products

[J1]	*MEMENTO: A Novel Approach for Class Incremental Learning of Encrypted Traffic*, **F. Cerasuolo**, A. Nascita, G. Bovenzi, G. Aceto, D. Ciuonzo, Antonio Pescapè, Dario Rossi, *submitted to Elsevier Computer Networks*
[C1]	*Explainable Mobile Traffic Classification: the case of Incremental Learning*, A. Nascita, **F. Cerasuolo**, G. Aceto, D. Ciuonzo, V. Persico, A. Pescapè, *submitted to International Conference on emerging Networking EXperiments and Technologies Workshop on "Explainable and Safety Bounded, Fidelitous, Machine Learning for Networking"*
[C2]	*Adaptive Intrusion Detection Systems: Class Incremental Learning for IoT Emerging Threats*, **F. Cerasuolo**, G. Bovenzi, C. Marescalco, F. Cirillo, D. Ciuonzo, A. Pescapè, submitted to *IEEE International Conference on Big Data Workshop "Machine Learning for Securing IoT Systems Using BigData"*

Next Year

- Exploration of different approach families for addressing **incremental expansion** in network traffic scenarios
- Usage of **multimodal architectures** to more effectively harness the diversity present in network traffic
- Investigation of **concept drift** in mobile network traffic
- **Class removal** from a classifier

Thank you for the attention!