UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

itee PhD information technology electrical engineering

DIETI

UNINA

Francesco Cerasuolo

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

Tutor: Prof. Antonio Pescapè

Cycle: XXXVIII

Year: Third

itee PhD information technology electrical engineering

Background information

- **MSc degree**: Computer Engineering
- **Research group/laboratory**: **Traffic Group/ARCLab**
- **PhD start date**: 01/11/2022
- **PhD end date**: 30/11/2025

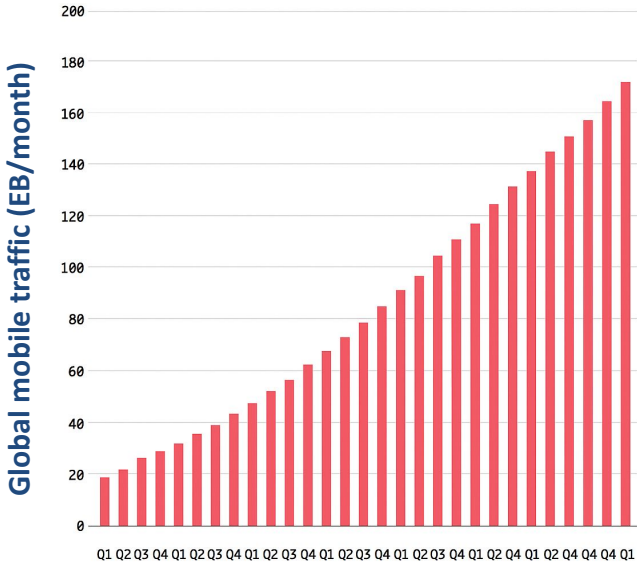
- **Scholarship type**: **UNINA**

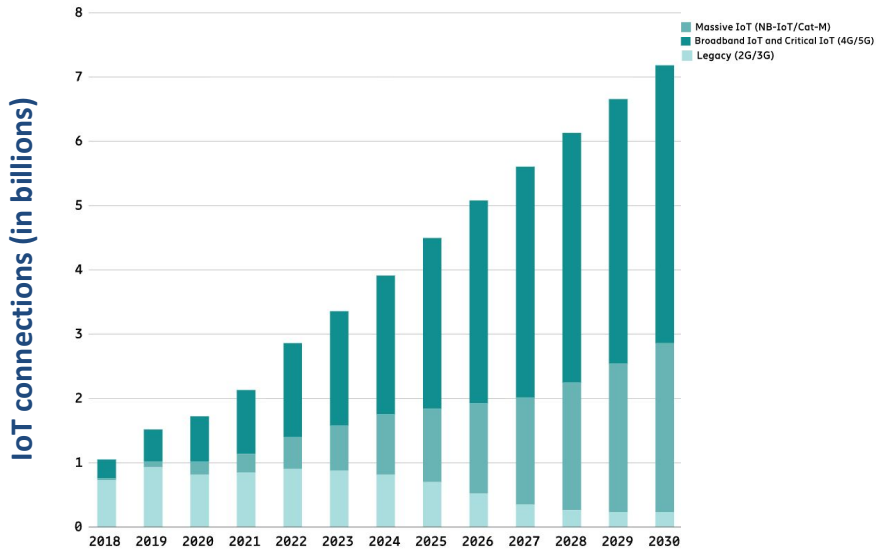
- **Involved Projects:**
  - **Innovation Lab** funded by **Huawei**

- **Research Period Abroad**: **University of Edinburgh**, Edinburgh, Scotland (03/10/2024 - 03/03/2025)

Research Area

Network traffic has grown exponentially, driven by the **widespread adoption** of **smartphones** and **Internet of Things (IoT)** devices





How to handle these changes?

Network Traffic Classification (TC)

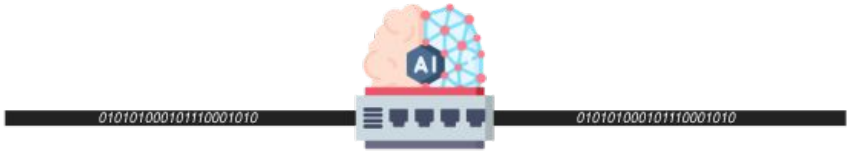
What's going through my network?

Applications

Resource Management
Traffic Engineering
Security

Research Area

Nowadays, recent research has increasingly leveraged **Machine and Deep Learning (ML and DL)** to automate classification tasks and enhance performance. While ML depends on hand-crafted features, DL learns directly from data, yet **challenges persist**



Continuous update

How can models *accurately classify* ever-changing network traffic *without full retraining*?

Adaptability

How can models maintain *high accuracy* when deployed in *different network environments*?

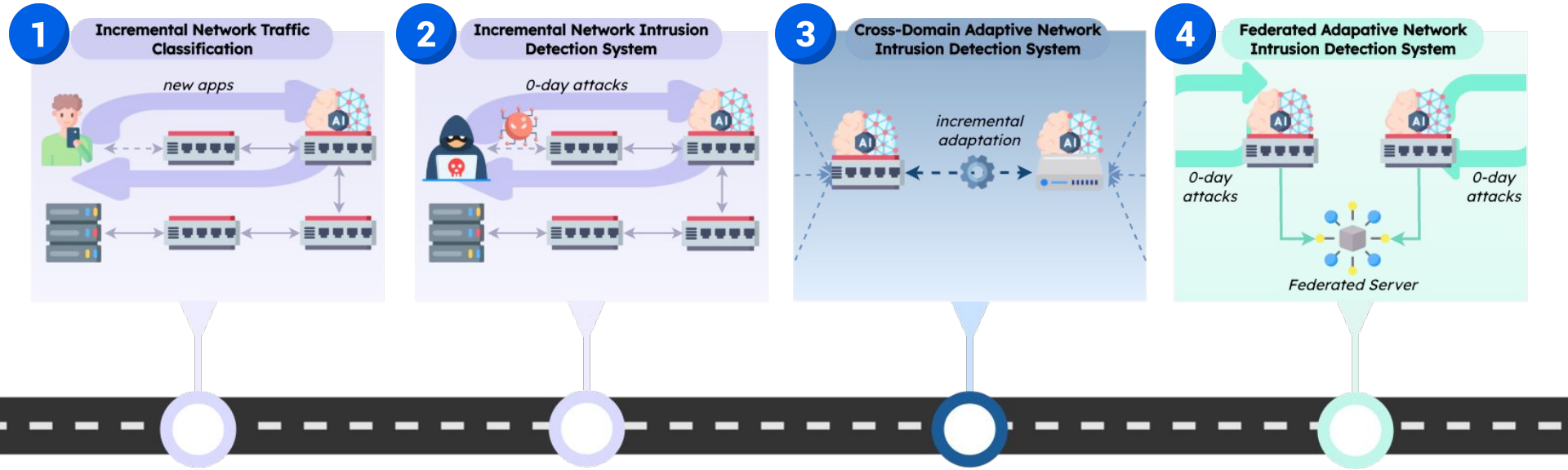
Decentralized Data

How can models be collaboratively trained in a *decentralized* manner to preserve *network data privacy* while ensuring *strong global performance*?

