KEYNOTE/PLENARY

Title:

Adversarial Time Series Threats in Cyber-Physical Sensor Networks

Speaker:

Prof. Salil Kanhere

School of Computer Science and Engineering, The University of New South Wales, Sydney

Abstract

Modern cyber-physical systems and IoT deployments rely on distributed sensor networks, where time-series data increasingly drive automated monitoring, forecasting, and control decisions. Machine learning models operating on these streams are now deeply embedded in networked infrastructure, spanning industrial control, smart cities, healthcare, and critical services. Yet adversarial robustness for such systems remains poorly understood, particularly under the constraints imposed by real-world networks.

This talk will examine adversarial attacks on time-series models deployed in sensor networks from three perspectives that directly reflect operational realities: sparse perturbations that modify only a small fraction of sensor readings, constraint-adhering perturbations that remain physically and statistically consistent across correlated sensors, and streaming attacks that operate under real-time and partial-visibility constraints. Across multiple multi-sensor IoT and industrial datasets, these attacks significantly degrade state-of-the-art models while evading anomaly detection mechanisms commonly used in networked monitoring systems.

We will conclude by discussing the implications of these results for the design of secure, networked sensing infrastructures. The talk highlights why detection alone is insufficient, how inter-sensor dependencies can be exploited rather than protected, and why defending time-series models in cyber-physical systems requires threat models that explicitly account for network topology, temporal dynamics, and online operation.

Biography

Salil Kanhere is a Professor at the School of Computer Science and Engineering at UNSW Sydney, Australia. His research interests span cybersecurity, pervasive computing, IoT, blockchain, and applied machine learning. He is an IEEE Fellow, an AAIS Fellow, and an ACM Distinguished Member. He received the Friedrich Wilhelm Bessel Research Award (2020) and the Humboldt Research Fellowship (2014) from the Alexander von Humboldt Foundation in Germany; the IEEE ComSoc IoT, Ad Hoc and Sensor Networks Technical Committee (IoT-AHSN TC) Technical Achievement and Recognition Award (2025); and 12 Best Paper Awards. He serves on the advisory board of three SMEs and has held visiting positions at RWTH Aachen, I2R Singapore, Technical University Darmstadt, the University of Zurich, and Graz University of Technology. Salil is the Editor in Chief of the Ad Hoc Networks journal and an Associate Editor of IEEE Transactions on Network and Service Management, Computer Communications, and Pervasive and Mobile Computing. He has participated in organising committees for several IEEE/ACM international conferences and is a member of the steering committees for IEEE LCN and IEEE ICBC. Salil has also co-authored two books.