Security Against Adversarial Examples

Submitted by willirn1 on Fri, 06/07/2019 - 3:19pm. Contributor:
David Wagner

ABSTRACT
Recent research suggests that modern machine learning methods are fragile and easily attacked, which raises concerns about their use in security-critical settings. I will survey several attacks on machine learning and directions for making machine learning more robust against attack. I will also briefly mention my own research in this area.
BIO: David Wagner is Professor of Computer Science at the University of California at Berkeley, with expertise in the areas of computer security and electronic voting. He has published over 100 peer-reviewed papers in the scientific literature and has co-authored two books on encryption and computer security. His research has analyzed and contributed to the security of cellular networks, 802.11 wireless networks, electronic voting systems, and other widely deployed systems.

Other available formats:

Security Against Adversarial Examples
Switch to normal viewerSwitch to experimental viewer

Presentations Academia Presentation