UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

itee PhD information technology electrical engineering

DIETI UNINA

Alfredo Nascita

eXplainable Artificial Intelligence for Network Traffic Analysis

Tutor: Prof. Valerio Persico

Cycle: XXXVII Year: Second

itee PhD information technology electrical engineering

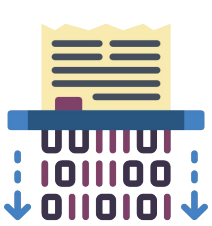
My background

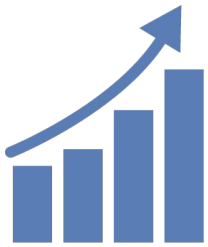
- MSc degree: MSc degree in Computer Engineering, University of Napoli Federico II
- PhD start date: 01/11/2021
- Research group/laboratory: Traffic Group/ARCLab
- Scholarship type: Unina

Research field of interest

- Network Traffic Analysis (NTA)
  - Collecting and examining network data
  - Understand and improve network performance

- Challenges
  - Rapid traffic growth
  - Network Heterogeneity & Dynamicity
  - Encryption Protocols

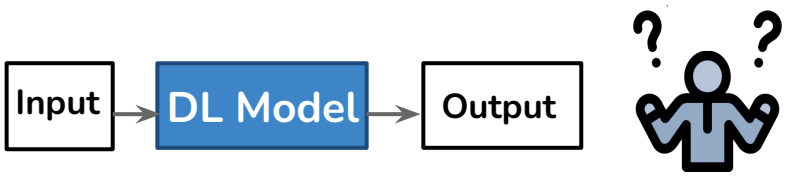




Research activity: Overview

Deep Learning is a promising strategy, to face these challenges but…

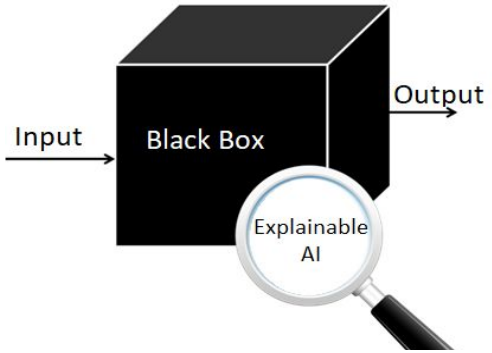
- Complex Architectures
- Black-box nature
- Lack of Interpretability



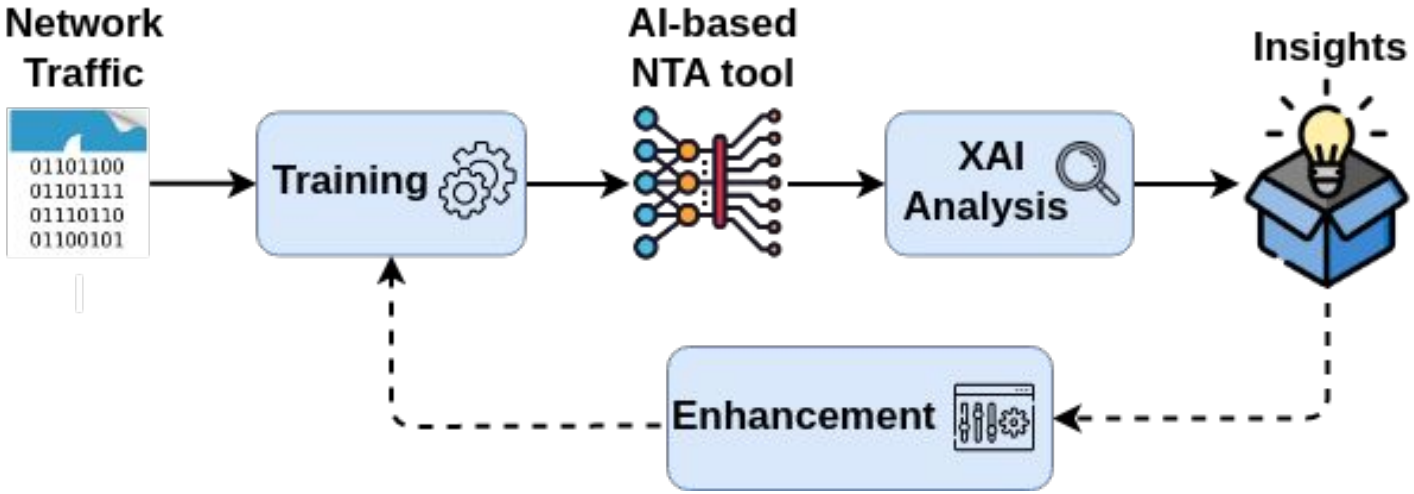
Network operators **struggle to understand inner workings and logic** of Artificial Intelligence (AI) models and tools