PhD thesis: in brief

This thesis proposes a new **incremental and adaptive methodology** for AI systems, enabling **continuous learning**, **dynamic adaptation**, and **privacy-preserving** operation for network traffic in **modern network environments**

PhD thesis: overview



Network Traffic Classification: basics

T = t_0: Train classifier from scratch with available apps/traffic types

Traditional learning paradigm:

- When new apps/traffic appear, **retrain from scratch** with all data

Drawbacks:

- Computationally **expensive**
- **Inefficient**—previous knowledge is not reused

Benefits:

- **Upper bound** for performance

Incremental learning paradigm:

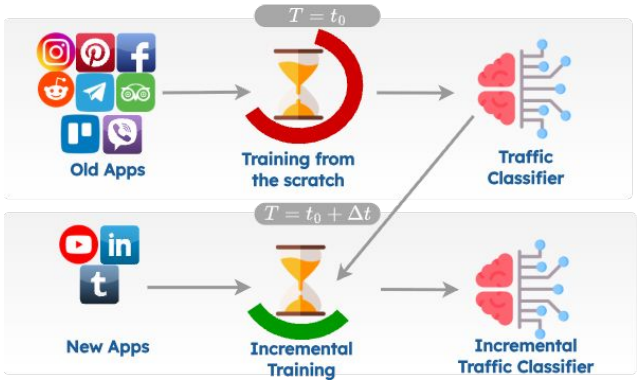
- When new apps/traffic appear, **update the existing classifier incrementally**

Drawbacks:

- **Forgetting** of old knowledge
- **Inability** of including new classes

Benefits:

- **Lower resource demanding**



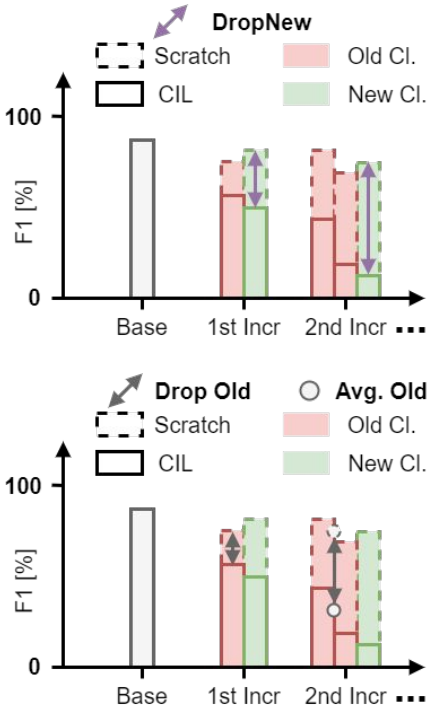
Incremental Learning: basics

To reduce forgetting, **different strategies** are enforced:

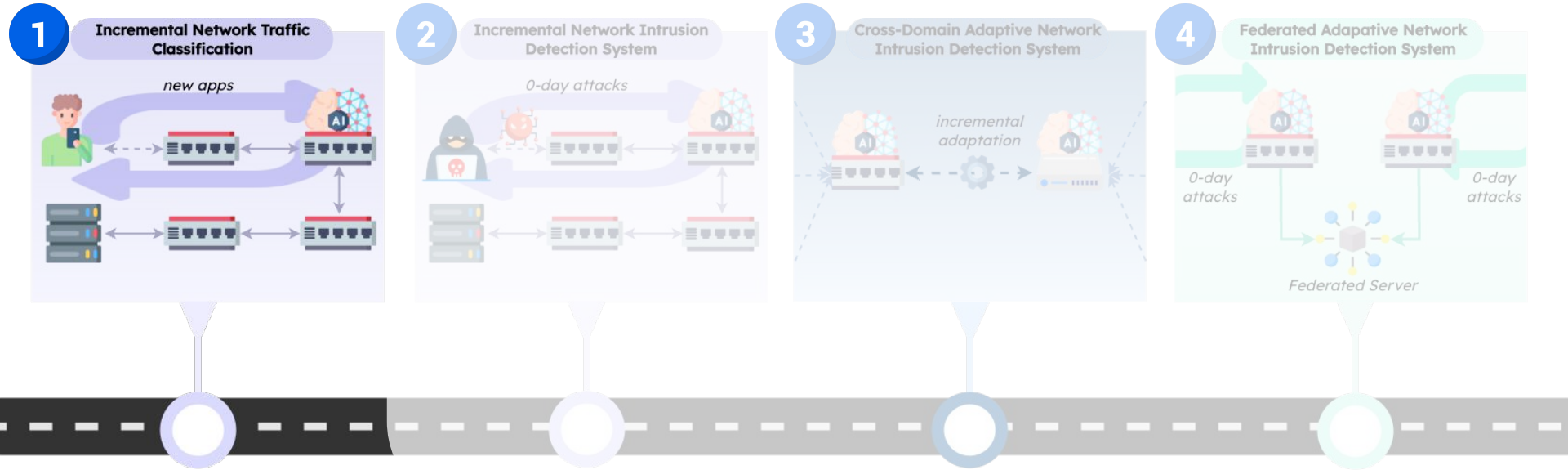
- **Rehearsal** — storage of old classes samples
- **Regularization** — minimizes the update of backbone parameters
- **Bias Correction** — corrects the bias towards recently learned classes

To quantify classification performance, this thesis leverage **F1 score**— i.e., harmonic mean of precision and recall

- **F1 Drop:** difference between *training-from-scratch* and *CIL*
  - **F1 DropNew:** how is the updated model reluctant to learn new classes?
  - **F1 DropOld:** how much is the forgetting with respect to the ideal performance?
  - **F1 DropAll:** how much far is the updated model from the upper bound?

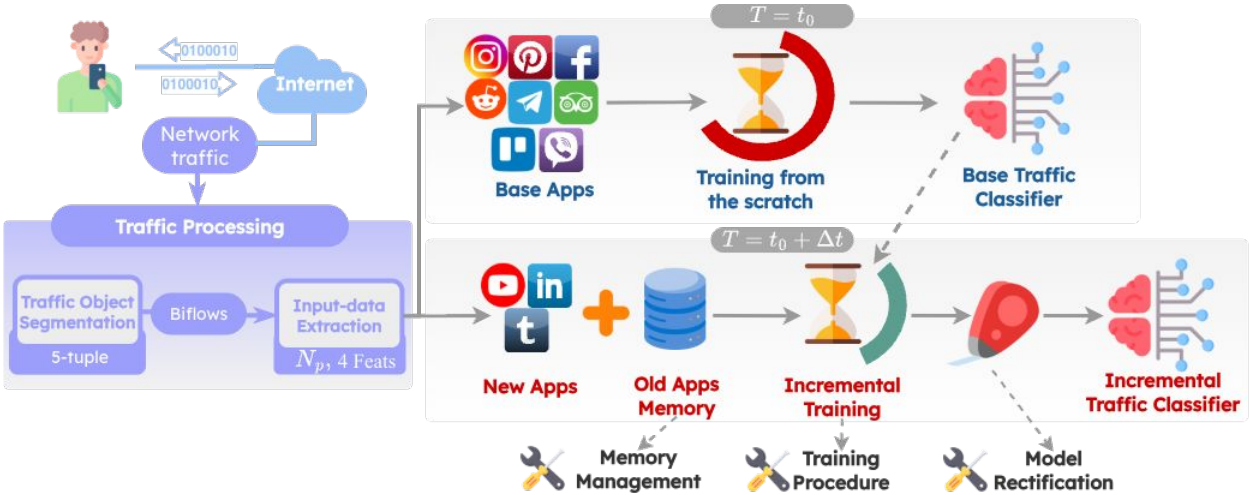


PhD thesis: overview



1 Incremental Network Traffic Classification: Concept

To deal with the **ever-changing nature of mobile network traffic**, this thesis introduce **Memento** — a novel **Class Incremental Learning (CIL)** approach for enhanced **incremental network traffic classification**



This thesis explores three **key aspects of incremental learning**, that converge in Memento:

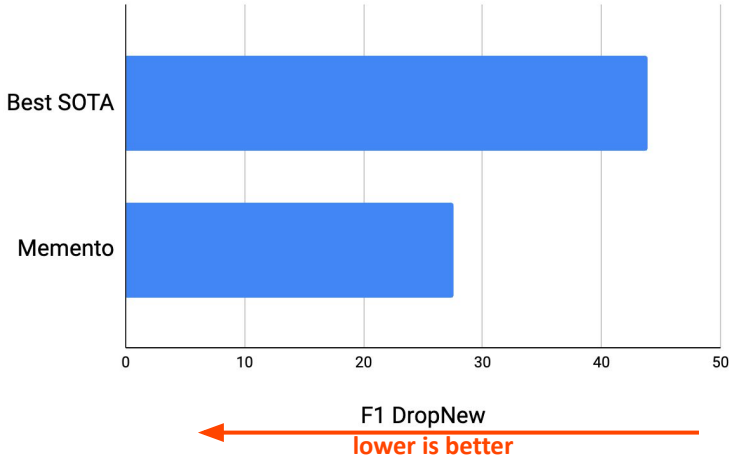
- **Memory management** — different ways to select only few old app samples and augment them
- **Training procedure** — refining incremental learning procedures
- **Model rectification** — mitigating bias in the model prediction toward new apps

