Soroush H. Zargarbashi

github.com/soroushzargar linkedin.com/in/soroushzargar zargarbashi@cs.uni-koeln.de
zargarbashi@cs.uni-koeln.de

Education

CISPA Helmholtz Center for Information Security - University of Cologne (Ongoing) 2022
Ph.D. in Artificial Intelligence (Trustworthy Machine Learning) ***Supervisor:*** *Prof. Dr. Aleksandar Bojchevski*

University of Tehran 2018 - 2021
M.Sc. in Computer Science

Isfahan University of Technology 2013 - 2018
B.Sc. in Computer Engineering (Software Major)

Expertise

Uncertainty Quantification • Conformal Prediction • Adversarial robustness • Graph neural networks

Relevant Taken Courses

Courses: Approximation Algorithm (19.5/20) • Data Science (19.25) • Advanced Algorithms(17.25/20) • Advanced Artificial Intelligence (18.48/20) • Machine Learning (17/20) • Graph Theory (16.78/20)

Publications

Conformal Prediction with Access to Epistemic Uncertainty | *Under prepration* 2025
- *Alireza Javanmardi**, Soroush H. Zargarbashi*, *Aleksandar Bojchevski, Willem Waegeman, Eyke Hüllermeier*

One Sample is Enough to make Conformal Prediction Robust | *Under prepration* 2025
- Soroush H. Zargarbashi, *Mohammad Sadegh Akhondzadeh, Aleksandar Bojchevski*

Eva: Evolutionary Attack on Graphs | *Under review* 2024
- Mohammad Sadegh Akhondzadeh*, Soroush H. Zargarbashi*, *Jimin Cao, Aleksandar Bojchevski*

Robust Conformal Prediction with a Single Binary Certificate | *Proceedings of the 13th ICLR* ICLR - 2024
- Soroush H. Zargarbashi, *Aleksandar Bojchevski*
- `TL;DR:` We show that for symmetric randomized smoothing methods (including almost all current certificates) with only one binary certificate we can attain robust conformal prediction. Therefore we significantly reduce the number of needed Monte-Carlo samples per input.

Robust yet Efficient Conformal Prediction Sets | *Proceedings of the 41st ICML* ICML - 2024
- Soroush H. Zargarbashi, *Mohammad Sadegh Akhondzadeh, Aleksandar Bojchevski*
- `TL;DR:` We leverage the distribution information of the model's output, to provide prediction sets that guarantee to include the true label with high probability even given the adversarial data.

Conformal Inductive Graph Neural Networks | *Proceedings of the 12th ICLR* ICLR - 2024
- Soroush H. Zargarbashi, *Aleksandar Bojchevski*
- `TL;DR:` We return prediction sets with a guarantee to cover the true label with adjustable probability. We propose an algorithm that works even when the graph is updated in a node- or edge-exchangeable sequence (inductive GNNs). Many uncertainty quantification methods do not work on GNN since i.i.d. assumption is violated.

Conformal Prediction Set for Graph Neural Networks | *Proceedings of the 40th ICML* ICML - 2023
- Soroush H. Zargarbashi, *Simone Antonelli, Aleksandar Bojchevski*
- `TL;DR:` We leverage the homophily structure in a graph to define efficient prediction sets with valid guarantees to include the true label. Our method works on top of any confidence approach.

A Multimodal Feature Embedding Approach to Diagnose Alzheimer's Disease | *ArXiv Preprint* 2019
- Soroush H. Zargarbashi, *Bagher Babaali*
- `TL;DR:` We use linguistic and acoustic feature extraction (commonly used in speaker identification methods) to diagnose Alzheimer's disease.

Experiences

Apple - R&D (Upcoming) May - Sep. 2025
Intern at machine intelligence team.

CISPA-Helmholtz Center for Information Security (Ongoing) Sep. 2022
Fully Funded Research Assistant

Arman Suba - Electricity Market Forecast 2020 - 2021
Backend Developer and Data Scientist

Speech Recognition Lab at University of Tehran 2018 - 2021
Research Assistant

Skills

Languages: Python, R, C++, C#
Libraries: Pytorch, Pytorch Geometric, Tensorflow, Librosa (speech processing)
Tools: Git/GitHub, Unix Shell, VS Code
Backend Development: Django Rest Framework, Docker, RabbitMQ

Academic Experiences

Reviewer | *NeurIPS, ICLR*

Attended Academic Events

- *HIDA PhD Meetup*: Event from Helmholtz Information & Data Science Academy on Machine Learning. Berlin 2024 - Presented poster: Certified conformal prediction sets
- *CISPA Trustworthy AI summer school*: 2022 on robustness, privacy and fairness of machine learning models. Saarbruecken- 2024
- *LoG Meetup* Learning on Graphs conference local meetup Munich 2023 - Presented poster: Conformal Prediction for GNNs

Master's Degree Thesis | *Fractional Fourier Transform in Deep Speech Enhancement*
`TL;DR:` We showed that the generalization short-term Fourier transform, to fractional transformation via eigen-decomposition can extract more meaningful features leading to a better speech enhancement.
Supervisors: Dr. Bagher Babaali, Prof. Tsao Yu

Teaching Assistant | *UzK: University of Cologne, IUT: Isfahan Uni. of Tech.*
Advanced Machine Learning (UzK) • Elements of Machine Learning (UzK) • Algorithm Design (IUT, 3 years) • Data Structures (IUT, 1 year)

Lab Instructor | *Tutor*
Advanced Programming (IUT, 2 years)

Honors and Awards

International IEEEXtreme Programming Contests
Ranked top 4% (11th contest among 3350 teams), top 6% (10th contest among 2000 teams), and top 7% (9th contest among 2477 teams)

References

Prof. Dr. Aleksandar Bojchevski | *Professor, University of Cologne*
Contact: a.bojchevski@uni-koeln.de

Dr. Bagher BabaAli | *Assistant Professor, University of Tehran*
Contact: babaali@ut.ac.ir

Dr. Ramin Javadi | *Assistant Professor, Isfahan University of Technology*
Contact: rjavadi@cc.ut.ac.ir