eXplainable Artificial Intelligence (XAI)

- Analyze models and data biases
- Justify model behaviours
- Enhance trust in decisions



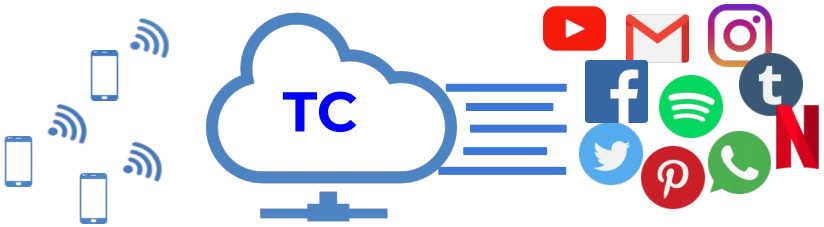
eXplainable NTA



Traffic Classification (TC)

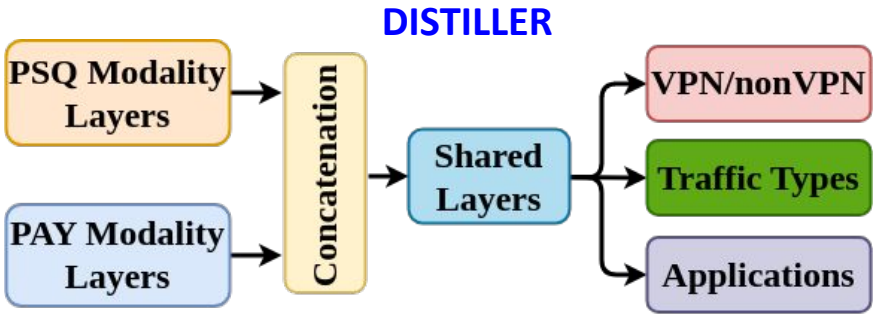
"What is flowing through my network?"

TC aims to associate **traffic objects** with the **apps/services** generating them



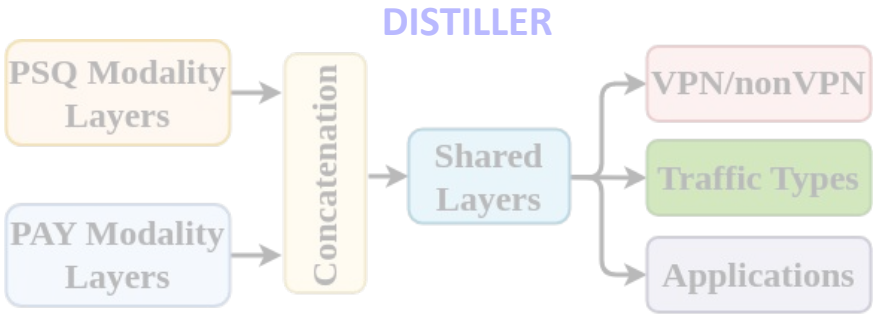
Multimodal & Multitask TC

- **Multimodal: different traffic views**
  - **PSQ:** Fields of the first 32 pkts
  - **PAY:** 784 Bytes of L4 payload
- **Multitask: multiple TC tasks simultaneously**



