Denizhan Kara

denizhankara.github.io | kara4@illinois.edu | github.com/denizhankara | linkedin.com/in/denizhankara

Education

University of Illinois at Urbana-Champaign Champaign, IL
Ph.D. in Computer Science *2022 – Present*

University of Illinois at Urbana-Champaign Champaign, IL
Masters Degree in Computer Science *2020 – 2021*

Koç University Istanbul, Turkey
Bachelor of Science in Electrical and Electronics Engineering & Physics (Double Major) *2012 – 2017*

Research Experience

Physics-Informed AI for Distributed IoT Systems
Graduate Researcher - CyPhy Research Group at UIUC *2022-Present*

- Developing robust and resilient Foundation models for distributed IoT systems using physics and signal processing.
- Foundation models: Large-scale ML models, e.g., GPT-3, fine-tuned for specific tasks in distributed environments.
- Utilizing physical signal processing phenomenons for developing Neurosymbolic AI architectures in IoT.
- The Neurosymbolic architectures utilize the existing domain knowledge and laws of nature alongside traditional data-based optimization techniques in Machine Learning to build efficient, lightweight, and explainable systems.

Resiliency and Security in Vehicular (V2X) Networks
Graduate Researcher - Systems Security Research Group at UIUC (SyNeRCyS@Illinois) *2020 – Present*

- Designed an embedded misbehavior detection framework for vehicular networks to combat adversarial attacks, integrating temporal data anomalies, vehicular trust, and a unique ML architecture.
- Expanding research on ML-driven adversarial mechanisms to assess V2X network vulnerabilities.

Stealthy Attacks on UAV Swarms and Defenses
Graduate Researcher - Systems Security Research Group at UIUC (SyNeRCyS@Illinois) *2020 – Present*

- Developed stealthy sensor-spoofing tactics targeting UAV security vulnerabilities.
- Formulated ML-driven adversarial strategies to manipulate sensor readings, thereby bypassing control systems and compromising UAV stability without triggering alerts.

Work Experience

Machine Learning Engineer 2020 – 2022
Prometeia

- Implemented an AI-based propensity scoring framework utilizing customer transaction histories as a time series, allowing the prediction of customer interests towards products in a bank.
- Implemented Deep Credit Risk Default Model with novel features from the customer transactional data, improved the recall by 25%.
- Implemented the image augmentation pipeline and an ML-based segmentation model for the Automatic Car Damage Estimation system for Allianz Insurance, improved the F1-score by 6%.

Software Design Engineer 2017 – 2020
Turkish Aerospace - Autopilot Systems Division

- Developed and maintained signal processing libraries for autopilot control system software. Implemented custom filter blocks that reduced signal processing delay by up to 20% and suppressed various noise modes.
- Led the interpretation of electromagnetic & vibrational noise components within sensor data for the autopilot system and developed signal filtering solutions compliant with control algorithms.
- Developed the Sensor Emulator Framework, allowing the autopilot department to perform realistic SIL simulations.
- Implemented an in-house data processing tool that allowed faster analysis of test data by other engineers.

Publications

- **Kara, D.**, Kimura, T., Liu, S., Li, J., Liu, D., Wang, T., Wang, R., & Abdelzaher, T. (2023). FreqMAE: Frequency-Aware Masked Autoencoder for Multi-Modal IoT Sensing. (To Proceedings of the ACM Web Conference 2024)
- **Kara, D**, Kyo Hyun Kim, Sibin Mohan, Monowar Hasan, Takayuki Shimizu, and Hongsheng Lu. "OVERTON: A Misbehavior Detection and Trust Framework for Vehicular (V2X) Networks." (To USENIX Security Symposium 2024)
- Wang, T., Li, J., Wang, R., **Kara, D.**, Liu, S., Wertheimer, D., Martin, A., Ganti, R., Srivatsa, M., & Abdelzaher, T. (2023, November). SudokuSens: Enhancing Deep Learning Robustness for IoT Sensing Applications using a Generative Approach. In Proc. ACM Sensys 2023
- Wang, T., **Kara, D.**, Li, J., Liu, S., Abdelzaher, T., & Jalaian, B. (2022, November). The Methodological Pitfall of Dataset-Driven Research on Deep Learning: An IoT Example. In MILCOM 2022-2022 IEEE Military Communications Conference (MILCOM) IEEE.
- Kim, K. H., **Kara, D.**, Paruchuri, V., Mohan, S., Kimberly, G., Osipychev, D., ... & Pajic, M. (2022, November). Insights on Using Deep Learning to Spoof Inertial Measurement Units for Stealthy Attacks on UAVs. In MILCOM 2022-2022 IEEE Military Communications Conference (MILCOM) (pp. 1065-1069). IEEE.
- Kim, K. H., **Kara, D.**, Paruchuri, V., Mohan, S., Kimberly, G., & Kim, J. (2023). Requiem: Stealthy Attacks via Finding Adversarial Examples of Non-ML Functions in Unmanned Aerial Vehicles. (Preprint, Target: IEEE Symposium on Security and Privacy 2024)
- **Kara, D.**, Bugra Akyuz, and Secil Arslan. "TRANSPROP: AI-based Propensity Scoring Framework Utilizing Transactional Data Stream." (Preprint, Target: Proceedings of the AAAI Conference on Artificial Intelligence)

Achievements

- **TUBITAK National Scholarship Programme for M.S studies,** Granted for placing among the top 50 students nationwide in TUBITAK (NSF of Turkey) Weighted ALES (National GRE) and GPA Score List.
- **TUBITAK National Undergraduate Scholarship Program For Natural Sciences,** Granted for academic success on Double Major studies in physics.
- **Koç University Vehbi Koç High Honors Award,** Selected among Vehbi Koç Scholars for outstanding academic performance and SPA over 3.50.
- **Turkish Prime Ministry Special Success Scholarship,** Granted for ranking among the top-100 students in the National University Entrance Exam among 2 million students.
- **Koç University Full-Merit Scholarship,** Granted for ranking among the top-100 students in the National University Entrance Exam among 2 million students.

Technical Skills

Languages: Python, C++, MATLAB, Java, SQL, R
Technologies: PyTorch, Tensorflow, AWS, Simulink, ROS, Spark, Docker