Onat Gungor

Personal Website | Google Scholar | 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 Machine Learning (ML), Cyber Security, ML-based Intrusion Detection, ML Security, LLM Security, Robust ML, Scalable ML, Predictive Analytics, Internet of Things (IoT), IoT Security

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.

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, and 7) the design of efficient hybrid state space models.

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 (# of citations: 212, h-index: 8, i10-index: 7)

1. Nilesh Prasad Pandey, Shriniwas Kulkarni, David Wang, **Onat Gungor,** Flavio Ponzina, Tajana Rosing. DPQ-HD: Post-Training Compression for Ultra-Low Power Hyperdimensional Computing. ACM Great Lakes Symposium on VLSI (GLSVLSI). 2025. **(accepted)**
2. Cagla Ipek Kocal, **Onat Gungor,** Aaron Tartz, Tajana Rosing, and Baris Aksanli. ReLATE: Resilient Learner Selection for Multivariate Time-Series Classification Against Adversarial Attacks. IEEE International Conference on Cyber Security and Resilience (CSR). 2025. **(accepted)**
3. Jing Chen, **Onat Gungor,** Zhengli Shang, Elvin Li, and Tajana Rosing. DYNAMITE: Dynamic Defense Selection for Enhancing Machine Learning-based Intrusion Detection Against Adversarial Attacks. IEEE/ACM Workshop on the Internet of Safe Things, co-located with 46th IEEE Symposium on Security and Privacy. 2025. **(accepted)**
4. Ye Tian, **Onat Gungor,** Xiaofan Yu, Tajana Rosing. Poster: Fine-grained Contextualized Activity Logs Generation based on Multi-Modal Sensor Data and LLM. ACM Conference on Embedded Networked Sensor Systems (SenSys). 2025.

5. Sean Fuhrman, **Onat Gungor,** Tajana Rosing. CND-IDS: Continual Novelty Detection for Intrusion Detection Systems. ACM/IEEE Design Automation Conference (DAC). 2025. (Acceptance Rate: 23%)
6. 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. (Acceptance Rate: 18%)
7. **Onat Gungor,** Amanda Rios, Nilesh Ahuja, Tajana Rosing. TS-OOD: An Evaluation Framework for Time-Series Out-of-Distribution Detection. AAAI’25 Workshop on AI for Time Series Analysis (AI4TS). 2025.
8. 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.
9. 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. (Acceptance Rate: 28%)
10. **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.
11. 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. (Acceptance Rate: 24%)
12. **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.
13. **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.
14. **Onat Gungor,** Tajana Rosing, Baris Aksanli. ROLDEF: Robust Layered Defense for Intrusion Detection Against Adversarial Attacks. Design, Automation and Test in Europe (DATE). 2024. (Acceptance Rate: 25%)
15. 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.
16. 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.
17. **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)**
18. **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. (Acceptance Rate: 25%)
19. **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.
20. **Onat Gungor,** Tajana Rosing, Baris Aksanli. DENSE-DEFENSE: Diversity Promoting Ensemble Adversarial Training Towards Effective Defense. *IEEE SENSORS*. 2022.
21. **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.
22. **Onat Gungor,** Tajana Rosing, Baris Aksanli. RESPIRE++: Robust Indoor Sensor Placement Optimization under Distance Uncertainty. *IEEE Sensors Journal*. 2021.
23. **Onat Gungor,** Tajana Rosing, Baris Aksanli. CAHEROS: Constraint-Aware Heuristic Approach for Robust Sensor Placement. *IEEE SENSORS*. 2021.
24. **Onat Gungor,** Tajana Rosing, Baris Aksanli. ENFES: Ensemble Few-Shot Learning for Intelligent Fault Diagnosis with Limited Data. *IEEE SENSORS*. 2021.
25. **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.
26. **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.
27. **Onat Gungor,** Tajana Rosing, Baris Aksanli. RESPIRE: Robust Sensor Placement Optimization in Probabilistic Environments. *IEEE SENSORS*. 2020. **(Best paper nominee)**
28. **Onat Gungor,** Baris Aksanli, Reyhan Aydogan. Algorithm Selection and Combining Multiple Learners for Residential Energy Prediction. *Future Generation Computer Systems (FGCS)*. 2019. (Impact factor: 6.2)

29. **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)**

Teaching Experience

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

- ✓ Semesters: Fa23, Sp22 (Instructor)
- ✓ Instructing 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 scripting, debugging, test-driven development, continuous integration, and clean coding.

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

- ✓ Semesters: Su22 (Instructor); Wi22 (TA)
- ✓ Instructing 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 logic 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 as serial/general-purpose I/O, timers, interrupts, ADC, DAC, and memory programming.

Mentoring

- Ye Tian (PhD): Multimodal Large Language Models and Physical World Comprehension; **Publication: SenSys'25**
- Nilesh Pandey (PhD): Efficient Machine Learning for Edge Computing; **Publication: GLSVLSI'25**
- Fatemeh Asgarinejad (PhD): Hyperdimensional Computing Against Adversarial Attacks; **Publication: ICCAD'24**
- Le Zhang (MS): Efficient Edge AI for Resource-Optimized Learning; **Publications: SenSys'25, ASPDAC'25**
- Sean Fuhrman (MS): Continual Novelty Detection for Network Intrusion Detection; **Publication: DAC'25**
- Ipek Kocal (MS): Resilient Time-series Classification Against Adversarial Attacks; **Publication: CSR'25, AI4TS'25**
- Abhilash Shankarampeta (MS): Adversarial Robustness of Multimodal Large Language Models
- Mitchell Timken (MS): ML for Cyber Attack Detection in SCADA Power Systems; **Publication: SmartNets'23**
- Jing Chen (BS): Dynamic Defense Design for ML-based IDS Against Adversarial Attacks; **Publication: SafeThings'25**
- Elvin Li, Charlie Shang (BS): Self-supervised Learning for Robust Intrusion Detection; **Publication: AICS'25, CSR'24**
- Harry Wang, Roshan Sood (BS): Robust LLM-Based Cybersecurity Question Answering Against Jailbreaking
- Jake Garnier (BS): Ensemble Learner for Electricity Consumption Prediction; **Publication: SmartGridComm'20**

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
- Ozyegin University, Valedictorian Award, June 2018

Academic Service and Outreach

- **Journal and Conference Reviews**
  - Journals: IEEE Transactions on Information Forensics and Security; IEEE Transactions on Dependable and Secure Computing; IEEE Internet of Things Journal; IEEE Transactions on Network and Service Management; IEEE Transactions on Industrial Informatics; IEEE Transactions on Industrial Electronics
  - Conferences: CSR'25, ECAI'25, ASPLOS'25, DATE'25, ECAI'24, MICRO'24, CODES+ISSS'23, DAC'23