1 Incremental Network Traffic Classification: Results (1/3)

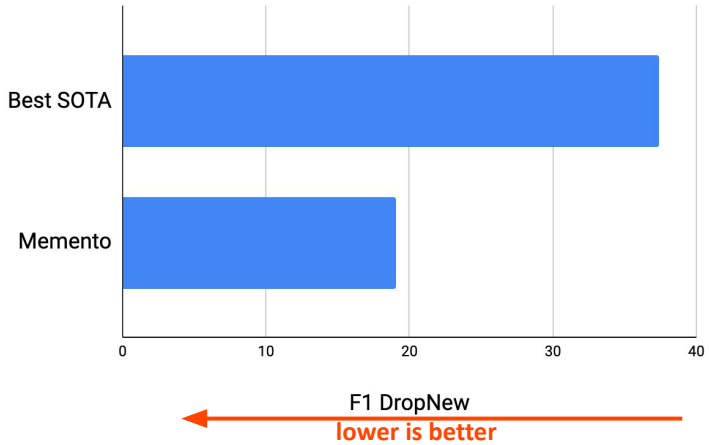
Memento shows a **consistent improvement in single-app addition scenarios**:

- Maintains **stable performance** on **previously learned apps**
- **Improves** performance on **newly added apps**

- Achieves up to a **16% improvement** in **new app classification** when expanding the classifier from **39 to 40 apps**[1]…



…and up to a **18% improvement** when expanding the classifier from **79 to 80 recognized apps**[2]



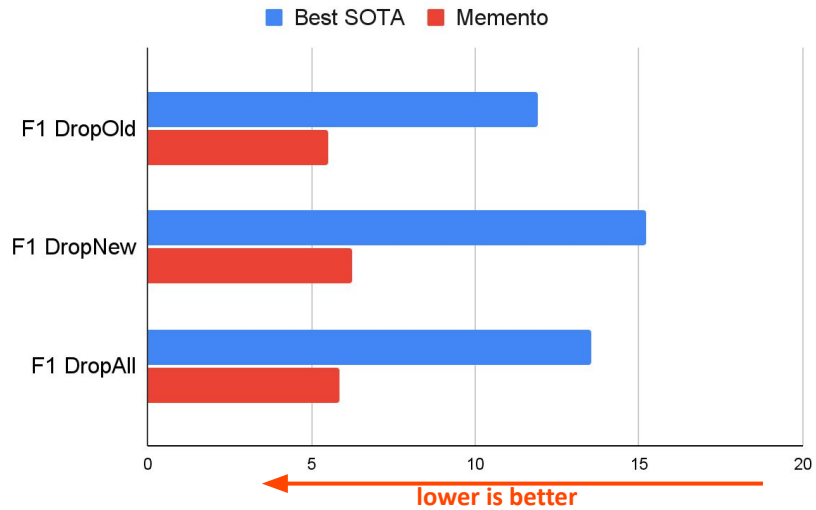
[1] results obtained on MIRAGE-19 dataset (https://traffic.comics.unina.it/mirage/mirage-2019.html)
[2] results obtained on CESNET-TLS22 dataset (https://zenodo.org/records/10610895)

1 Incremental Network Traffic Classification: Results (2/3)

Similarly, **Memento** outperform best SOTA approach in **many-app addition** scenarios, by obtaining…

…up to a **3% improvement** in **all the set of apps** when expanding the classifier from 20 to 40 apps[1]

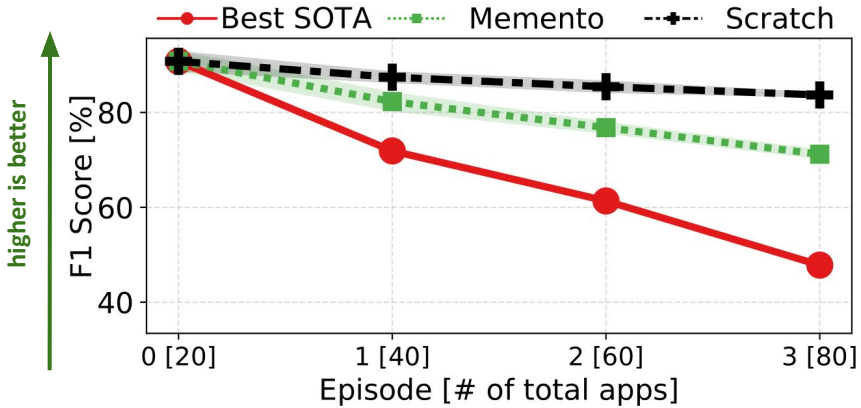
…and **>6% improvement** when expanding the classifier from 40 to 80 recognized apps[2]



[1] results obtained on MIRAGE-19 dataset (https://traffic.comics.unina.it/mirage/mirage-2019.html)
[2] results obtained on CESNET-TLS22 dataset (https://zenodo.org/records/10610895)

1 Incremental Network Traffic Classification: Results (3/3)

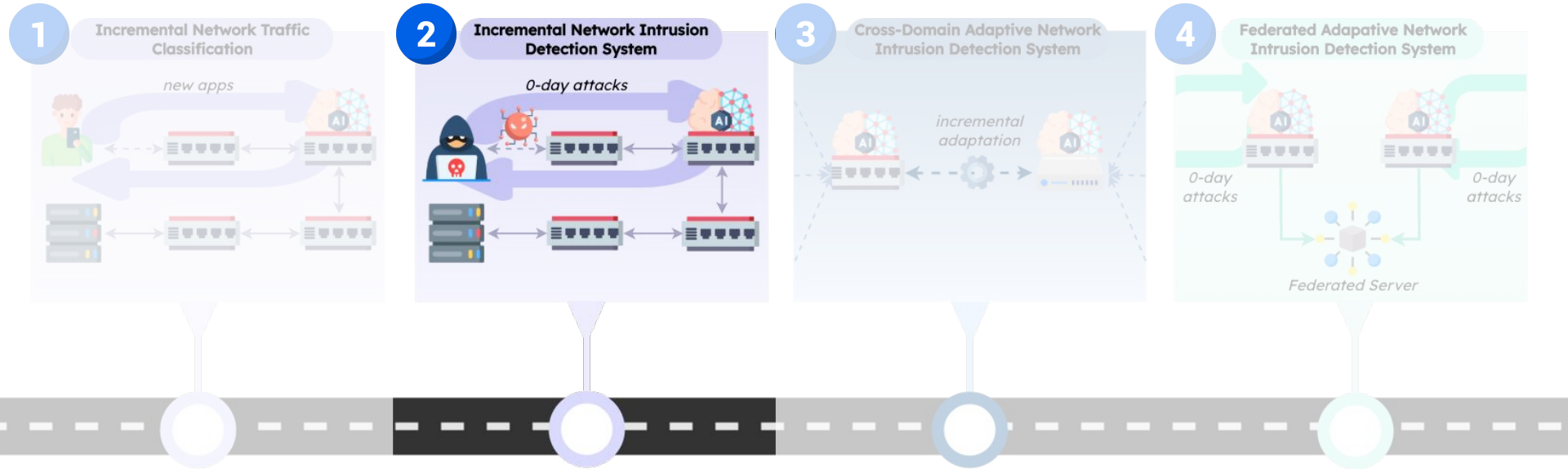
Then, **Memento** achieves the **best results in a multi-increment scenario**, where the classifier is expanded from **20 apps to 80 apps** over three incremental steps, obtaining **+26% overall** compared to best SOTA approach[1]



Lastly, **Memento save up to 90% of training time** of the ideal *training-from-scratch* approach in **single-app increments**, while up to **17% in many-app addition**

