Onat Gungor

ogungor@ucsd.edu

Contact

Phone: 858-333-1990

Address

Department of Computer Science and Engineering, University of California San Diego, 3235 Voigt Dr, La Jolla, CA 92093

Profile

Research Interests Artificial Intelligence (AI), Machine Learning (ML), Cyber Security, ML Security, Efficient and Robust ML, Predictive Analytics, Internet of Things (IoT), IoT Security, Hyperdimensional Computing

Centers and Collaborators I am actively involved in several research centers including *PRISM*, *CoCoSys*, and *TILOS*; and I collaborate with Intel Labs, and Lawrence Berkeley Lab on various AI-related research projects.

Academic Work Experience

UC San Diego, Computer Science and Engineering Department, La Jolla, CA **January 2024 – Current**

Postdoctoral Scholar

- ✓ Sample projects include: 1) contrastive deep feature modeling for time-series out-of-distribution detection, 2) self-supervised continual learning for ML-based intrusion detection, 3) dynamic defense design for ML-based intrusion detection against adversarial attacks, 4) multimodal LLMs for autonomous driving scenario understanding, 5) an adaptive edge-cloud framework for LLM-based cybersecurity question answering, 6) efficient adversarial defense design for multimodal LLMs against jailbreaking, 7) the design of efficient hybrid state space models, and 8) efficient learning solutions and edge-cloud collaboration for resource-optimized learning.

UC San Diego & San Diego State University, Computer Engineering, San Diego, CA **September 2019 – December 2023**

Graduate Student Researcher

- ✓ Sample projects during my PhD include: 1) robust layered defense for ML-based intrusion detection against adversarial attacks, 2) hyperdimensional computing adversarial attack design for secure IoT, 3) resilient stacking ensemble against adversarial attacks for remaining useful life estimation, 4) diversity-induced optimally weighted ensemble learning for IIoT predictive analytics, and 5) robust indoor sensor placement under distance uncertainty.

Education

2019 - 2023 **UC San Diego and San Diego State University, San Diego, CA**
PhD, Electrical and Computer Engineering
PhD Thesis: Towards Intelligent, Secure, and Efficient Industrial Internet of Things

2016 - 2019 **Ozyegin University, Istanbul, Turkey**
Bachelor of Science, Computer Science and Engineering

2014 - 2018 **Ozyegin University, Istanbul, Turkey**
Bachelor of Science, Industrial Engineering
Minor: Business Administration

Publications

1. Sean Fuhrman, **Onat Gungor,** Tajana Rosing. CND-IDS: Continual Novelty Detection for Intrusion Detection Systems. ACM/IEEE Design Automation Conference (DAC). 2025. (accepted)
2. Le Zhang, Quanling Zhao, Run Wang, Shirley Bian, **Onat Gungor,** Flavio Ponzina, Tajana Rosing. ORCA: Offload Rethinking by Cloud Assistance for Efficient Environmental Sound Recognition on LPWANs. ACM Conference on Embedded Networked Sensor Systems (SenSys). 2025. (accepted)
3. **Onat Gungor**, Amanda Rios, Nilesh Ahuja, Tajana Rosing. TS-OOD: An Evaluation Framework for Time-Series Out-of-Distribution Detection and Prospective Directions for Progress. AAAI’25 Workshop on AI for Time Series Analysis (AI4TS). 2025.

