Denizhan Kara

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

Education

University of Illinois at Urbana-Champaign Champaign, IL
Ph.D. in Computer Science - Siebel School of Computing and Data Science *Aug. 2022 – Present*

University of Illinois at Urbana-Champaign Champaign, IL
Master of Computer Science -Siebel School of Computing and Data Science *Aug. 2020 – Dec. 2021*

Koç University Istanbul, Turkey
B.Sc. in Electrical and Electronics Engineering & Physics (Double Major) *Sep. 2012 – Jun. 2017*

Research Experience

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

– Developing foundation model architectures integrating domain knowledge and physical laws with state-of-the-art self-supervised learning techniques used in training large language models.
– Aiming to build efficient, lightweight, and explainable AI systems for IoT applications deployable on edge devices.
– Collaborated with a multidisciplinary team, resulting in publications in top-tier conferences such as ACM SenSys, WWW, and NeurIPS.

Research Scientist Intern Jun. 2024 – Sep. 2024
US Army Research Laboratory (DEVCOM ARL) *Adelphi Laboratory Center, MD*

– Investigated robust moving vehicle classification techniques using deep learning and foundation models, enhancing detection accuracy by integrating physical signal processing.
– Optimized training processes for large-scale models and datasets by leveraging distributed computing resources, resulting in a 30% performance improvement.
– Developed physics-guided foundation model training techniques, incorporating generalizable decay models to enhance feature extraction and model robustness.

Graduate Researcher Aug. 2020 – Present
Resiliency and Security in Vehicular (V2X) Networks *Systems Security Research Group at UIUC*

– Designed an embedded misbehavior detection framework for vehicular networks to combat adversarial attacks, integrating temporal data anomalies, vehicular trust, and a novel ML architecture.
– Expanded research on ML-driven adversarial mechanisms to assess V2X network vulnerabilities, leading to improved network security protocols.

Graduate Researcher Aug. 2020 – Present
Stealthy Attacks on UAV Swarms and Defenses *Systems Security Research Group at UIUC*

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

Publications

Peer-Reviewed Publications

[1] **Kara, D.**, Kimura, T., Liu, S., Li, J., Liu, D., Wang, T., Wang, R., & Abdelzaher, T. (2024). *FreqMAE: Frequency-Aware Masked Autoencoder for Multi-Modal IoT Sensing.* Proceedings of the ACM Web Conference 2024 (WWW 2024).

[2] **Kara, D.**, Kimura, T., Chen, Y., Li, J., Wang, R., Chen, Y., Kaplan, L., Bhattacharyya, J., & Abdelzaher, T. (2024). *PhyMask: An Adaptive Masking Paradigm for Efficient Self-Supervised Learning in IoT.* In Proceedings of the 22nd ACM Conference on Embedded Networked Sensor Systems (SenSys 2024) (to appear).

[3] Wang, T., Yang, Q., Wang, R., Sun, D., Li, J., Chen, Y., Hu, Y., Yang, C., Kimura, T., **Kara, D.**, & Abdelzaher, T. (2024). *Fine-grained Control of Generative Data Augmentation in IoT Sensing.* Advances in Neural Information Processing Systems (NeurIPS 2024) (to appear).

[4] Kimura, T., Li, J., Wang, T., **Kara, D.**, Wigness, M., Bhattacharyya, J., Srivatsa, M. B., Liu, S., Diggavi, S., & Abdelzaher, T. (2024). *VibroFM: Towards Micro Foundation Models for Robust Multimodal IoT Sensing.* IEEE International Conference on Mobile Ad-Hoc and Smart Systems (MASS 2024) (to appear).

[5] Wang, T., Li, J., Wang, R., **Kara, D.**, Liu, S., Wertheimer, D., Martin, A., Ganti, R., Srivatsa, M., & Abdelzaher, T. (2023). *SudokuSens: Enhancing Deep Learning Robustness for IoT Sensing Applications using a Generative Approach.* Proceedings of the 21st ACM Conference on Embedded Networked Sensor Systems (SenSys 2023).

[6] Wang, T., **Kara, D.**, Li, J., Liu, S., Abdelzaher, T., & Jalaian, B. (2022). *The Methodological Pitfall of Dataset-Driven Research on Deep Learning: An IoT Example.* MILCOM 2022 IEEE Military Communications Conference.