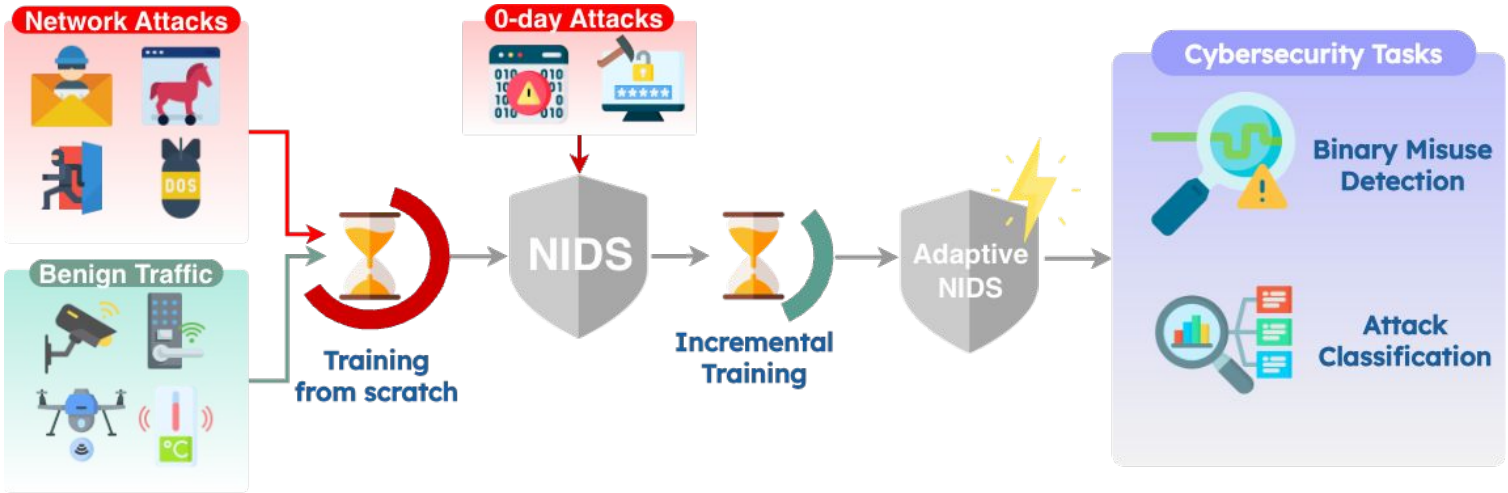
[1] results obtained on CESNET−TLS22 dataset (https://zenodo.org/records/10610895)

PhD thesis: overview



2 Adaptive Network Intrusion Detection System: Concept

To tackle the challenges posed by **evolving threats**, this thesis further employ **Memento** to enable **adaptive Network Intrusion Detection Systems (NIDS)**



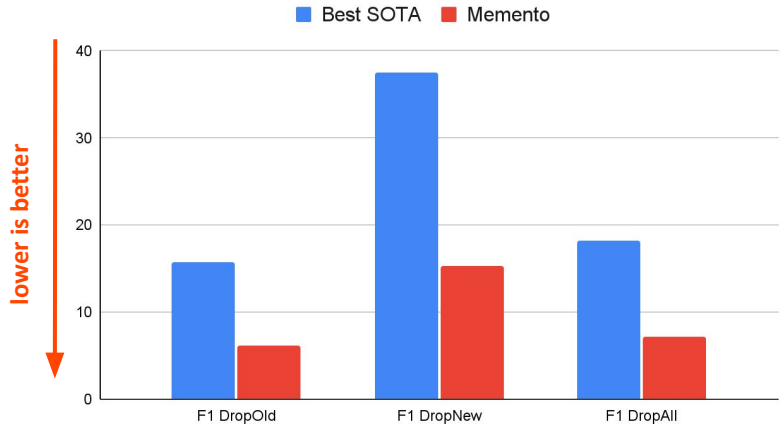
This thesis explores **three key hyperparameters** of adaptive NIDS:

- **Feature set optimization** — extract from traffic the most informative features to maximize performance
- **Earliness of classification** — ensuring attacks are detected as early as possible to enable timely countermeasures
- **Robustness to old threats** — optimizing retained information to preserve knowledge of previously seen attacks

2 Adaptive Network Intrusion Detection System: Results

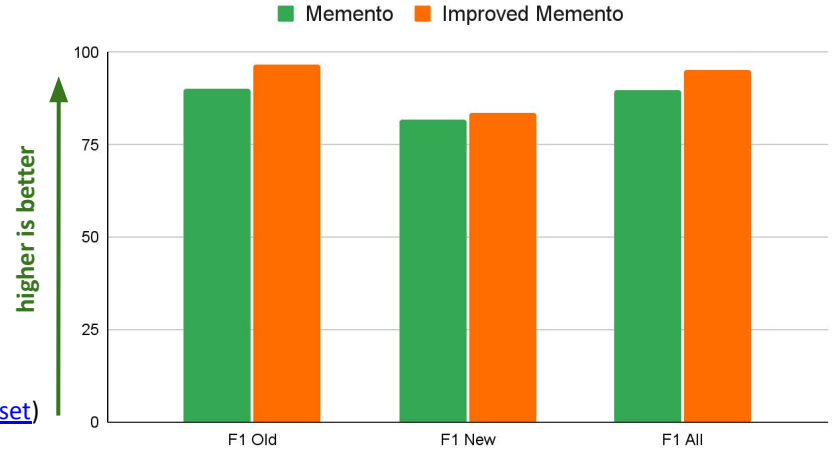
Memento consistently **improves incremental attack classification:**

- **+10% F1** on previously seen attacks
- **+12% F1** on newly observed attacks
- **Up to 95% reduction** in training time compared to the *ideal training-from-scratch*



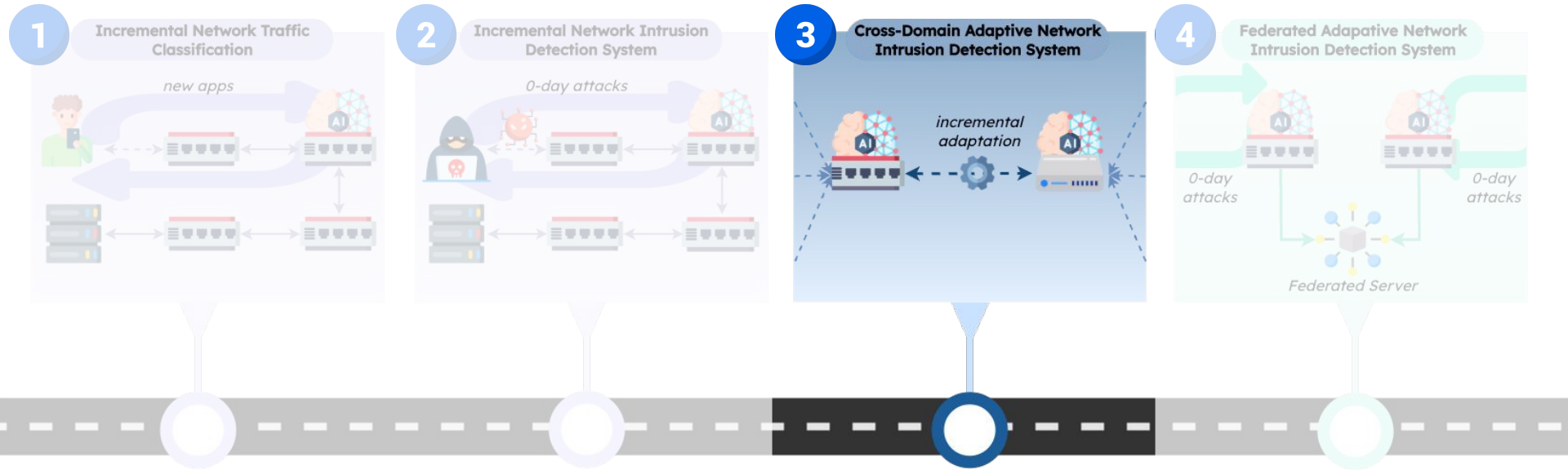
Additional results of `Memento` includes:

