

Adversarial Security of Brain-Computer Interfaces

Professor Dongrui Wu 伍冬睿

Huazhong University of Science and Technology

Abstract

A brain-computer interface (BCI) enables direct communication between the brain and external devices. It can be used to research, enhance or repair human cognitive and sensory-motor functions. Electroencephalograms (EEGs) are frequently used in BCIs. However, EEG-based BCIs are subject to adversarial attacks, which are small perturbations that may be difficult to be detected by human eyes or computer algorithms, but can dramatically change the EEG decoding output and hence may hurt the user. Adversarial security is very important to the broad real-world applications of BCIs. This talk will introduce the implementation and defense against adversarial attacks to EEG-based BCIs.



Dongrui Wu (IEEE Fellow) received a B.E in Automatic Control from the University of Science and Technology of China, Hefei, China, in 2003, an M.Eng in Electrical and Computer Engineering from the National University of Singapore in 2006, and a PhD in Electrical Engineering from the University of Southern California, Los Angeles, CA, in 2009. He is now Chair Professor and Vice Dean of School of Artificial Intelligence and Automation, Huazhong University of Science and Technology, Wuhan, China. His research interests include brain-computer interface and machine learning. He has more than 200 publications (19000+ Google Scholar citations; h=72), with 7 outstanding paper awards from IEEE. His team won National Champion of the China Brain-Computer Interface Competition in seven successive years (2019-2025). He is the Editor-in-Chief of IEEE Transactions on Fuzzy Systems.