Acoustic Side Channel Attacks on Robots

1. Background

In recent years, robot technology has gained increasing popularity, with its deployment in various use cases such as cleaning, patrolling, and monitoring. Unfortunately, this inevitably makes robots attractive targets for cyberattacks, enabling attackers to obtain information about the robot and its surroundings. Among the many attack vectors on robots, existing research has demonstrated that the acoustic channel is one of the most effective methods for extracting information. For example, a microphone placed next to a robot arm can record the robot's sound and predict the arm's position, while a cellphone placed next to a 3D printer can extract the printed objects by analyzing the printer nozzle's movement sounds. Therefore, it is crucial to comprehensively and systematically explore acoustic attacks to cover more scenarios and reveal the full security implications of acoustic attacks on robots.

2. Project Description

This project aims to explore acoustic channel attacks on cleaning and security robots. The primary goal is to train a machine learning model that can detect different types of robots based on their emitted sounds and extract their movement routes to understand their working environments. Specifically, the framework consists of three major components:

1. Robot Identification Model: A machine learning model that identifies the type and model of the robot based on its sound. This model is trained to recognize distinct acoustic signatures produced by different robots, enabling accurate identification.

2. Robot Movement Identification: A machine learning model that identifies the movement of the robot based on its sound. This model is trained to detect and classify different movements, such as moving forward, moving backward, rotating left, and rotating right, by analyzing the acoustic features associated with each movement.

3. Visual Representation: An OpenCV or OpenGL-based software to plot the robot's movement based on the movement predictions. This component serves as a visual representation of the prediction model, allowing people to see the robot's movements and routes in a graphical format for better understanding and analysis.

2.1. Project Goals

1. Implement a Machine Learning-Based Acoustic Attack on Robots

2. Demonstrate Adversaries' Ability to Retrieve Robot Movement and Path Based on ML Detection

3. Demonstrate Adversaries' Ability to Retrieve the Floor Plan of the Environment Based on Robot Movement

4. Provide Full Documentation of the ML Model and Guidance for the Visual Representation Software

2.2. Other Requirements

1. Students should compile a list of necessary computational hardware for training and testing machine learning models.

2. The movement detection model should be capable of running on standard laptops with limited computing power. While it is preferable for the model to run on mobile platforms as well, this is not a requirement.

3. All components must be capable of functioning without an Internet connection.

4. Propose potential mitigation methods to defend against this vulnerability.

2.3. Ethical Requirement

All participating students must consent to an ethical agreement stating that concepts, knowledge, or skills acquired from this project will not be used in any harmful way in real-world scenarios.

3. **Desired Skill Set**
    1. Basic Programming Skills
    2. Familiar with different types of ML modeling (ANN, CNN)
    3. Taking/Taken related courses in cybersecurity and robotics is a plus
    4. 5. Familiar with oepnCV and/or openGL is a plus
4. **Preferred Team Size: 3-5 students**
5. **Location of Work: Mines Campus**
6. **Client Liaison: Guannan Liu (guannan.liu@mines.edu)**