Abstract and bio, György Dán, professor KTH

AI for Energy Security: A Blessing or a Threat

Machine learning an AI have found numerous applications in the area of energy systems recently, from building energy managements systems, through controlling the cooling of data centers to state estimation and solving optimal power flow in power systems. While there is no one-size-fits all ML solution to these problems, well designed ML solutions often outperform algorithmic approaches under computing time constraints. This raises the question whether they are equally effective in computing attacks against these systems. In this talk we discuss recent results that show that this is indeed the case, and through the examples of automatic generation control and secondary control of microgrids we highlight the pressing need for assessing the adversarial robustness of optimization and control schemes in power systems.

Bio György Dán, professor KTH

György Dán is a professor at KTH Royal Institute of Technology, Stockholm, Sweden. He received the M.Sc. in computer engineering from the Budapest University of Technology and Economics, Hungary in 1999, the M.Sc. in business administration from the Corvinus University of Budapest, Hungary in 2003, and the Ph.D. in Telecommunications from KTH in 2006. He worked as a consultant in the field of access networks, streaming media and videoconferencing 1999-2001. He was a visiting researcher at the Swedish Institute of Computer Science in 2008, a Fulbright research scholar at University of Illinois at Urbana-Champaign in 2012-2013, and an invited professor at EPFL in 2014-2015. He served as area editor of Computer Communications 2014-2021, and has been editor of IEEE Transactions on Mobile Computing 2019-2023. He currently serves as director of third cycle education at EECS. His research interests include the design and analysis of content management and computing systems, game theoretical models of learning in networked systems, and cyber-physical system security and resilience.