EE209AS Project Proposal

Background

Z-Wave is a wireless communication protocol using radio frequency ranging from 800 MHz to 900 MHz. Even though ZWave is a fairly new communication protocol developed at 2001 by a Danish company called Zensys, popularity of using Z-Wave device has increased every year. Therefore, security of using Z-Wave communication protocol has become an essential thing to be evaluated. Under most cases, ZWave are used for home automation devices such as door/Window sensors, locker sensors etc. ZWave operates at various frequency under different countries' regulation. Particularly, it operates at 868.42MHz in Europe and 908.42MHz in the US. Z-Wave has three types of data rate at 9.6 kbits/s, 40 kbits/s and 100 kbits/s, where 9.6 kbits/s are for older version chips. Correspond to each different data rate, there are two types of encoding channel. 9.6 kbits/s need to use Manchester encoding channel and NRZ encoding channel is for 40 kbits/s and 100 kbits/s.

Each Z-Wave network can have up to 232 nodes where only one node can be the primary controller. The process of adding new nodes to the system is called inclusion, and exclusion means remove current node from the network. Maximum communication distance between two nodes is roughly 30 meters. Primary controller holds a 4 bytes Device ID which will be shared to nodes connected under the same Z-Wave network. Every node in the same network will also maintain a 8 bits Node ID. All these ID information can be located in the MAC layer frame where PHY layer Frame contains necessary preamble, start of frame and end of frame information. Detailed data information including command type, command, and values is stored in the Application layer frame. In addition, signal transform type is defined by Frame Control value from MAC layer, which includes singlecast, ACK, multicast, and broadcast frame types.

Objective

For evaluating purposes, our goal is to sniff Z-Wave signals between Z-Wave devices by using SDR and demodulate received signal on PC. According to datasheet of different type of sensors, we are going to interpret received signal numbers into meaningful information.

Device and Software

Z-Wave devices we plan to use are home security sensors like motion sensors, illumination sensors, etc. A hub that can be used as the primary controller in the Z-Wave network.
Devices we choose to receive Z-Wave signal is Limesdr or RTL-SDR. Depending on hardware configuration situation, we will decide which SDR device to use after thoroughly evaluation. In addition, if we choose to use RTL-SDR, we will need a separate antenna connected to receive better signal.

Time Schedule

Time	Objective
Week 4	Read Z-Wave related paper
Week 5 and Week 6	Configure devices
Week 7	Demodulate signals and collect raw data
Week 8	Collect and understand data
Week 9	Interpret data to human activities
Week 10	Analyze collected information and discussion
Week 11	Report and presentation preparation

Reference

[1] http://www.rfwireless-world.com/Tutorials/z-wave-protocol-stack.html
[2] http://zwavepublic.com/sites/default/files/command_class_specs_2017A/SDS13781-5%20Z-Wave%20Application%20Command%20Class%20Specification.pdf
[3] https://pdfs.semanticscholar.org/10e1/21b903366ea81b94ca0c2e61c095cc087695.pdf
[4] *Series G: Transmission Systems and Media, Digital Systems and Networks,G.9959.(2015.01).*