129

Deep Learning-based approach for Device Authentication Using RF Fingerprinting: Identifying malicious transmitter

Radio Frequency (RF) fingerprinting is a new technology that can be used to authenticate advanced devices. This work looks into the feasibility of using different fundamental characteristics for RF fingerprinting. Our deep convolutional neural network architectures take raw and processed IQ samples as input to identify devices under various practical conditions, including changing channels, noise levels, training data sizes, and computational overheads. The contribution of the work are as follows (i) We provide a comprehensive performance evaluation of both a custom-designed and a modified pre-trained architecture, with insights on which one may be preferred under specific environmental conditions, (ii) We report sensitivity to number of devices, training set size, signal-to-noise ratio, and environmental channel. Training data are real-time transmissions from thousands of devices.