- Tuning `Memento`'s adaptive NIDS hyperparameters yields up to **+7% improvement in attack classification**
- In binary misuse detection, `Memento` achieves **>84% PAUC** in distinguishing malicious vs. benign traffic



*shown results are obtained on `IoT-NID` dataset (https://ieee-dataport.org/open-access/iot-network-intrusion-dataset)

PhD thesis: overview

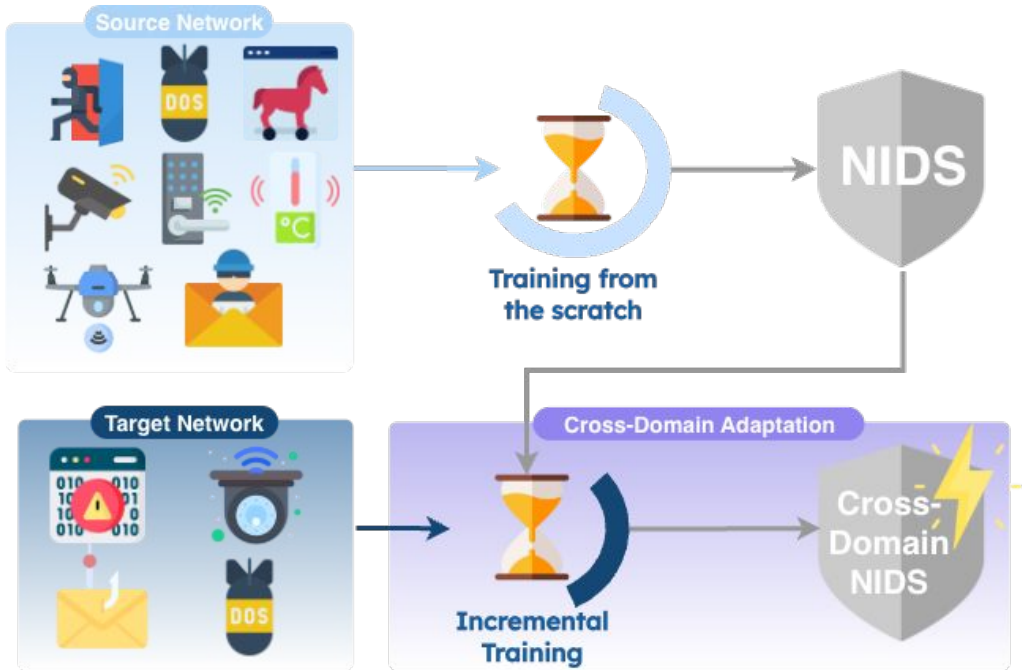


3 Cross-Domain Adaptive Network Intrusion Detection System: Concept

To address the **adaptability of models across different networks**, this thesis investigates **cross-domain and adaptive NIDS**, focusing on how NIDS can remain effective under **heterogeneous environments** and **evolving attack scenarios**

This approach combines **Domain Incremental Learning (DIL)** and **Class Incremental Learning (CIL)** to enable a NIDS to update its knowledge of known attacks while learning new ones.

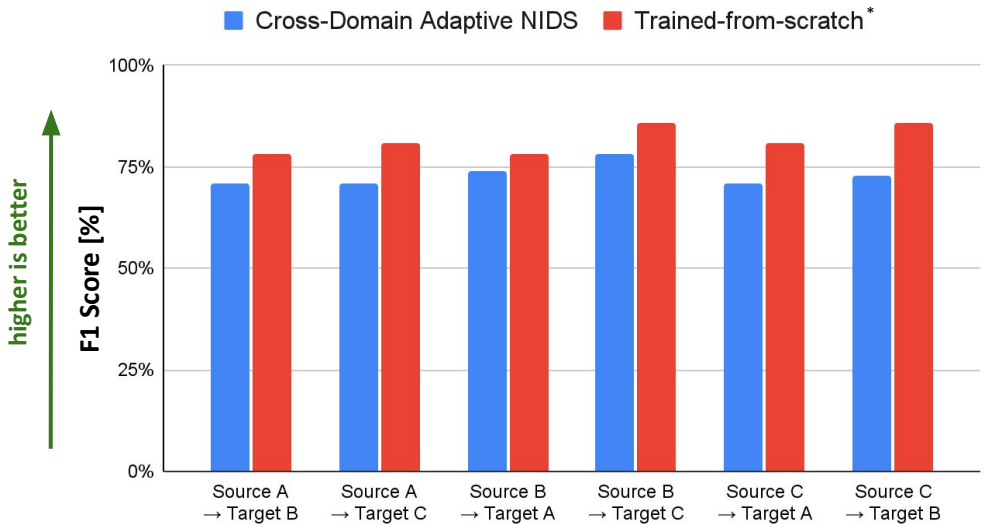
This allows a NIDS trained on one network **to adapt across domains**, detecting **attacks and legitimate traffic in multiple environments**



3 Cross-Domain Adaptive Network Intrusion Detection System: Results

To enable **cross-adaptation NIDS**:

- **Attack labels are standardized** so that similar attacks share the same name across networks
- **Biased and irrelevant traffic samples are removed** to improve generalization across domains

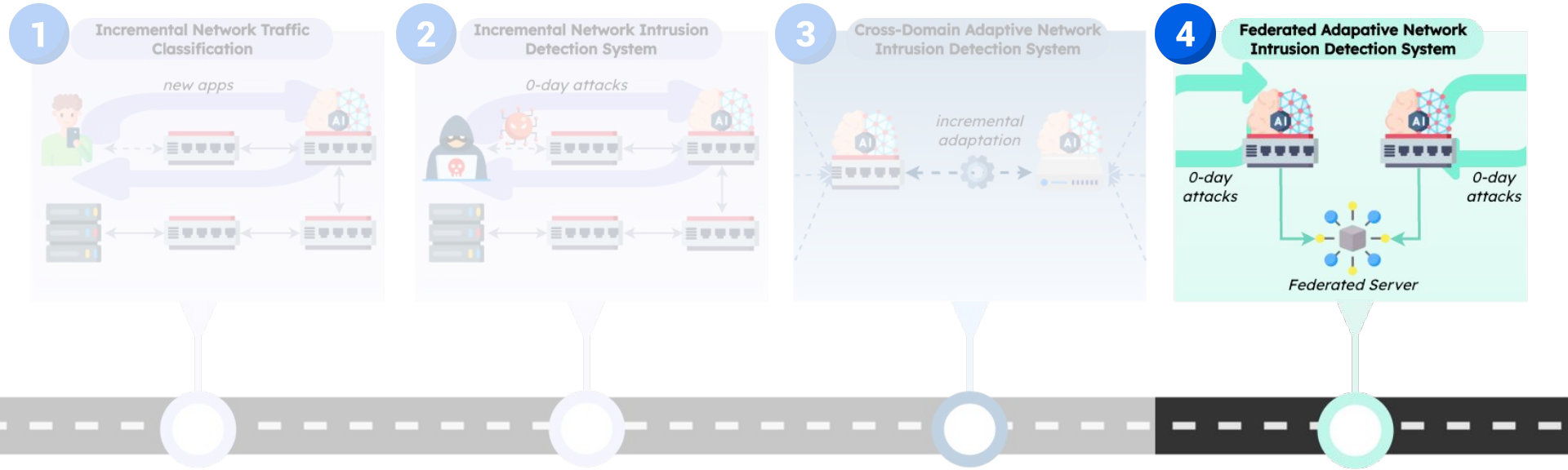


Our findings assess that:

- A **NIDS trained on source traffic performs poorly on target traffic**, achieving only **30% F1 Score** even for benign vs. malicious classification
- Cross-domain adaptive NIDS **performance differs of 4–13% from trained-from-scratch model**
- Cross-domain adaptive NIDS achieves **up to 50% reduction in training time**

