Date: 13th February 2024 (Tuesday)
Time: 5:30PM
Room: RM101

Title: Spiking Neural Networks: Training and Adversarial Robustness Properties

Speaker: Dr. Bhaskar Mukhoty (MBZUAI)

Abstract:
Spiking Neural Networks (SNNs) are the next-generation artificial neural network that better approximates the biological neurons. They are known for their faster processing and ultra-low power requirement on neuro-morphic hardware. Mimicking biological neurons, they communicate through spikes, replacing the popular continuous activation functions with the Heaviside function. Ad-hoc surrogate functions are popularly used in SNN training for back-propagation of loss through the Heaviside.

We establish a theoretical result that using the zeroth-order technique on the Heaviside functions on expectation is equivalent to using surrogate functions in back-propagation, providing a basis for using the latter. Further, the proposed local zeroth order technique lends itself to certain computational advantages and better generalization over the surrogates [NeurIPS'23].

Superior adversarial robustness properties of SNNs are reported in the recent literature when the inputs are rate-encoded, i.e., every pixel is encoded by a series of independent Bernoulli samples. By establishing a theoretical connection with randomized smoothing, we provide the first theoretical proof for the adversarial robustness of rate-encoded SNNs. Through this novel connection, we also improve the adversarial training of such a network [ICLR'24].

Speaker: Dr. Bhaskar Mukhoty is a postdoctoral research associate at the Mohamed bin Zayed University of Artificial Intelligence hosted by Dr. Bin Gu and Dr. Huan Xiong. He is a recipient of the Outstanding PhD Thesis Award from IITK in 2023. He obtained his Ph.D. in Machine Learning from the Department of CSE, IIT Kanpur, under the supervision of Dr. Purushottam Kar and Prof. Sandeep K. Shukla. He is interested in developing scalable Machine Learning / Deep Learning algorithms with theoretical guarantees on possibly corrupted training and test data. His research efforts have resulted in more than half a dozen publications at leading venues such as ICLR, NeurIPS, AAAI and others.