4. Cagla Ipek Kocal, **Onat Gungor,** Tajana Rosing, Baris Aksanli. ReLATE: Resilient Learner Selection for Multivariate Time-Series Classification Against Adversarial Attacks. AAAI’25 Workshop on AI for Time Series Analysis (AI4TS). 2025.
5. Elvin Li, Zhengli Shang, **Onat Gungor,** Tajana Rosing. SAFE: Self-Supervised Anomaly Detection Framework for Intrusion Detection. AAAI’25 Workshop on AI for Cyber Security (AICS). 2025.
6. Le Zhang, **Onat Gungor,** Flavio Ponzina, Tajana Rosing. E-QUARTIC: Energy Efficient Edge Ensemble of Convolutional Neural Networks for Resource-Optimized Learning. Asia and South Pacific Design Automation Conference *(ASP-DAC)* 2025.
7. **Onat Gungor,** Amanda Rios, Priyanka Mudgal, Nilesh Ahuja, Tajana Rosing. A Robust Framework for Evaluation of Unsupervised Time-series Anomaly Detection. International Conference on Pattern Recognition (ICPR) 2024.
8. Fatemeh Asgarinejad, Flavio Ponzina, **Onat Gungor,** Tajana Rosing, Baris Aksanli. HDXpose: Harnessing Hyperdimensional Computing's Explainability for Adversarial Attacks. *ACM/IEEE International Conference on Computer-Aided Design (ICCAD)* 2024.
9. **Onat Gungor,** Tajana Rosing, Baris Aksanli. A2HD: Adaptive Adversarial Training for Hyperdimensional Computing-Based Intrusion Detection Against Adversarial Attacks. *IEEE International Conference on Cyber Security and Resilience (CSR)*. 2024.
10. **Onat Gungor,** Elvin Li, Zhengli Shang, Yutong Guo, Jing Chen, Johnathan Davis, Tajana Rosing. Rigorous Evaluation of Machine Learning-based Intrusion Detection Against Adversarial Attacks. *IEEE International Conference on Cyber Security and Resilience (CSR)*. 2024.
11. **Onat Gungor,** Tajana Rosing, Baris Aksanli. ROLDEF: Robust Layered Defense for Intrusion Detection Against Adversarial Attacks. *Design, Automation and Test in Europe (DATE).* 2024.
12. Xiaofan Yu, Minxuan Zhou, Fatemeh Asgarinejad, **Onat Gungor,** Baris Aksanli, Tajana Rosing. Private and Secure Learning at the Edge with Hyperdimensional Computing. *ACM/IEEE Design Automation Conference (DAC)*, 2023.
13. Mitchell Timken, **Onat Gungor,** Tajana Rosing, Baris Aksanli. Analysis of Machine Learning Algorithms for Cyber Attack Detection in SCADA Power Systems. *International Conference on Smart Applications, Communications and Networking (SmartNets)*. 2023.
14. **Onat Gungor,** Tajana Rosing, Baris Aksanli. Adversarial-HD: Hyperdimensional Computing Adversarial Attack Design for Secure Industrial Internet of Things. *IEEE/ACM Workshop on the Internet of Safe Things, co-located with CPS-IoT Week*. 2023. **(Best paper runner-up)**
15. **Onat Gungor,** Tajana Rosing, Baris Aksanli. HD-I-IoT: Hyperdimensional Computing for Resilient Industrial Internet of Things Analytics. *Design, Automation and Test in Europe (DATE).* 2023.
16. **Onat Gungor,** Tajana Rosing, Baris Aksanli. DENSE-DEFENSE: Diversity Promoting Ensemble Adversarial Training Towards Effective Defense. *IEEE SENSORS*. 2022.
17. **Onat Gungor,** Tajana Rosing, Baris Aksanli. STEWART: Stacking Ensemble for White-Box Adversarial Attacks Towards More Resilient Data-driven Predictive Maintenance. *Computers in Industry.* 2022.
18. **Onat Gungor,** Tajana Rosing, Baris Aksanli. CAHEROS: Constraint-Aware Heuristic Approach for RObust Sensor Placement. *IEEE SENSORS*. 2021.
19. **Onat Gungor,** Tajana Rosing, Baris Aksanli. ENFES: Ensemble Few-Shot Learning for Intelligent Fault Diagnosis with Limited Data. *IEEE SENSORS*. 2021.
20. **Onat Gungor,** Tajana Rosing, Baris Aksanli. DOWELL: Diversity-induced Optimally Weighted Ensemble Learner for Predictive Maintenance of Industrial Internet of Things Devices. *IEEE Internet of Things Journal*. 2021.
21. **Onat Gungor,** Tajana Rosing, Baris Aksanli. RESPIRE++: Robust Indoor Sensor Placement Optimization under Distance Uncertainty. *IEEE Sensors Journal*. 2021.
22. **Onat Gungor,** Tajana Rosing, Baris Aksanli. OPELRUL: Optimally Weighted Ensemble Learner for Remaining Useful Life Prediction. *IEEE International Conference on Prognostics and Health Management (ICPHM)*. 2021.
23. **Onat Gungor,** Jake Garnier, Tajana Rosing, Baris Aksanli. LENARD: Lightweight Ensemble Learner for Medium-term Electricity Consumption Prediction. *IEEE International Conference on Smart Grid Communications.* 2020.
24. **Onat Gungor,** Tajana Rosing, Baris Aksanli. RESPIRE: Robust Sensor Placement Optimization in Probabilistic Environments. *IEEE SENSORS*. 2020. **(Best paper nominee)**
25. **Onat Gungor,** Baris Aksanli, Reyhan Aydogan. Algorithm Selection and Combining Multiple Learners for Residential Energy Prediction. *Future Generation Computer Systems (FGCS)*. 2019.
26. **Onat Gungor,** Umut Cakan, Reyhan Aydogan, Pinar Ozturk. Effect of Awareness of Other Side’s Gain on Negotiation Outcome, Emotion, Argument and Bidding Behavior. International Workshop on Agent-Based Complex Automated Negotiation *(ACAN)* 2019. **(Best student paper)**