Multimodal & Multitask TC

- **Multimodal: different traffic views**
  - **PSQ:** Fields of the first 32 pkts
  - **PAY:** 784 Bytes of L4 payload
- **Multitask: multiple TC tasks simultaneously**

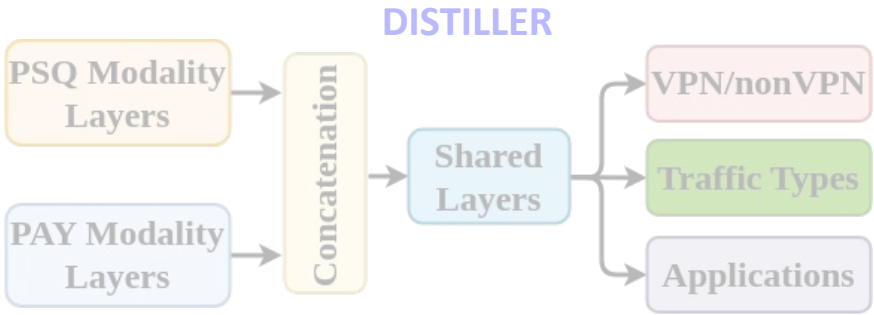


Methodology

- **Interpretability**: SHAP, Integrated Gradients
- **Architectural Improvements**
- **Calibration** Analysis
- **Compression Techniques** (Pruning, Quantization, …)

Multimodal & Multitask TC

- **Multimodal: different traffic views**
  - **PSQ:** Fields of the first 32 pkts
  - **PAY:** 784 Bytes of L4 payload
- **Multitask: multiple TC tasks simultaneously**



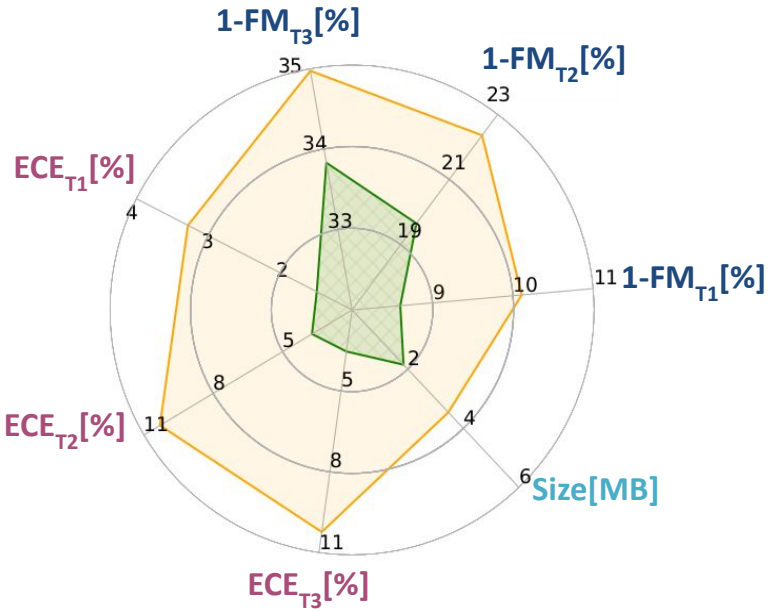
Methodology

- **Interpretability**: SHAP, Integrated Gradients
- **Architectural Improvements**
- **Calibration** Analysis
- **Compression Techniques** (Pruning, Quantization, …)

Results

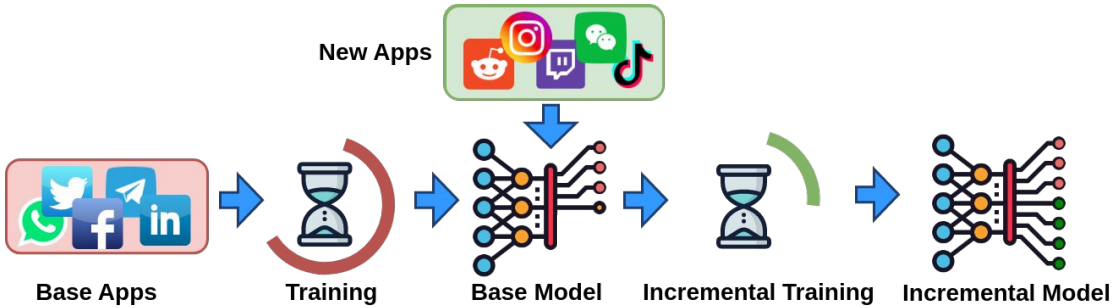
- **Reliability:** - 50% Expected Calibration Error
- **Feasibility:**
  - XAI-driven input reduction (12 pkts, 256 bytes)
  - -58% Training Times, -50% Model Size
- **Performance:** + 2% F-Measure

