University of Cyprus
Department of Electrical and Computer Engineering

Title: A Control-Theoretical Zero-Knowledge Proof Scheme for Networked Control Systems

Gabriele Oliva

Associate Professor in Automatic Control

University Campus Bio-Medico of Rome

Wednesday 9th of October 2024, 17:00 - 18:00

Room: ΧΩΔ02 -B107

Abstract: Networked Control Systems (NCS) are pivotal for sectors like industrial automation, autonomous vehicles, and smart grids. However, combining communication networks with control loops brings complexities and security vulnerabilities, necessitating strong protection and authentication measures. This talk introduces an innovative Zero-Knowledge Proof (ZKP) scheme tailored for NCSs, enabling a networked controller to prove its knowledge of the dynamical model and its ability to control a discrete-time linear time-invariant (LTI) system to a sensor, without revealing the model. This verification is done through the controller's capacity to produce suitable control signals in response to the sensor's output demands. The completeness, soundness, and zero-knowledge properties of the proposed approach are demonstrated. The scheme is subsequently extended by considering the presence of delays and output noise. Additionally, a dual scenario where the sensor proves its model knowledge to the controller is explored, enhancing the method's versatility.

Biography: Gabriele Oliva received the M.sc and the Ph.D. degrees in computer science and automation engineering from the University Roma Tre of Rome, Italy, in 2008 and 2012, respectively. He is currently an Associate Professor in automatic control with the University Campus Bio-Medico of Rome, Italy, where he directs the Complex Systems & Security Laboratory (CoserityLab). Since 2019, he serves as Associate Editor on the Conference Editorial Board of the IEEE Control Systems Society. Moreover, since 2022 he is an Associate Editor for the IEEE Control Systems Letters Journal. His main research interests include distributed multi-agent systems, optimization, estimation, decision-making and critical infrastructure protection.