UNIVERSITÀ DI PISA

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

Dottorato di Ricerca in Ingegneria dell'Informazione

Doctoral Course

"Secure and Resilient Cyber-Physical Systems for Smart Living"

Prof. Sajal K. Das, Ph.D., IEEE Fellow
Curator's Distinguished Professor
Daniel St. Clair Endowed Chair
Department of Computer Science
Missouri University of Science and Technology
Rolla, MO, USA

E-mail address: sdas@mst.edu

Short Abstract:

Cyber-Physical Systems (CPS), comprising Internet of Things (IoT), have a wide variety of applications to smart environments, such as smart grid, smart transportation, smart water distribution networks, smart manufacturing, smart healthcare, and smart agriculture. The aim is to improve human quality of life and make the society a safer place to live in. However, smart living CPS and IoT domains are vulnerable to a wide variety of unsafe events, threats, adversarial attacks (e.g., false data injection, data poisoning or evasion, deliberate data manipulation or perturbation). Detecting and interpreting such threats in real time is vital to proactively respond to the underlying cause and prevent immediate impacts on civilians and the economy. Threats manifest themselves as anomalies in the sensed time series data and machine learning model parameters, and can be formulated as an anomaly detection problem, where we first learn the underlying mathematical structure of benign behavior and then detect anomalies as deviations from the learned structure.

This research-based Ph.D. course aims to cover a unified theory for detecting anomalies (threats) in smart living CPS in a lightweight, timely, and unsupervised manner. The approach is based on deriving invariants and latent space that use time series data analytics, machine learning, information theory, and reputation scoring, and ecology models. The proposed unified theory will be validated using real-world data collected from multiple CPS and IoT domains such as smart grid, smart transportation, and smart water networks. The course will be concluded with future research directions.

Course Contents in brief:

- Sensors, IoT, CPS and UAV Networks
- Smart Environments
- Security Challenges in CPS
- Machine Learning and Mathematical Models
- Mobile Crowd Sensing

- Securing Smart Living CPS
  - Smart Grid
  - Smart Transportation
  - Smart Water Distribution
- Smart Agriculture and Smart Healthcare
- Conclusions and Open Problems

Total # of hours of lecture: 16

References:

1. A. Oluyomi, S. Abedzadeh, S. Bhattacharjee, and S. K. Das, "Unsafe Events Detection in Smart Water Meter Infrastructure via Noise-Resilient Learning," *IEEE/ACM Conference on Cyber-Physical Systems (ICCPS)*, Hong Kong, May 2024.
2. P. Roy, S. Bhattacharjee, S. Abezadeh, and S. K. Das, "Noise Resilient Learning for Attack Detection in Smart Grid PMU Infrastructure," *IEEE Transactions on Dependable and Secure Computing* (Special Issue on Reliability and Robustness in AI-Based Cybersecurity Solutions), 21(2): 618-635, Mar-Apr 2024.
3. M. J. Islam, J. P. Talusan, S. Bhattacharjee, F. Tiausas, A. Dubey, K. Yasumoto, S. K. Das, "Scalable Pythagorean Mean based Incident Detection in Smart Transportation Systems," *ACM Transactions on Cyber-Physical Systems*, 8(2):20, May 2024. (Preliminary version in ICCPS'22.)
4. S. Bhattacharjee and S. K. Das, "Unifying Threats against Information Integrity in Participatory Crowd Sensing," *IEEE Pervasive Computing*, 22(4): 66-75, Oct 2023.
5. A. Vangala, A. K. Das, A. Mitra, S. K. Das, and Y.-H. Park, "Blockchain-Enabled Authenticated Key Agreement Scheme for Mobile Vehicles-Assisted Precision Agricultural IoT Networks," *IEEE Transactions on Information Forensics and Security*, 18: 904-919, 2023.
6. S. Bhattacharjee and S. K. Das, "Building a Unified Data Falsification Threat Landscape for IoT/CPS Applications" *IEEE Computer* (Cover Issue: Better Living Through Challenges), 56(3): 20-31, Mar 2023.
7. P. Ranjan, A. Gupta, F. Coro, and S. K. Das, "Securing Federated Learning against Overwhelming Collusive Attackers," *IEEE Global Communications Conference* (Globecom), pp. 1448-1453, Dec 2022.
8. V. P. K. Madhavarapu, P. Roy, S. Bhattacharjee, and S. K. Das, "Active Learning Augmented Folded Gaussian Model for Anomaly Detection in Smart Transportation," *IEEE International Conference on Communications* (ICC), South Korea, May 2022.
9. S. Bhattacharjee, V. P. Madhavarapu, and S. K. Das, "A Diversity Index based Scoring Framework for Identifying Smart Meters Launching Stealthy Data Falsification Attacks," *ACM Asia Conference on Computer and Communications Security* (Asia CCS), pp. 26-39, June 2021.
10. S. Bhattacharjee, V. K. P. Madhavarapu, S. Silvestri, and S. K. Das, "Attack Context Embedded Data Driven Trust Diagnostics in Smart Metering Infrastructure," *ACM Transactions on Privacy and Security*, 24(2): 9:1-9:36, Apr 2021.
11. S. Bhattacharjee and S. K. Das, "Detection and Forensics against Stealthy Data Falsification in Smart Metering Infrastructure," *IEEE Transactions on Dependable and Secure Computing*, 18(1): 356-371, 2021.
12. A. Sturaro, S. Silvestri, M. Conti, and S. K. Das, "A Realistic Model for Failure Propagation in Interdependent Cyber-Physical Systems," *IEEE Transactions on Network Science and Engineering* (Special Issue on Network Science for High-Confidence Cyber-Physical Systems), 7(2): 817-831, Apr-June 2020.
13. R. P. Barnwal, N. Ghosh, S. K. Ghosh, and S. K. Das, "Publish or Drop Traffic Event Alerts? Quality-aware Decision Making in Participatory Sensing-based Vehicular CPS," *ACM Transactions on Cyber-Physical Systems* (Special Issue on Transportation Cyber-Physical Systems), 4(1): 9:1 – 9:28, Jan 2020.
14. S. Bhattacharjee, N. Ghosh, V. K. Shah, and S. K. Das, "QnQ: Quality and Quantity based Unified Approach for Secure and Trustworthy Mobile Crowdsensing," *IEEE Transactions on Mobile Computing*, 19(1): 200-216, Jan 2020.
15. S. Roy and S. K. Das, *Principles of Cyber-Physical Systems: An Interdisciplinary Approach*, Cambridge University Press, 2020.
16. S. K. Das, K. Kant and N. Zhang, *Handbook on Securing Cyber-Physical Critical Infrastructure: Foundations and Challenges*, Morgan-Kauffman, 2012.
17. D. J. Cook and S. K. Das, *Smart Environments: Technology, Protocols and Applications*, John Wiley, 2005.