*trained-from-scratch on both source and target dataset

PhD thesis: overview

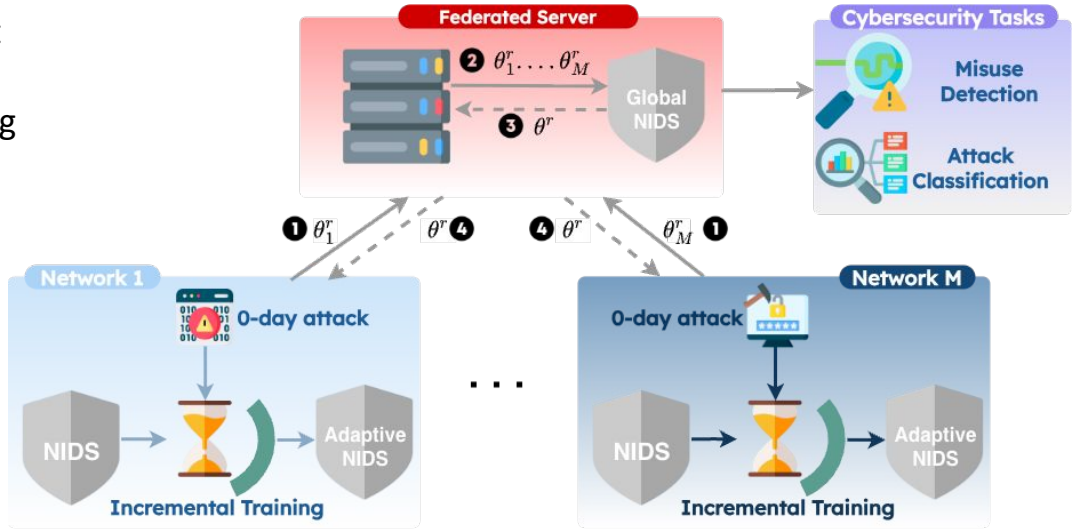


4 Federated Adaptive Network Intrusion Detection System: Concept

To tackle the challenges of **distributed data and continuous updates**, we devise a **Federated Class Incremental Learning (FCIL) framework** for adaptive and scalable NIDS, extending CIL approaches to work in a **federated setup**, ultimately resulting in **Memento+**

This thesis investigates several strategies, that converge into MEMENTO+:

- **Tailored bias correction strategy**— designing a client-specific strategy to correct model bias
- **FL aggregation algorithms** — evaluating different aggregation methods for FCIL
- **Federated incremental scenarios** — exploring various number of clients in the federated network
- **Federated client communications** — exploring various synchronization rounds number in the FCIL process



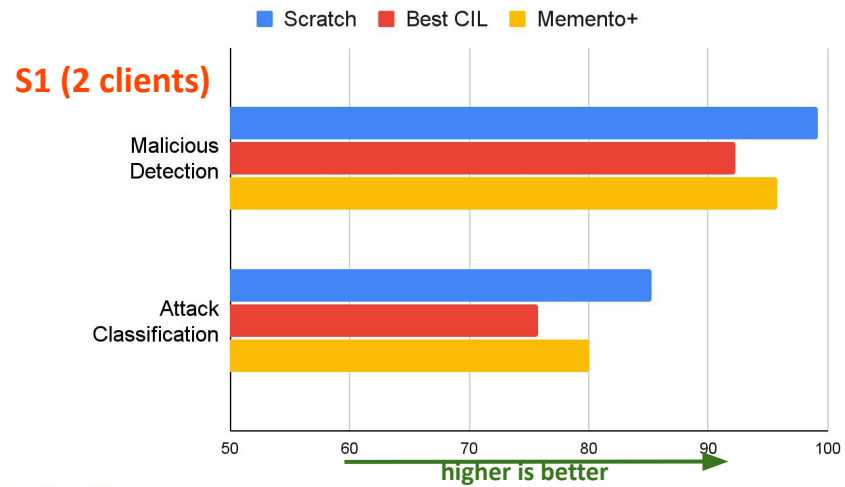
4 Federated Adaptive Network Intrusion Detection System: Results

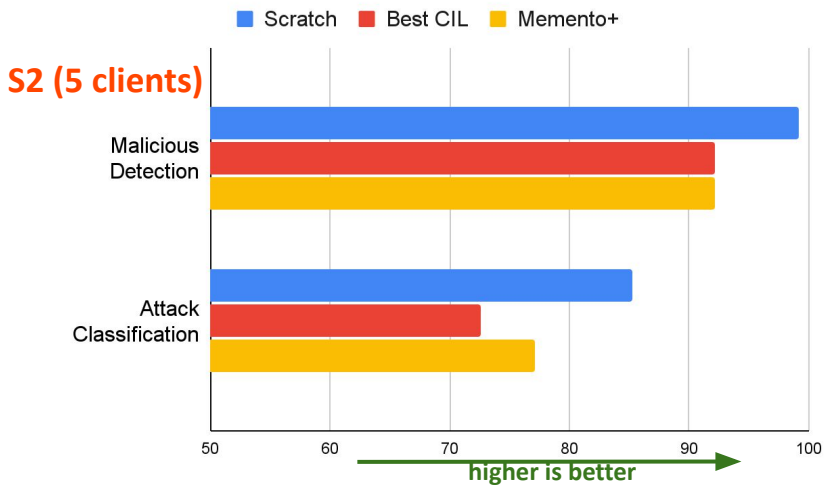
Memento+ in a federated and incremental setup **outperforms SOTA FCIL** for single attack addition:

- in **small network (S1, 2 clients)** obtains **≈79% F1** with 10 sync rounds.
- in **larger network (S2, 5 clients)** reaches **≈75% F1** with 100 sync rounds

This thesis quantify the **cost of decentralized incremental training** compared to centralized (and incremental) approaches:

- MEMENTO+ outperforms the best CIL in both federated scenarios
- Performance distant from training-from-scratch **5% in few-clients scenario** and **7% in many-clients one**





*shown results are obtained on TON_IoT dataset (https://research.unsw.edu.au/projects/toniot-datasets)

Conclusions

This thesis investigates **Class Incremental Learning (CIL)** for network traffic analysis and intrusion detection, proposing **MEMENTO**, ensuring adaptability and scalability in modern networks. Key contributions include:

- **Incremental Network Traffic Classification:**
  - Memento achieves up to +16% F1 Score improvement on new classes and +3% gain in knowledge retention, saving up to 94% training time
- **Adaptive Network Intrusion Detection System:**
  - Memento detects zero-day attacks with up to 95% F1 Score and 96% PAUC, while preserving recognition of known threats
- **Cross-domain Adaptability Network Intrusion Detection System:**
  - Combining CIL and DIL achieves meaningful adaptation across heterogeneous environments, with up to 78% in classifying both network traffic
- **Federated Adaptive Network Intrusion Detection System:**
  - Memento+ achieves up to 99% detection of malicious traffic and 83% F1 Score in classifying new threats under decentralized and privacy-preserving conditions

Summary of study activities

8 Courses:

- On the challenges and impact of Artificial Intelligence in the Insurance domain (PhD Course)
- IoT Data Analysis (PhD Course)
- Data Analytics (MSc Course)
- Statistical data analysis for science and engineering research (PhD Course)
- Using Deep Learning properly (PhD Course)
- Ethics&AI (PhD Course)
- Hands-on Network Intrusion Detection via Machine and Deep Learning (PhD Course)
- Strategic Orientation for STEM Research & Writing (PhD Course)

2 PhD Schools:

- 2023 PhD school of Network Traffic Measurement Analysis Conference (TMA), Napoli, Italy
- 2024 PhD school of Network Traffic Measurement Analysis Conference (TMA), Dresden, Germany

25 Seminars

9 Conferences Attended as a Speaker:

- IEEE Global Communications Conference (GLOBECOM)
- Network Traffic Measurement and Analysis (TMA) (2023, 2024)
- IFIP/IEEE Networking
- IEEE Symposium on Computers and Communications (ISCC)
- IEEE International Conference on Big Data (BigData)
- Italian Conference on CyberSecurity (ITASEC) (2023, 2024)
- Italian Networking Conference (INW)