[7] Kim, K. H., **Kara, D.**, Paruchuri, V., Mohan, S., Kimberly, G., Osipychev, D., & Pajic, M. (2022). *Insights on Using Deep Learning to Spoof Inertial Measurement Units for Stealthy Attacks on UAVs.* MILCOM 2022 IEEE Military Communications Conference.

[8] Wang, R., Zhang, Y., Li, J., Liu, S., Sun, D., Wang, T., Wang, T., Chen, Y., **Kara, D.**, & Abdelzaher, T. (2024). *MetaHKG: Meta Hyperbolic Learning for Few-shot Temporal Reasoning.* Proceedings of the 47th International ACM SIGIR Conference on Research and Development in Information Retrieval.

[9] Li, J., Chen, Y., Kimura, T., Wang, T., **Kara, D.**, Hu, Y., Hanafy, W. A., & Abdelzaher, T. (2024). *Acies-OS: A Content-Centric Platform for Edge AI Twinning and Orchestration.* 33rd International Conference on Computer Communications and Networks (ICCCN).

Preprints and Under Review

[1] Kimura, T., Li, J., Wang, T., **Kara, D.**, Chen, Y., Hu, Y., & Wigness, M. (2024). *On the Efficiency and Robustness of Vibration-based Foundation Models for IoT Sensing: A Case Study.* arXiv preprint arXiv:2404.02461.

[2] Kim, K. H., **Kara, D.**, Paruchuri, V., Mohan, S., Kimberly, G., & Kim, J. (2024). *Requiem for a Drone: A Machine-Learning Based Framework for Stealthy Attacks Against Unmanned Autonomous Vehicles.* arXiv preprint arXiv:2407.15003.

[3] Kim, K. H., **Kara, D.**, Paruchuri, V., Mohan, S., Kimberly, G., & Kim, J. (2024). *Requiem: Stealthy Attacks via Finding Adversarial Examples of Non-ML Functions in Unmanned Aerial Vehicles.* (Target: IEEE Symposium on Security and Privacy 2024).

[4] **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.* (Target: USENIX Security Symposium 2025).

[5] **Kara, D.**, Bugra Akyuz, and Secil Arslan. *TRANSPROP: AI-based Propensity Scoring Framework Utilizing Transactional Data Stream.* (Target: Proceedings of the AAAI Conference on Artificial Intelligence).

Technical Skills

Programming Languages: **Python** (Advanced), C++ (Intermediate), Java (Intermediate), MATLAB (Intermediate), R (Intermediate), SQL (Intermediate)
Frameworks and Libraries: PyTorch, TensorFlow, scikit-learn, NumPy, Pandas
Tools and Technologies: AWS, Docker, Spark, ROS, Simulink, Git, WandB

Work Experience

Machine Learning Engineer Jan. 2020 – Aug. 2022
Prometeia *Istanbul, Turkey*

– Implemented an AI-based propensity scoring framework utilizing customer transaction histories as time series, predicting customer interests towards bank products with improved accuracy.

- Developed a deep credit risk default model with novel customer transaction data features, improving recall by 25%.
- Enhanced an automatic car damage estimation system for Allianz Insurance by implementing an image augmentation pipeline and ML-based segmentation model, increasing F1-score by 6%.

Software Design Engineer Jul. 2017 – Dec. 2019

Turkish Aerospace - Autopilot Systems Division *Ankara, Turkey*

- Developed and maintained signal processing libraries for autopilot control system software, reducing signal processing delay by up to 20%.
- Led the interpretation of electromagnetic and vibrational noise within sensor data, developing signal filtering solutions compliant with control algorithms.
- Created a sensor emulator framework, enabling realistic software-in-the-loop simulations for the autopilot department.

Achievements

- **TUBITAK National Scholarship Programme for M.S studies**: Awarded for ranking among the top 50 students nationwide in TUBITAK (NSF of Turkey) Weighted ALES and GPA.
- **Koç University Vehbi Koç High Honors Award**: Recognized for outstanding academic performance with a GPA over 3.50.
- **Turkish Prime Ministry Special Success Scholarship and Koç University Full-Merit Scholarship**: Granted for ranking among the top 100 students in the National University Entrance Exam out of 2 million candidates.