Midterm Project Report
02/15/2018

Methods and Procedures

The Proxmark3 is used under Windows 8.1/10 environment;
Utilized Proxmark3 low frequency related commands to capture, save, plot, send and simulate data from the car door;
After analysing and trying possible methods of transmitting data between laptops, we decided to use one-to-one Wi-Fi network: one laptop create a Wi-Fi hotspot and the other laptop join this network so that they can share files in the public folder.

Work Completed

Learned the usage of Proxmark3 and completed the tool setup;
The “lf snoop” of Proxmark3 cannot work normally due to the bugs in it. We upgraded the firmware of Proxmark3 and fixed the “lf snoop” command;
In order to meet the time constraint of the keyless entry system, we wrote batch files to execute all the commands at one time:
One batch file (auto_get.bat) is used by one SDR to capture signal from the car door and then send. Related Proxmark3 commands are in get.txt.
Another batch file (auto_send.bat) is used to send the signal data that saved in the laptop to the other SDR so that it can simulate the LF tag from buffer. Related Proxmark3 commands are in send.txt.
Used the SDR to capture the 125 kHz signal from the car door and successfully got the data from a Toyota car (toyota.txt);

Work Planned for Next Step

Transmit and replay the signal, verify if the time constraint met;
Test the final product on different cars, compare results;
Modification and improvement on the method.