Secure Systems & Network Engineering

Advanced Security

Lab 2 Software Defined Radio

Grebennikov Sergey, Polovinkin Andrey, Radostev Ilia

January 23, 2018

433MHz protocol analyzer
433 MHz devices can be received by the SDR.

Problem

System setup

Our task was to sniff and analyze signal from 433MHz device. After that it is possible to perform replay attack. Unfortunately, we were not provided any kind of such a device, so we decided to deploy our own system.

- Raspberry Pi 3 - serves as a gateway controller (smart home controller)
- Arduino Uno - Sniffer
- Arduino Nano - Receiver (smart table lamp)

For smart home emulation we used open source project iot-433mhz. It allows control of IoT devices using Arduino. Using our deployed system we were able to control our smart lamp sending 433MHz signal which was also detected by GQRX tool. Finally, the signal was also captured by our sniffer and was successfully replayed to control smart lamp.

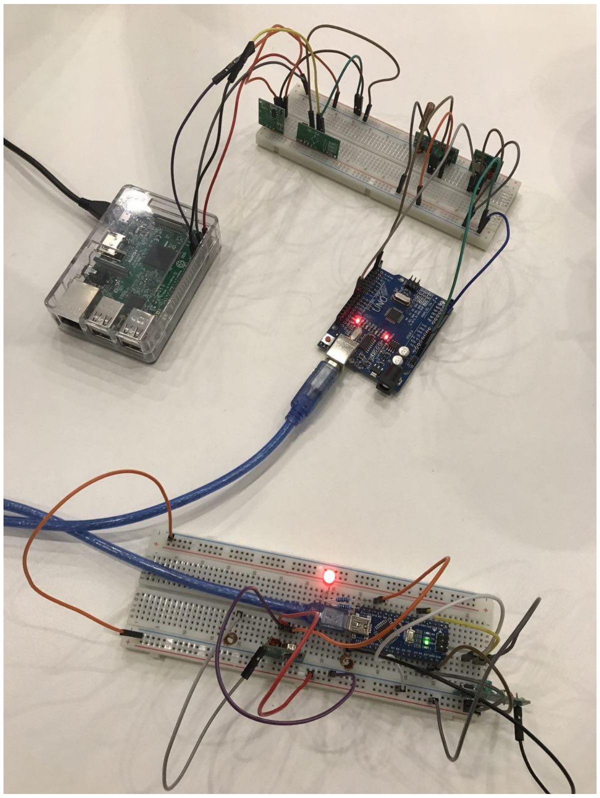

Figure 1: Smart system setup

Analyze protocol

The captured turn-on signal is shown below (raw data)

```
11004,292,1156,288,1124,312,1132,264,1132,304,1104,316,1104,320,
1116,320,1108,312,1116,312,1116,356,1060,356,1072,416,1004,388,
1032,388,1080,344,1056,1076,332,1072,344,1068,352,1112,316,1080,
348,1100,368,340,1100,352,1100
```

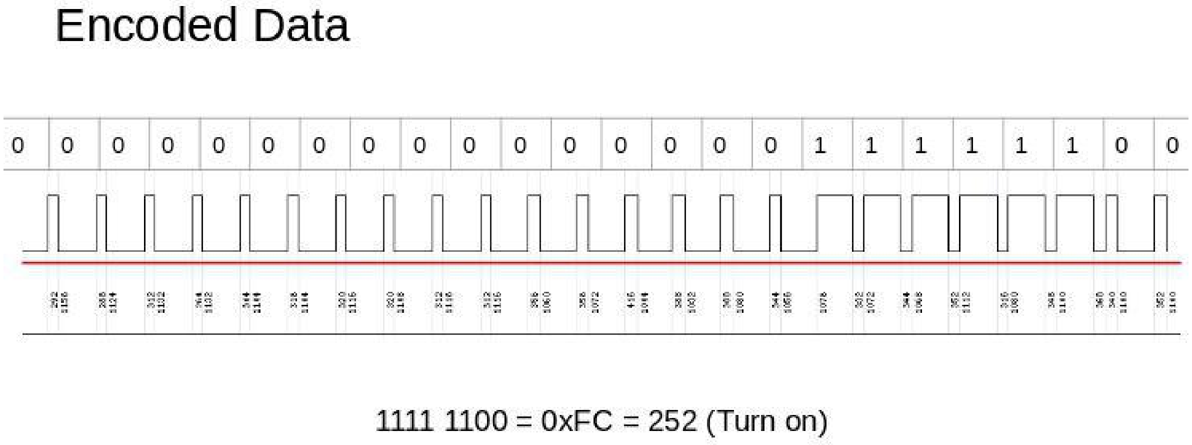

Figure 2: Manchester encoded signal

The same signal, converted to Manchester encoding, IEEE 802.3 is show below

Final value is 252 which was used for turning the lamp on. Similarly, it works for turn-off signal (decimal value 254).

Question 1

Can you retrieve the secret code that is being transmitted?

Answer Yes. 433 MHz has no pairing. When a signal is sent, the transmitter broadcast the signal on 433MHz frequency and anyone who has a receiver that works on 433MHz frequency can get the same signal.

Question 2

Is there any logic added to the signal?

Answer The data is transmitted over longer distances along with supporting weaker signals. In addition, it also increases the noise level and complicates detecting the beginning of a message. To compensate this effect the messages are usually prefixed by a static header. Also, if the original proprietary receiver supports multiple senders at the same time, the protocol needs to be capable of distinguishing sensors using an ID. To ensure the data is received correctly it is used checksums (CRCs).

In addition to the fields mentioned above proprietary RF 433 MHz protocols eventually contain more data:

- Sensor type
- Payload length
- Sensor status
- Battery information
- Message id

Question 3

Can you find other devices?

Answer Yes, we can. We can identify devices that broadcast into air such as IoT sensors and detectors.

Results

- 433 MHz protocol does not provide security
- All security mechanism should be implemented on the application layer