Securing IoT and Edge Devices under Audio Adversarial Attacks

RUTGERS

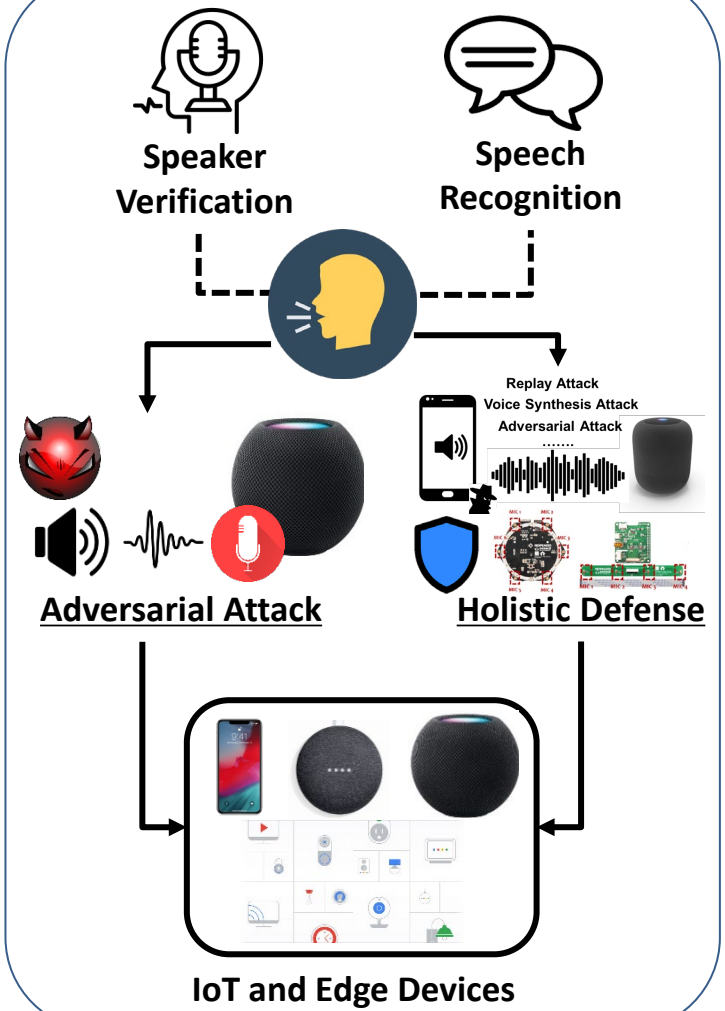
THE UNIVERSITY OF TENNESSEE KNOXVILLE

Challenge:

- Investigate audio adversarial attacks under practical conditions
- Achieve a holistic defense against various audio attacks
- Enable the defense to in new acoustic environments with low training cost

Solutions:

- Generate universal, synchronization-free, and target audio adversarial perturbations
- Build a holistic defense against adversarial attacks using multichannel audio
- Employ domain adaptation to enable environment-independent defense



Scientific Impact:

- Understand the nature of audio adversarial attacks in the physical world
- Build attack-resilient voice-controllable IoT and edge systems
- Develop a new computing paradigm in audio-based adversarial machine learning

Broader Impact and Broader Participation:

- Advance the foundation of audio adversarial attacks
- Involve curriculum design and K-12 students
- Facilitate emerging voice assistant systems

Yingying (Jennifer) Chen, Bo Yuan
Rutgers University, 2114220
Jian Liu
University of Tennessee at Knoxville, 2114161