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: First

itee PhD information technology electrical engineering

My background

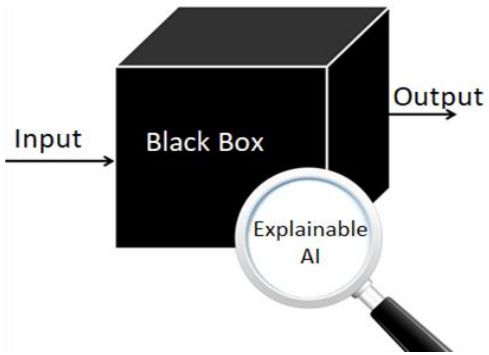
- MSc degree: MSc degree in Computer Engineering from University of Naples Federico II
- Research group/laboratory: Traffic Group/ARCLab
- PhD start date: 01/11/2021
- Scholarship type: Unina

Research field of interest

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

Network operators need to understand inner workings and logic behind Artificial Intelligence models and tools

- eXplainable Artificial Intelligence (XAI)
  - Analyze models and data biases
  - Justify model behaviours
  - Enhance trust in decisions



Summary of study activities

- Ad hoc PhD courses:
  - Statistical data analysis for science and engineering research
  - Imprenditorialità Accademica
  - Machine Learning for Science and Engineering Research

- Courses attended borrowed from MSc curricula:
  - Network Security (Computer Engineering MSc)

- PhD Schools:
  - Network Traffic Measurement and Analysis (TMA) PhD School
  - eXplainable Artificial Intelligence Summer School (XAISS)

Summary of study activities

- 19 seminars

- Conferences:
  - INFOCOM 10th International Workshop on Security and Privacy in Big Data (BigSecurity) 2022
  - ISCC 2nd IEEE International Workshop on "Distributed Intelligent Systems" (DistInSys) 2022
  - Ital-IA 2022, Secondo Convegno Nazionale CINI sull'Intelligenza Artificiale

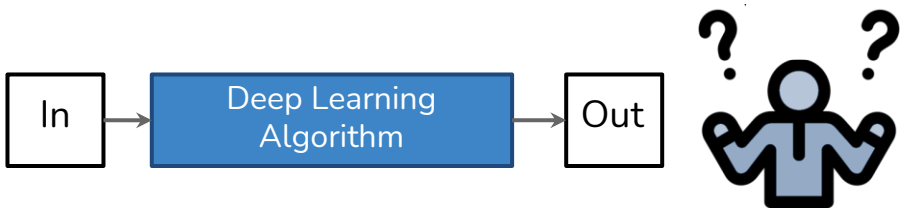
Research activity: Overview

Network Traffic Analysis Challenges

- Encryption Protocols
- Network Heterogeneity & Dynamicity
- Traffic rapid growth

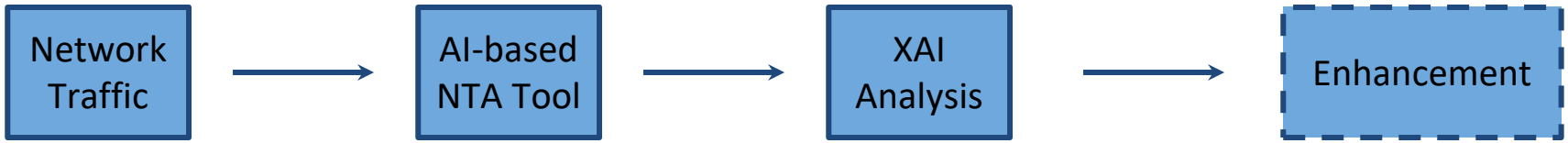
Deep Learning is a promising approach to face these unprecedented challenges, but… why should we trust it?

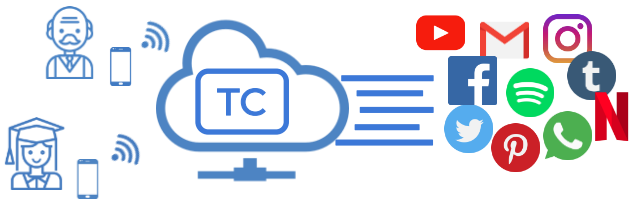
- Complex Architectures
- Black-box nature
- Lack of Interpretability



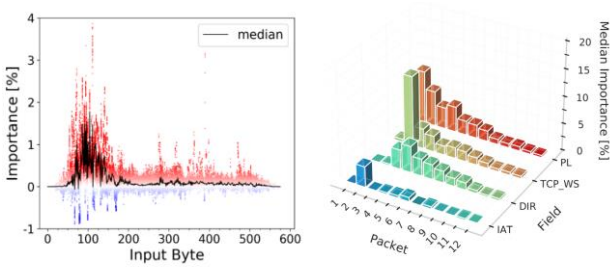
eXplainable NTA

- Objective
  - Obtain Explainability for AI-based NTA decisions
  - Design and Implementation of more efficient and effective tools
- Methodology





Mobile Traffic Classification



Input Importance (SHAP, IG)
Calibration Analysis

Input size reduction
Timeliness of decisions
Calibrated outputs

Products

[P1]	*Improving Performance, Trust, and Feasibility in Multitask Traffic Classification with XAI,* A. Nascita, A. Montieri, G. Aceto, V. Persico, A. Pescapé, submitted to *IEEE Transactions on Network and Service Management (TNSM)* 2022 - *under review*
[P2]	*A Comparison of Machine and Deep Learning Models for Detection and Classification of Android Malware Traffic, G. Bovenzi, F. Cerasuolo, A. Montieri, A. Nascita, V. Persico, A. Pescapé, ISCC 2nd IEEE International Workshop on Distributed Intelligent Systems (DistInSys) – published*
[P3]	*Machine and Deep Learning Approaches for IoT Attack Classification*, A. Nascita, F. Cerasuolo, D. Di Monda, J. T. A. Garcia, A. Montieri, and A. Pescapè. INFOCOM 10th International Workshop on Security and Privacy in Big Data (BigSecurity) - published
[P4]	*On the Integration of Blockchain and SDN: Overview, Applications, and Future Perspectives* - A. Rahman, A. Montieri, D. Kundu, Md R. Karim, Md J. Islam, S. Umme, A. Nascita, A. Pescapé, *Springer's Journal of Network and Systems Management, Special Issue on Blockchains and Distributed Ledgers in Network and Service Management - published*

Next Year

- Explainability for other NTA problems
  (e.g., Anomaly detection or Traffic Prediction)
- Investigation of Explainability-by-design approaches
- Comparative evaluation of XAI methods
  (properties and metrics for explanations)

Thank you for the attention!