Sofiane Ennadir

✉ ennadir@kth.se ☎ +46700183367 Scholar 🔗 sennadir.github.io

Summary

I am a researcher at Microsoft Gaming (King AI Labs-ABK). My research focuses on the foundations and applications of large-scale models in real-world use cases, with an emphasis on theoretically understanding the internal mechanisms of Transformer-based architectures and Large Language Models (LLMs). In parallel, in line with the research conducted during my PhD, I also investigate the robustness and safety of deep learning systems, aiming to establish theoretical insights that support Responsible AI practices. Across both directions, my goal is to bridge fundamental theory with practical defenses and architectural adaptations to build reliable and trustworthy AI.

Experience

AI/ML Researcher *Stockholm, Sweden*
Microsoft Gaming (ABK - King AI Labs) *August 2024 – Present*

- Internship (From August 2024 to February 2025), then full-time researcher.
- Working on understanding and applying Transformer-Based models and on Self-supervised representation learning on Continuous-Time Dynamic Graphs (CTDG).

Research Intern *New York, USA*
Flatiron Institute - Simons Foundation *May 2024 – Aug 2024*

- Affiliated to the Polymathic AI initiative, I worked on extending the usage of the Joint-Embedding Predictive Architectures (JEPA) for time series pre-training.

Research Intern *Paris, France*
BNP Paribas *June 2020 – Dec 2020*

- Worked within the RISK Artificial Intelligence Research center (Risk AIR) on the Interpretability of ML/DL Models, mainly using counterfactual explanations in a black-box model approach.

Research Scholar *Louisville, KY*
University of Louisville *June 2019 – Sep 2018*

- Worked with Professor Hichem Frigui on a ML-based approach to detect Lung Cancer from CT Images. The output was a Computer Aided Diagnosis System with a 94% (±0.6) accuracy on the Luna Challenge.

Education

KTH Royal Institute Of Technology *2021 – 2025*
PhD candidate in Deep Learning for graphs

- Thesis: On the Adversarial Robustness and Applications of Graph Neural Networks (GNNs).
- Supervisor: Professor Michalis Vazirgiannis and Professor Henrik Boström.
- Thesis accepted and defense expected in November 2025.

Ecole Polytechnique - IPP Paris *2019 – 2021*
MSc in Applied Mathematics - Data Sciences

- Thesis: Interpretability and Explicability of Machine Learning Models.
- Supervisors: Professor Eric Moulines and Professor Erwan Le Pennec.

EMINES School Of Industrial Management - UM6P *2014 – 2019*
Master Of Engineering

- A Co-Directed Program by Ecole Polytechnique and supervised by Professor Eric Moulines including 2 years preparatory classes and 3 years General, Industrial Management Engineering Courses.

Publications

[1] Pool Me Wisely: On the Effect of Pooling in Transformer-Based Models.
S. Ennadir*, L. Zólyomi*, O. Smirnov, T. Wang, J. Pertoft, F. Cornell, L. Cao.
Conference on Neural Information Processing Systems (NeurIPS), 2025

[2] Enhancing Graph Classification Robustness with Singular Pooling.
S. Ennadir*, O. Smirnov*, Y. Abbahaddou, L. Cao, J. Lutzeyer.
Conference on Neural Information Processing Systems (NeurIPS), 2025

[3] Expressivity of Representation Learning on CTDGs: An Information-Flow Centric Review.
S. Ennadir*, G. Zarzar*, F. Cornell*, L. Cao, O. Smirnov, T. Wang, L. Zólyomi, B. Brinne, S. Asadi.
Transactions on Machine Learning Research (TMLR), 2025

[4] If You Want to Be Robust, Be Wary of Initialization.
S. Ennadir, J. Lutzeyer, M. Vazirgiannis, E. Bergou.
Conference on Neural Information Processing Systems (NeurIPS), 2024

[5] Joint Embeddings Go Temporal.
S. Ennadir, S. Golkar, L. Sarra.
TSALM Workshop, Conference on Neural Information Processing Systems (NeurIPS), 2024

[6] Bounding the Expected Robustness of Graph Neural Networks Subject to Node Feature Attacks.
Y. Abbahaddou*, **S. Ennadir***, J. Lutzeryer, M. Vazirgiannis, H. Boström.
International Conference on Learning Representations (ICLR), 2024

[7] A Simple and Yet Fairly Effective Defense for Graph Neural Networks.
S. Ennadir, Y. Abbahaddou, J. Lutzeryer, M. Vazirgiannis, H. Boström.
AAAI Conference on Artificial Intelligence (AAAI), 2024

[8] UnboundAttack : Generating Unbounded Adversarial Attacks to Graph Neural Networks.
S. Ennadir, A. Alkhatib, G. Nikolentzos, M. Vazirgiannis, H. Boström.
International Conference on Complex Networks and their Applications (CNA), 2023

—
(* denotes equal contribution.)

Academic Service and Outreach

Talks

- On the Effect of Initialization on Advesarial Robustness - LOG Conference Meetup - Sweden.
- From Bounds to Defenses: A Comprehensive Look at GNN Robustness - Metis Spring School.
- Theoretically Upper-Bounding the Expected Adversarial Robustness of GNNs - Collective ML.
- Adversarial Robustness of GNNs - MoroccoAI.

Awards

- WASP Doctoral Scholarship funded by the Knut and Alice Wallenberg Foundation 2021
- OCP Full Excellence merit scholarship for outstanding results in entrance examination. 2014

Teaching

- Introduction to LLMs & Deep Learning on Graphs - Ecole Polytechnique.
- Deep Learning for time series, NLP and Graphs - Ecole Polytechnique Executive Education.

Academic Reviewing

- Neurips (2025, 2024), ICLR (2026, 2025), KDD (2025), Learning On Graphs (2024), TMLR.