WiSpider

Team C2: Thomas Horton King, Ethan Oh, Anish Singhani
18-500 Capstone Design, Spring 2023
Electrical and Computer Engineering Department, Carnegie Mellon University

Carnegie Mellon University

Pitch: Finding Covert Wireless Devices

- There has been massive growth in the number of wireless IoT devices in the past 20 years
- Hidden or concealed off-the-shelf devices can easily infringe on an individual's privacy
- Users need a way to non-cooperatively find these devices

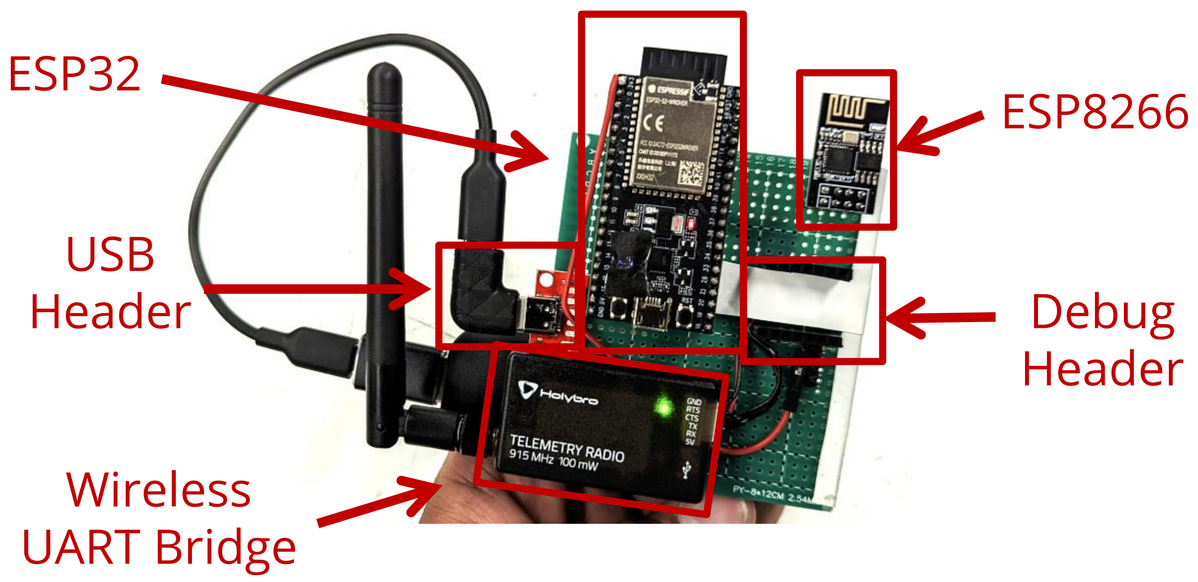
- We developed **WiSpider**, a product that **finds** Wi-Fi devices and **localizes them with a median of 0.8m accuracy** with a total of **40m range**
- Crucially, WiSpider can operate **even if the devices are not connected to the same network**
- WiSpider visualizes the results on a **GUI** and **an AR app**, allowing the user to find the devices in the environment

Target Devices

Architecture: Time-of-Flight sensing with ACK Exploit

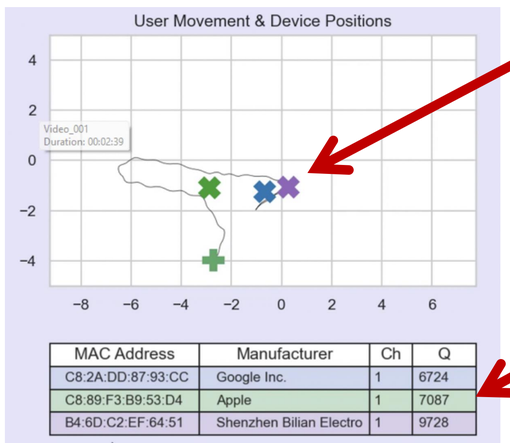
- Can send **fake attack packets** which devices respond to even if the transmitting device is unprivileged
- **Measure the time** between transmitting and receiving the spoofed packets
- Combine camera self-localization as the user moves