Tutorship Activities

- Bachelor's and Master's Degree courses in Computer Engineering

Research products

International Journal Publications:

J1. **F. Cerasuolo**, A. Nascita, G. Bovenzi, G. Aceto, D. Ciuonzo, A. Pescapè, D. Rossi, MEMENTO: A Novel Approach for Class Incremental Learning of Encrypted Traffic, **Elsevier Computer Networks**, 245, p.110374

J2. G. Bovenzi, **F. Cerasuolo**, D. Ciuonzo, D. Di Monda, I. Guarino, A. Montieri, V. Persico, A. Pescapé, Mapping the landscape of generative AI in network monitoring and management, **IEEE Transactions on Network and Service Management**, 22, p. 2441

J3. **F. Cerasuolo**, G. Bovenzi, D. Ciuonzo, A. Pescapè, Adaptable, Incremental, and Explainable Network Intrusion Detection Systems for Internet of Things, **Elsevier Engineering Applications of Artificial Intelligence**, 144, p.110143

J4. **F. Cerasuolo**, G. Bovenzi, D. Ciuonzo, A. Pescapè, Attack-Adaptive Network Intrusion Detection Systems for IoT Networks through Class Incremental Learning, **Elsevier Computer Networks**, 263, p. 111228

J5. R. Carillo, **F. Cerasuolo**, G. Bovenzi, D. Ciuonzo, A. Pescapè, Explainable federated class incremental learning for Encrypted Network Traffic classification, **Elsevier Computer Networks**, 269, p. 111448

J6. R. Carillo, **F. Cerasuolo**, G. Bovenzi, D. Ciuonzo, A. Pescapè, A Federated and Incremental Network Intrusion Detection System for IoT Emerging Threats, **IEEE Transaction on Network Service Management**—*under review*

Research products

International Conference Publications:

C1. V. Spadari, **F. Cerasuolo**, G. Bovenzi, A. Pescapè, An MLOps Framework for Explainable Network Intrusion Detection with MLflow, **2024 IEEE Symposium on Computers and Communications (ISCC)**

C2. **F. Cerasuolo**, G. Bovenzi, V. Spadari, D. Ciuonzo, A. Pescapè, Explainable Few-Shot Class Incremental Learning for Mobile Network Traffic Classification, **2024 IEEE Global Communications Conference**

C3. **F. Cerasuolo**, I. Guarino, V. Spadari, G. Aceto, A. Pescapè, XAI for interpretable multimodal architectures with contextual input in mobile network traffic classification, **2024 IFIP Networking Conference**

C4. **F. Cerasuolo**, G. Bovenzi, A. Montieri, A. Pescapè, Class Incremental Learning for Network-Agnostic Intrusion Detection Systems, **2025 IEEE Research and Technologies for Society and Industry (RTSI)**

C5. R. Carillo, **F. Cerasuolo**, A. Pescapè, E. Kanaki, P. Chatzimisios, Federated Incremental Learning for Encrypted Network Traffic Classification, **2025 IEEE International Conference on Blockchain Computing and Applications (BCCA)**

International Workshop Publications:

W1. A. Nascita, **F. Cerasuolo**, G. Aceto, D. Ciuonzo, V. Persico, A. Pescapè, Explainable Mobile Traffic Classification: the case of Incremental Learning, **Workshop on 'Explainable and Safety Bounded, Fidelitous, Machine Learning for Networking (CoNEXT 2023)**

W2. **F. Cerasuolo**, G. Bovenzi, C. Marescalco, F. Cirillo, D. Ciuonzo, A. Pescapè, Adaptive intrusion detection systems: Class incremental learning for IoT emerging threats, **2023 IEEE International Conference on Big Data**

Thank You

Backup Slides

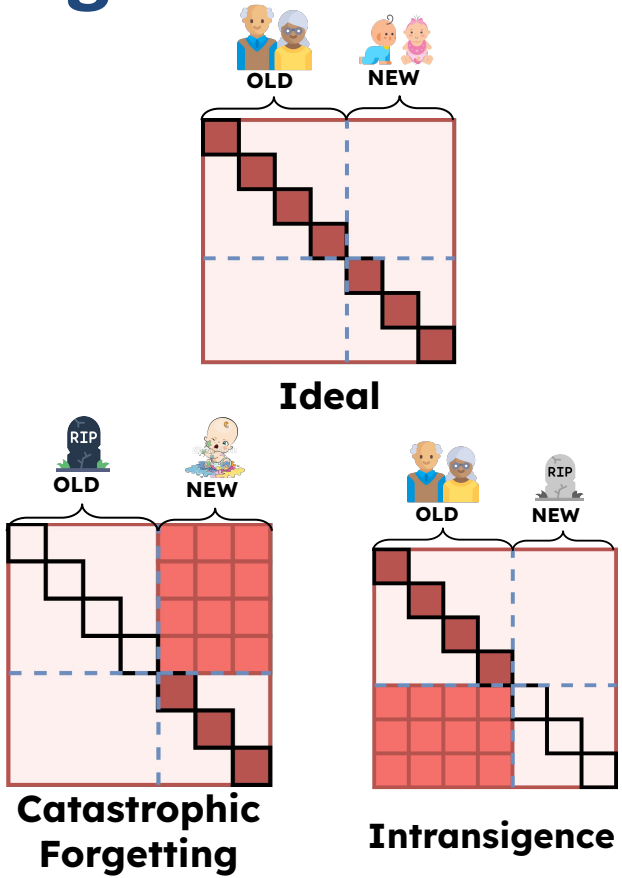
Incremental Learning: issues

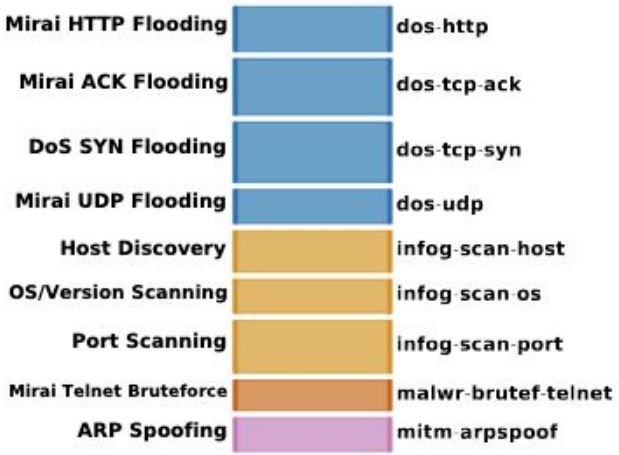
Ideal Performance
- perfect matching between predicted and actual classes

Catastrophic Forgetting
- model tends to forget knowledge related to old classes

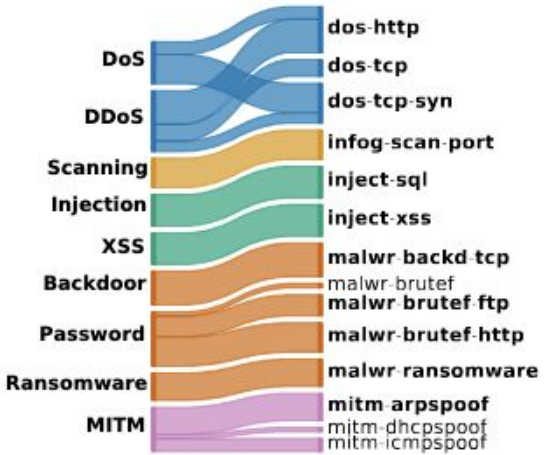
Intransigence
- inability to learn new classes

To reduce forgetting, **different strategies** are enforced:
- **Rehearsal** — storage of old classes samples
- **Regularization** — minimizes the update of model backbone parameters
- **Bias Correction** — corrects the bias introduced by recently learned classes

