Onat Gungor

ogungor@ucsd.edu
GoogleScholar

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, Security, Time-series Analysis, Predictive Analytics, Internet of Things, Cyber-physical Systems, Hyperdimensional Computing

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

Academic Work Experience

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

- ✓ At System Energy Efficiency Lab, working on time-series anomaly detection, ML security against adversarial attacks, self-supervised, continual learning solutions for IoT security, and ML-based network and host intrusion detection.
- ✓ Sample projects include 1) robust framework for evaluation of unsupervised time-series anomaly detection, 2) effective defense mechanism for ML-based intrusion detection against adversarial attacks, 3) unsupervised continual learning for intrusion detection, and 4) energy efficient learning for resource-optimized learning.

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

- ✓ Sample projects during my PhD include 1) robust layered defense for intrusion detection against adversarial attacks, 2) hyperdimensional computing adversarial attack design for secure IIoT, 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 & 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
Bachelor Thesis: Algorithm Selection for Residential Energy Prediction

2014 - 2018 **Ozyegin University, Istanbul, Turkey**
Bachelor of Science, Industrial Engineering
Minor: Business Administration
Bachelor Thesis: Automated Prediction Tool for Unilever Tea Sales

Teaching Experience

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

- ✓ Semesters: Fa23, Sp22
- ✓ Instructing the undergraduate 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
- ✓ Instructing the 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 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.

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

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

IE 342 - Ozyegin University, Industrial Engineering Department, Istanbul, Turkey

- ✓ Semesters: Sp18 (Teaching Assistant)
- ✓ Gave lectures in problem sessions of the course "Mathematical Optimization and Exact Methods".

IE 203 - Ozyegin University, Industrial Engineering Department, Istanbul, Turkey

- ✓ Semesters: Fa17 (Teaching assistant)
- ✓ Gave lectures in discussion sessions of the course "Engineering Economics" and held office hours.

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

Mentoring

- Fatemeh Asgarinejad (PhD): Harnessing Hyperdimensional Computing's Explainability for Adversarial Attacks
- Le Zhang (MS): Energy Efficient Edge Ensemble of Convolutional Neural Networks for Resource-Optimized Learning
- Sean Fuhrman (MS): Unsupervised Continual Learning for Industrial Internet of Things Intrusion Detection
- Ipek Kocal (MS): Resilient Time-series Classification Against Adversarial Attacks
- Mohammed Ibrar (MS): Hyperdimensional Computing for RSSI-based BLE Localization
- Mitchell Timken (MS): Machine Learning for Cyber Attack Detection in SCADA Power Systems
- Sai Singapati, Kavan Mehta (MS): Ensemble Learning for Electricity Consumption Prediction
- Jing Chen, Johnathan Davis, Yutong Guo (BS): Realistic Defense for ML-based IDS Against Adversarial Attacks
- Elvin Li, Charlie Shang (BS): Self-supervised Learning for Robust Intrusion Detection
- David Anwyl, Hunter Trieu, Jiasheng Zhou, Ishaan Kale (BS): Anomaly-based Host Intrusion Detection
- Ata Altyyev (BS): Resilient Hyperdimensional Computing Against Adversarial Attacks
- Jake Garnier (BS): Lightweight Ensemble Learner for Medium-term Electricity Consumption Prediction

Publications

1. Le Zhang, Flavio Ponzina, **Onat Gungor,** 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. (accepted)
2. **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. (accepted)
3. 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. (accepted)
4. **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. (accepted)

5. **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. (accepted)
6. **Onat Gungor,** Tajana Rosing, Baris Aksanli. ROLDEF: RObust Layered DEFense for Intrusion Detection Against Adversarial Attacks. *Design, Automation and Test in Europe (DATE).* 2024.
7. Xiaofan Yu, Minxuan Zhou, Fatemeh Asgarinejad, **Onat Gungor,** Baris Aksanli, Tajana Rosing. Private and Secure Learning at the Edge with Hyperdimensional Computing. *IEEE/ACM Design Automation Conference (DAC)*, 2023.
8. 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.
9. **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)**
10. **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.
11. **Onat Gungor,** Tajana Rosing, Baris Aksanli. DENSE-DEFENSE: Diversity Promoting Ensemble Adversarial Training Towards Effective Defense. *IEEE SENSORS*. 2022.
12. **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.
13. **Onat Gungor,** Tajana Rosing, Baris Aksanli. CAHEROS: Constraint-Aware HEuristic Approach for RObust Sensor Placement. *IEEE SENSORS*. 2021.
14. **Onat Gungor,** Tajana Rosing, Baris Aksanli. ENFES: ENsemble FEw-Shot Learning for Intelligent Fault Diagnosis with Limited Data. *IEEE SENSORS*. 2021.
15. **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.
16. **Onat Gungor,** Tajana Rosing, Baris Aksanli. RESPIRE++: Robust Indoor Sensor Placement Optimization under Distance Uncertainty. *IEEE Sensors Journal*. 2021.
17. **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.
18. **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 (SmartGridComm).* 2020.
19. **Onat Gungor,** Tajana Rosing, Baris Aksanli. RESPIRE: Robust Sensor Placement Optimization in Probabilistic Environments. *IEEE SENSORS*. 2020. **(Best paper nominee)**
20. **Onat Gungor,** Baris Aksanli, Reyhan Aydogan. Algorithm Selection and Combining Multiple Learners for Residential Energy Prediction. *Future Generation Computer Systems (FGCS)*. 2019.
21. **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)**

Academic Service and Outreach

- **Journal and Conference Reviews**
    - IEEE Transactions on Information Forensics and Security
    - IEEE Transactions on Industrial Informatics
    - IEEE Internet of Things Journal
    - IEEE Transactions on Industrial Electronics
    - Conferences: ECAI'24, MICRO'24, DAC'23, SENSORS'22
- **Graduate Mentor in ENLACE Research Program, 2021**
    - **Students:** Denisse Gabriela López, Mauricio Monroy, Marian Alondra Chavira, María Pimentel Villegas
    - **Project:** Optimally Weighted Ensemble Learner for Remaining Useful Life Estimation