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

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

- Developed a novel misbehavior detection framework against adversarial attacks in vehicular networks.
- The framework is a local misbehavior detection solution embedded into each vehicle, which combines temporal data anomalies and a vehicular trust mechanism with a novel ML architecture.
- Developed various V2X network models for experimentation in an open-source simulation environment (VEINS).
- Working on ML-based adversarial mechanisms for the evaluation of V2X network vulnerabilities.

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

- Working on implementing stealthy sensor-spoofing attacks to compromise UAV security systems.
- Design ML-based adversarial attack mechanisms that additively change sensor values to bypass the existing control mechanisms (EKF) and drift & crash the UAV without alarms.
- Attacks are implemented on virtual UAVs with the Gazebo simulator. Implementations are tested on real hardware, a programmable UAV that runs Linux and the PX4 autopilot to demonstrate attacks on UAV systems.
- Worked on developing multiple UAV missions suitable for training ML models generating adversarial attacks.

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.
- Implemented an in-house data processing tool that allowed faster analysis of test data by other engineers.
- Developed the Sensor Emulator Framework, allowing the autopilot department to perform realistic SIL simulations.

Publications

- **Kara, Denizhan**, Kyo Hyun Kim, Sibin Mohan, Monowar Hasan, Takayuki Shimizu, and Hongsheng Lu. "OVERTON: A Misbehavior Detection and Trust Framework for Vehicular (V2X) Networks." *31st USENIX Security Symposium (USENIX Security 22).* (Under review)
- **Kara, Denizhan**, Bugra Akyuz, and Secil Arslan. "TRANSPROP: AI-based Propensity Scoring Framework Utilizing Transactional Data Stream." *Proceedings of the AAAI Conference on Artificial Intelligence.* 2022 (Under review)

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: AWS, PyTorch, Tensorflow, Simulink, Spark, Storm, Kubernetes, ROS