DISTILLER ➡ MY PROPOSAL



Smaller area ⟶ better model

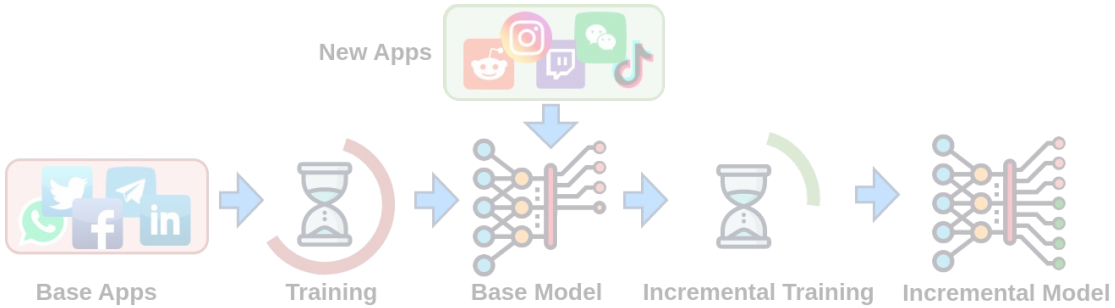
The Incremental Case



Class Incremental Learning (CIL)

Training from scratch

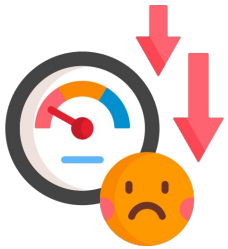
The Incremental Case



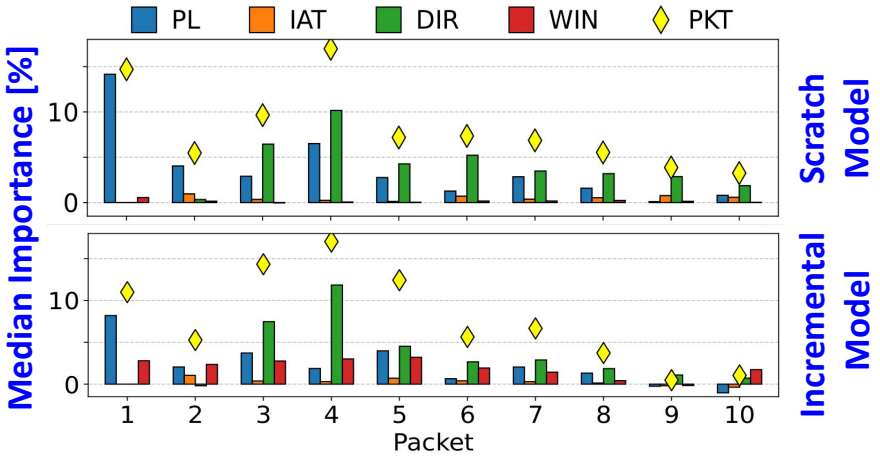
Class Incremental Learning (CIL)

Training from scratch

- Performance of CIL approaches is **not satisfactory** (significant gap w.r.t. the scratch model)



- New XAI-based methodology to **grasp differences** between scratch and incremental models
  - **Input Importance**
  - Analysis of **Base Models**
  - Analysis of **Incremental Models**



Summary of study activities

- Ad hoc PhD courses:
  - On the challenges and impact of Artificial Intelligence in the Insurance domain
  - Using Deep Learning properly
  - IoT Data Analysis

