Midterm Report

Yaying Ye, Yueyang Sun

Current Progress

We have read paper about Z-wave protocol and its security analysis. We find that most of the Z-wave device are poorly encrypted and should be easy to understand after some research. We also have reference on some Z-wave demodulation example online and try to understand the algorithm to replicate its function. We're using GNU Radio to connect with the SDR to validate whether we're able to pick up any Z-wave signal.

We're currently working on setting up the LimeSDR on Ubuntu. The PCs we have are Mac pro and Chromebook. Since installing virtual box on Mac has serious delay on action, we choose to install Ubuntu on Chromebook and it works fine. We try to install transceiver Firmware and FPGA image on LimeSDR and LimeSuite, a GUI for LimeSDR to gain insight of the received signal. However, the firmware version and FPGA gateway always mismatch while device detecting. We try to search for solution on LimeSDR forum but we could not find a way to solve it. The solution we propose is to switch to RTL-SDR, a cheaper SDR but only with receiver. We also install RTL-SDR package on Ubuntu and run GNU Radio to pick up the Z-wave signal. We're able to observe the FFT Z-Wave with center frequency of 908.42MHz. We think switching to RTL-SDR would be more practical to our project.

Next Step

1. Demodulate and decode the received Z-wave signal
2. Analyze the Z-wave instruction and identify each part of the instruction
3. Read the targeted Z-wave sensor datasheet and understand its functionality
4. Monitor the activity of the Z-wave sensors for a period
5. Build model for detection of Z-wave sensor of an unknown home setting
6. Investigate experimental data and propose future work