Mentoring

- Nilesh Pandey (PhD): Efficient Machine Learning and Hybrid State Space Models for Edge Computing
- Ye Tian (PhD): Multimodal Large Language Models and Physical World Comprehension
- Le Zhang (MS): Efficient Edge Ensemble and Edge-Cloud Collaboration for Resource-Optimized Learning
- Sean Fuhrman (MS): Continual Novelty Detection for Network Intrusion Detection
- Ipek Kocal (MS): Resilient Time-series Classification Against Adversarial Attacks
- Abhilash Shankarampeta (MS): Adversarial Robustness of Multimodal Large Language Models
- Jing Chen (BS): Dynamic Defense Design for ML-based IDS Against Adversarial Attacks
- Elvin Li, Charlie Shang (BS): Self-supervised Learning for Robust Intrusion Detection
- Ishaan Kale, Jiasheng Zhou (BS): Anomaly-based Host Intrusion Detection
- Harry Wang, Roshan Sood (BS): Robust LLM-Based Cybersecurity Question Answering Against Jailbreaking
- Matilda Gaddi (BS): Adaptive Edge-Cloud Framework for Cybersecurity Question Answering Using LLMs

Honors and Awards

- Best paper runner-up, ACM/IEEE SafeThings, May 2023
- San Diego State University, University Graduate Fellowship, August 2021
- Best paper nominee, IEEE SENSORS Conference, October 2020
- Best student paper, International Workshop on Agent-based Complex Automated Negotiations (ACAN), 2019
- Ozyegin University High Honor Degree, 2019: Faculty of Engineering, Computer Science and Engineering
- Ozyegin University, Valedictorian Award, June 2018

Teaching Experience

CSE 15L – UC San Diego, Computer Science and Engineering Department

- ✓ Semesters: Fa23, Sp22
- ✓ Instructor of the undergraduate freshman level course "Software Tools and Techniques".
- ✓ The class teaches useful software tools and techniques such as version control, Vim, Unix commands, shell script debugging, test-driven development, continuous integration, and clean coding.

CSE 140 – UC San Diego, Computer Science and Engineering Department (Instructor)

- ✓ Semesters: Su22
- ✓ Instructor of the undergraduate junior level course "Components and Design Techniques for Digital Systems".
- ✓ The class teaches digital logic design, using topics such as Boolean logic, finite state machines, combinational lc design, combinational modules, Mealy and Moore machines, and sequential modules.

COMPE 375 - San Diego State University, Electrical and Computer Engineering Department

- ✓ Semesters: Su21, Su22 (Teaching Assistant)
- ✓ Assisted the undergraduate junior level course "Embedded Systems Programming".
- ✓ This class teaches programming and debugging code for multiple microcontrollers, using topics such serial/general-purpose I/O, timers, interrupts, ADC, DAC, and memory programming.

CSE 140 – UC San Diego, Computer Science and Engineering Department

- ✓ Semesters: Wi22 (Teaching Assistant)
- ✓ Assisted the undergraduate junior level course "Components and Design Techniques for Digital Systems".

Academic Service and Outreach

- **Journal and Conference Reviews**
  - IEEE Transactions on Information Forensics and Security
  - IEEE Internet of Things Journal
  - IEEE Transactions on Industrial Informatics
  - IEEE Transactions on Industrial Electronics
  - IEEE Transactions on Network and Service Management
  - Conferences: ASPLOS'25, DATE'25, ECAI'24, MICRO'24, DAC'23, SENSORS'22