Hardware Diagram

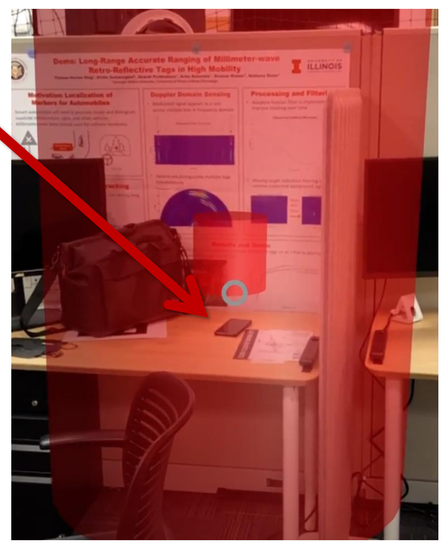


Software Diagram

Computer GUI

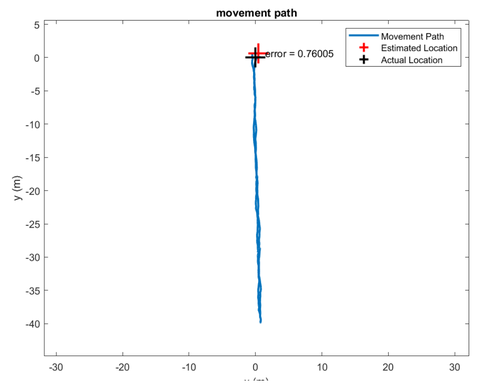


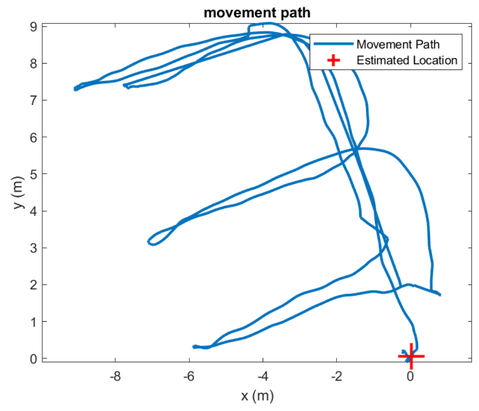
AR Interface



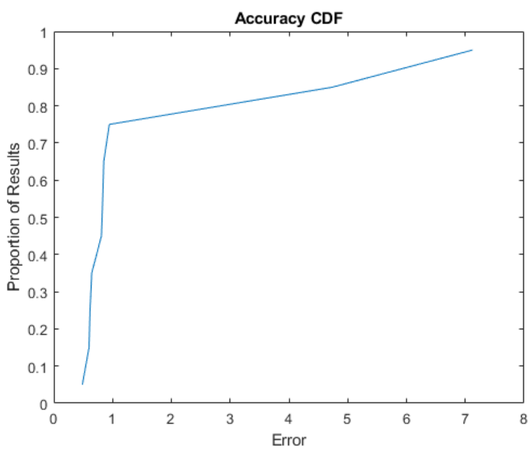
System Evaluation

- Move across an entire room for 3 minutes and collect data for 5 minutes, and verify localization accuracy at the end of the trace.





- We achieve an **overall median accuracy of 0.8m**
- We verify resolution with targets **within 0.2m**
- Total Cost: **$143.60**
- Detection Range: **40m**
- Detection Rate: **90%**



Acknowledgements

We would like to thank the works before us that made our project possible: Polite Wi-Fi (2020), ARENA (2021), Wi-Peep (2002), and Lumos (2022)

Thank you to Professor Hyung Kim and Omkar Savkur for their feedback and guidance