CV of the Teacher

Dr. Sajal K. Das is a Curators' Distinguished Professor of Computer Science, and the Daniel St. Clair Endowed Chair at Missouri University of Science and Technology, where he was the chair of Computer Science Department during 2013-2017. He also served the National Science Foundation (NSF) as a Program Director in the Computer and Network Systems Division. His interdisciplinary research interests include mobile and pervasive computing, wireless and sensor networks, cyber–physical systems, IoT, UAVs, smart environments, data science, machine learning, cyber security, biological and social networks, applied graph theory and game theory. Dr. Das has made fundamental contributions to these areas and published more than 300 papers in high quality journals and more than 400 papers in refereed conference proceedings. He holds 5 US patents, co-authored 4 books and 60 book chapters, and directed over $25 million funded research projects. His h-index is 102 with more than 44,000 citations according to Google Scholar. He is a recipient of 14 Best Paper Awards in prestigious conferences like ACM MobiCom and IEEE PerCom, and numerous awards for teaching, mentoring and research including the IEEE Computer Society's Technical Achievement Award for pioneering contributions to sensor networks and mobile computing, and the University of Missouri System President's Award for Sustained Career Excellence. Dr. Das serves as the founding Editor-in-Chief of Elsevier's *Pervasive and Mobile Computing* journal, and Associate Editor of the *IEEE Transactions on Dependable and Secure Computing*, *IEEE Transactions on Sustainable Computing*, *IEEE/ACM Transactions on Networking*, and *ACM Transactions on Sensor Networks*. A founder of IEEE PerCom, WoWMoM, SMARTCOMP and ACM ICDCN conferences, he has served as General and Program Chair of numerous conferences and workshops. He has graduated 11 postdoctoral fellows, 51 Ph.D. scholars, 31 M.S. thesis students, and numerous undergraduate researchers. Currently 10 Ph.D. students and 4 postdocs are being mentored by him. Dr. Das is a Distinguished Alumnus of the Indian Institute of Science, Bangalore, and a Fellow of the IEEE, National Academy of Inventors (NAI), and Asia-Pacific Artificial Intelligence Association (AAIA), His academic genealogy includes Thomas Alva Edison.

Final Exam: method of final examination to be determined

Room and Schedule:

Room: *Meeting Room, Dept. of Information Engineering, Largo Lazzarino 1, Pisa*

Schedule:

May 12 – 2:00-6:00 pm

May 13 – 10:30-12:30 am; 2:00-4:00 pm

May 14 – 10:30-12:30 am; 2:00-4:00 pm

May 15 – 10:30-12:30 am; 2:00-4:00 pm