- 13 Seminars

- PhD School:
  - Network Traffic Measurement and Analysis (TMA) PhD School

Summary of study activities

- Tutorship:
  - Co-supervisor of two master theses in Computer Engineering on the XAI topic
  - practical lectures/seminars during the courses of *Internet Data Analysis* and *Computer Networks* (Master and Bachelor Degree in Computer Engineering)

- Conferences:
  - 19th Italian Networking Workshop 2023 (INW2023)
    Presentation of the Contribution: *Extending Traffic Classifiers to New Applications via Class-Incremental Learning*
  - Italian Conference on Cybersecurity 2023 (ITASEC2023)
    Presentation of the Article: *Machine and Deep Learning Approaches for IoT Attack Classification*
  - 7th edition of the Network Traffic Measurement and Analysis Conference (TMA Conference 2023)

Products

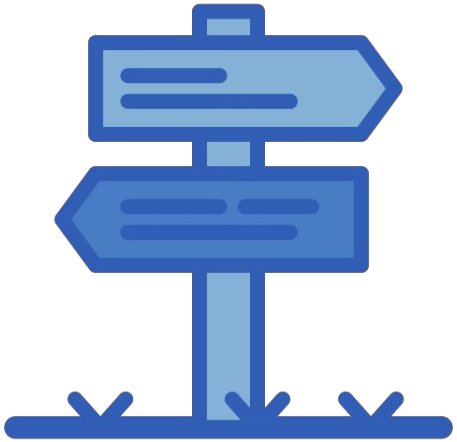
[J1]	*Improving Performance, Reliability, and Feasibility in Multimodal Multitask Traffic Classification with XAI,* **A. Nascita**, A. Montieri, G. Aceto, D. Ciuonzo, V. Persico, A. Pescapé. *Accepted for publication in IEEE Transactions on Network and Service Management (TNSM) 2023*
[J2]	*Benchmarking Class Incremental Learning in Deep Learning Traffic Classification*, G. Bovenzi, **A. Nascita**, L. Yang, A. Finamore, G. Aceto, D. Ciuonzo, A. Pescapé, D Rossi. *Accepted for publication in IEEE Transactions on Network and Service Management (TNSM) 2023*
[J3]	*MCOTM: Mobility-Aware Computation Offloading and Task Migration for Edge Computing in Industrial Iot*, W. Qin, H. Chen, L. Wang, Y. Xia, **A. Nascita**, A. Pescapé. *Accepted for publication in Elsevier Future Generation Computer Systems (FGCS) journal*
[J4]	*MEMENTO: A Novel Approach for Class Incremental Learning of Encrypted Traffic*, F. Cerasuolo , **A. Nascita** , G. Bovenzi , G. Aceto , D. Ciuonzo , A. Pescapé , D. Rossi. *Submitted to Elsevier Computer Networks*

Products

[J5]	*An Integration Perspective of Security, Privacy, and Resource Efficiency for IoT-Fog Networks*, S. Javanmardi, **A. Nascita**, A. Caruso, G. Loukas, A. Pescapè, *submitted to IEEE Communications Magazine*
[C1]	*Cross-Evaluation of Deep Learning-based Network Intrusion Detection Systems*, C. Guida, **A. Nascita**, A. Montieri, A. Pescapé, *accepted for presentation in the 10th International Conference on Future Internet of Things and Cloud (FiCloud 2023)*
[C2]	*Explainable Mobile Traffic Classification: the case of Incremental Learning*, **A. Nascita**, F. Cerasuolo, G. Aceto, D. Ciuonzo, V. Persico, A. Pescapé, *accepted for presentation in the 19th International Conference on emerging Networking EXperiments and Technologies, Workshop on 'Explainable and Safety Bounded, Fidelitous, Machine Learning for Networking'*

WiP / Next Year

- Extend analysis on the **incremental case** to develop **adaptive and interpretable** classifiers
- Explainability for other NTA problems (e.g., **anomaly detection**)
- **Explainability-by-design** approaches
- **Research period abroad** at Huawei France



Thank you for the attention!