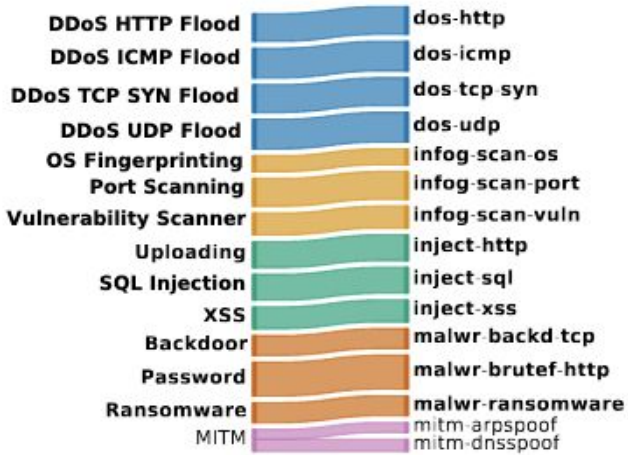




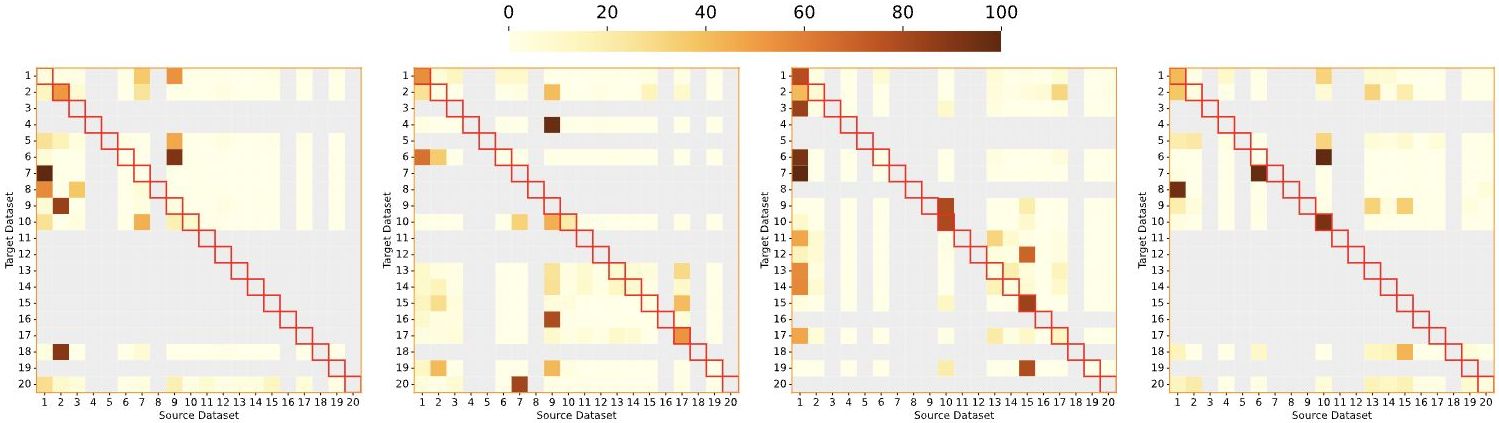
(a) IoT-NID



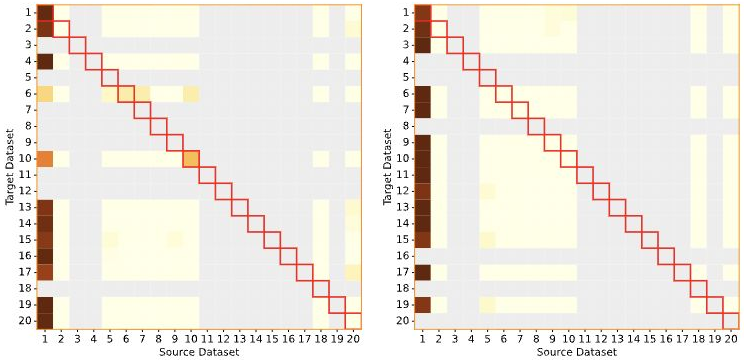
(b) TON_IoT



(c) Edge-IIoT



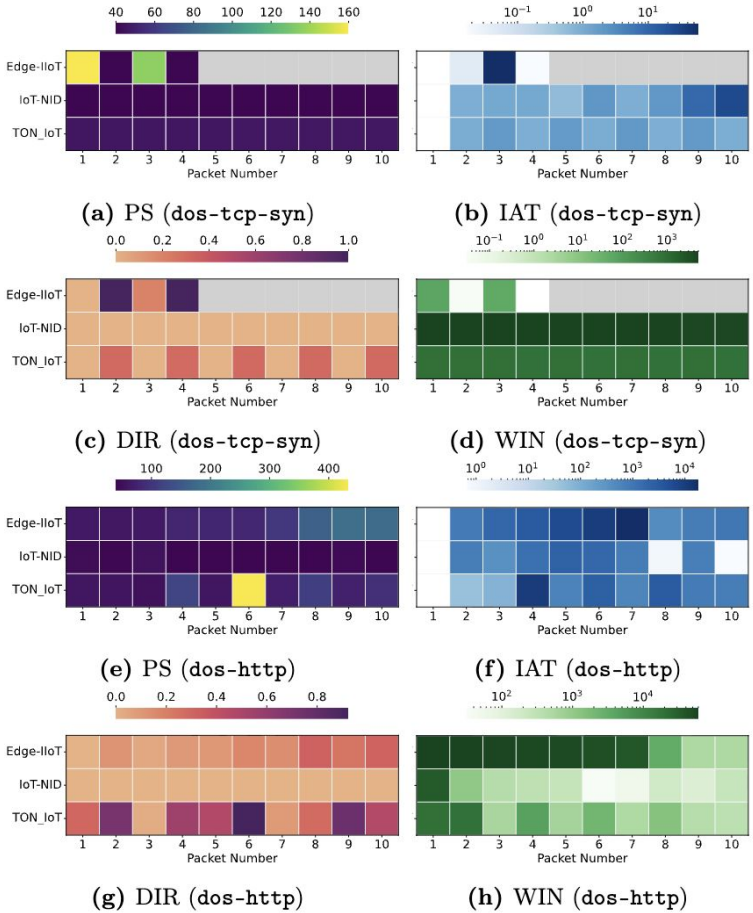
(a) ⟨Edge-IIoT,IoT-NID ⟩ **(b)** ⟨Edge-IIoT,TON_IoT ⟩ **(c)** ⟨TON_IoT,Edge-IIoT ⟩ **(d)** ⟨TON_IoT,IoT-NID ⟩



(e) ⟨IoT-NID,TON_IoT ⟩ **(f)** ⟨IoT-NID,Edge-IIoT ⟩

N°	Classes	N°	Classes
1	benign	11	infog-scan-vuln
2	dos-http	12	inject-http
3	dos-icmp	13	inject-sql
4	dos-tcp	14	inject-xss
5	dos-tcp-ack	15	malwr-backd-tcp
6	dos-tcp-syn	16	malwr-brutef-ftp
7	dos-udp	17	malwr-brutef-http
8	infog-scan-host	18	malwr-brutef-telnet
9	infog-scan-os	19	malwr-ransomware
10	infog-scan-port	20	mitm-arpspoof

(g) Classes Encoding


40 60 80 100 120 140 160
10^{-1} 10^{0} 10^{1}
Edge-IIoT
IoT-NID
TON_IoT
1 2 3 4 5 6 7 8 9 10
Packet Number
(a) PS (dos-tcp-syn)
(b) IAT (dos-tcp-syn)
0.0 0.2 0.4 0.6 0.8 1.0
10^{-1} 10^{0} 10^{1} 10^{2} 10^{3}
(c) DIR (dos-tcp-syn)
(d) WIN (dos-tcp-syn)
100 200 300 400
10^{0} 10^{1} 10^{2} 10^{3} 10^{4}
(e) PS (dos-http)
(f) IAT (dos-http)
0.0 0.2 0.4 0.6 0.8
10^{2} 10^{3} 10^{4}
(g) DIR (dos-http)
(h) WIN (dos-http)