

Sofiane ENNADIR

 [sennadir.github.io](https://github.com/sennadir) |  ennadir@kth.se |  +46.7.00.18.33.67

EDUCATION

KTH Royal Institute of Technology

Mar 2021 - Present

Ph.D candidate in Deep Learning for graphs

- Working under the supervision of Prof. Michalis Vazirgiannis (KTH/Ecole Polytechnique) where I investigate the adversarial robustness of Graph Neural Networks (GNNs) and their applications.

Ecole Polytechnique - IPP Paris

Sep 2019 - Dec 2020

MSc in Data Science - M2 Data Science

- Under the supervision of Prof. Eric MOULINES and Prof. Erwan LE PENNEC.
- **Course work:** Deep Learning, Advanced learning for text and Graph, Optimization for Data Sciences, Statistical Learning Theory.

EMINES School Of Industrial Management - UM6P

Sep 2014 - Aug 2019

Master of Engineering

- A Co-Directed Program by Ecole Polytechnique (L'X) and supervised by Prof. Eric MOULINES including 2 years preparation to EMINES-UM6P's Engineering cycle and a 3 years General, Industrial Management Engineering Courses.

PROFESSIONAL EXPERIENCE

- **Mar. 2021 – Present** PhD/Researcher at **KTH Royal Institute of Technology** Stockholm

- **June – Dec. 2020** Research Intern at **BNP Paribas** Paris

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

- **April – Sep. 2019** Visiting Associate at **Boston Consulting Group - BCG** Casablanca

- Applied Data Science based methodologies to resolve diverse client challenges, leveraging statistical and Machine Learning techniques for actionable insights and impactful solutions.

- **June – Sep. 2018** Research Scholar at **University of Louisville** Louisville, KY

- Worked with Prof. Hichem Frigui on developing a ML-based approach to detect Lung Cancer.

PUBLICATIONS

[Graph Convolutional Networks With Orthogonal Weights Are More Robust.](#)
ABBAHADDOU Y.¹, ENNADIR S.¹ & Al. - Under Review at ICLR 2024.

[A Simple and Yet Fairly Effective Defense for Graph Neural Networks.](#)
ENNADIR S. & Al. - Accepted at AAAI 2024.

¹Denotes Equal Contribution

- [Initial version](#) presented at *AdvML Workshop, ICML 2023*.

[UnboundAttack : Generating Unbounded Adversarial Attacks to Graph Neural Networks](#)

ENNADIR S. & Al. - Oral at the 12th International Conference on Complex Networks and their Applications 2023.

[Conformalized Adversarial Attack Detection for Graph Neural Networks.](#)

ENNADIR S. & Al. - Oral at the 12th Symposium on Conformal and Probabilistic Prediction with Applications.

[Generating Graph Perturbations to Enhance the Generalization of GNNs.](#)

ENNADIR S. & Al. - Under Review

[Structure-Aware Antibiotic Resistance Classification Using Graph Neural Networks.](#)

Qabel A., ENNADIR S. & Al. - AI4Science Workshop, Neurips 2022.

- [Extended version](#) is currently under review.

[Interpretable Graph Neural Networks for Tabular Data.](#)

Alkhatib A., ENNADIR S. & Al. - To be submitted.

SKILLS

Languages | *Fluent:* English (Toef Score 102). *Native:* Arabic, French
Programming | *Proficient:* Python. - *Prior experience:* MATLAB, C++, SQL, HTML.
Software Tools | PyTorch, PyTorch Geometric, Deep Graph Library, TensorFlow.

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

REFERENCES

Prof. Michalis Vazirgiannis KTH/ Ecole Polytechnique - [mvaz@kth.se]

Prof. Henrik Boström KTH - [bostromh@kth.se]

Prof. Eric Moulines Ecole Polytechnique - [eric.moulines@polytechnique.edu]

Prof. Hichem Frigui University of Louisville - [h.frigui@louisville.edu]