Your 598 ID: 5107

Title of paper: Audio Adversarial Examples: Targeted Attacks on Speech Attacks.

What is their primary result? The primary result of the paper is to demonstrate that the use of neural networks in audio recognition tasks is vulnerable to adversarial attacks; that is, attacks where the main objective of the attacker is to make the neural network classify an instance x similar to a natural instance y as any target t chosen by the attacker.

Why is this important?

What are their key ideas?

What are the limitations, either in performance or applicability?

What might be an interesting next step based on this work?

What's the architecture?

How did they train and evaluate it?

Did they implement something?

Grader's 598 ID: