Report Date: 10/14/2022
To: ematson@purdue.edu, ahsmith@purdue.edu, lee3450@purdue.edu
From: 454P

- Seokhyeon Bang (kzrt0123@cau.ac.kr)
- Junyoung Jang (junjang99@cau.ac.kr)
- Yuseon Choi (181133@jnu.ac.kr)
- Minju Ro (romj98@cau.ac.kr)
- Doyong Kwon (doyong365@knu.ac.kr)

Summary

The main objective of this week was to learn how to use HackRF One device and to find a plausible method of hacking that can be applied to LoRaWAN. At first, the team members discussed about LoRaWAN hacking plan. Several known methods for hacking wireless networks were found during the research. WiFi jamming was conducted to test HackRF and verify whether jamming is appropriate for LoRaWAN hacking. Also writing the research paper was conducted, especially the literature ew. Pre-works were reviewed and summarized to write paper.

What 454P completed this week:

- Learn HackRF to receive the packet of the LoRaWAN and conducting jamming.

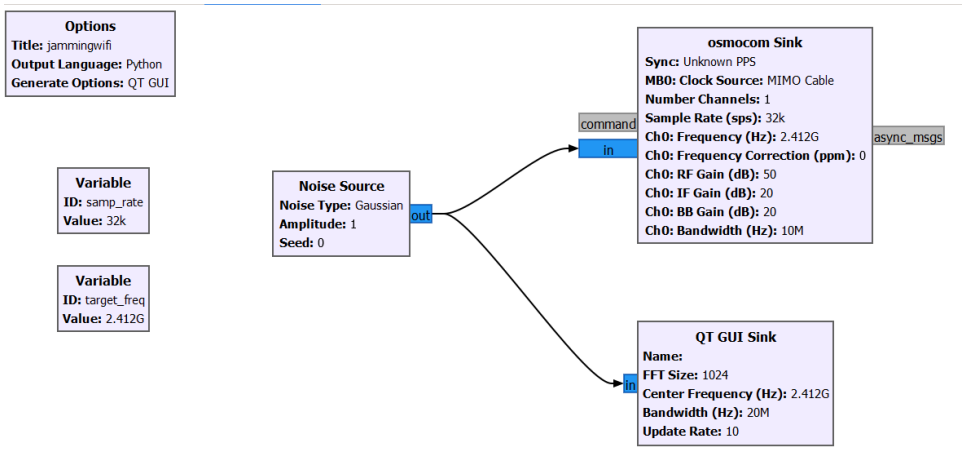

Fig. 1. Flowgraph of WiFi jamming

There were official videos[1] and documents[2] which *greatscottgadgets* offered. Learning how to use hackRF was conducted with these references.

Trying known methods of hacking wireless networks definitely helped the team to understand the concept of network hacking. For this reason, jamming WiFi was conducted [3]. GNU radio[4] was used to control the hackRF device. Microsoft Window 11 was used as the OS. Experimental Hotspot WiFi frequency was 2.4GHz with channel 1 which is 2.412GHz. The frequency was determined with a WiFi analyzer program [5]. Making gaussian noise with 20MHz bandwidth jamming WiFi successfully jammed the wireless signal which causing the client device to get disconnected [6].

- Learn Scapy to analyze the packet.

Scapy is a packet manipulation program. Scapy is an appropriate tool for analyzing packets and crafting network packets. There were several videos[7] in Youtube which were tutorials to sniff the packet of the TCP/IP. However, there were no videos of sniffing the packet of the LoRaWAN. Instead, there was a guide page[8] which has several commands that can be used to analyze network packets.

- Set up the Dragino gateway.

  To make an environment that is similar to the actual implementation, and also to test with different kind of devices, installation of a basic station[9] rather than a packet forwarder[10] was tested using Dragino LSP8N[11]. The gateway was connected to the switch and the local LoRaWAN network. For gateway to be a basic station, websocket server[12], which in real life situation it must be a cloud server[13], should be opened on network and application server. To make that work, by using mosquitto[14], network and application server opened new port as websocket on 3001[15] to allow connection through that port. By doing so, the connection between gateway and servers were established. However, only connection was opened, and still LoRa packets from gateway nor the server were sent to each other. So, research about what cloud LNS(LoRaWAN Network Service)[16] actually do was attempted.

- Complete literature review

  Abstract and Introduction were revised according to the feedbacks our group received. References for writing literature review were specified. Literate review was completed and submitted to TA for feedback.

Things to do by next week

- Jamming multi-channel LoRaWAN
- Setting up Dragino gateway as a gateway
- Figuring out appropriate hacking methods which is attempted to other wireless networks
- Preparing for midterm presentation
- Revisioning paper
- Investigating how cloud LNS works

Problems or challenges:

Jamming the WiFi was hard because the WiFi had to be in an identifiable frequency channel. It needed an extra program to listen to radio signals and to analyze their own frequencies. There was a problem with jamming multi-channel. However, progressed modern wireless networks as LoRaWAN use multi channels, so there is need to figure out the way sending multiple signals at once.

There were several trials to use Scapy commands to analyze a packet, however it was not working. It would be a challenge because there were no explain or examples of the commands.

References

[1] *Great scott gadgets*. [Online]. Available: https://greatscottgadgets.com/sdr/. [Accessed: 14-Oct-2022]

[2] "Welcome to hackrf's documentation!¶," *Welcome to HackRF's documentation! - HackRF documentation*. [Online]. Available: https://hackrf.readthedocs.io/en/latest/index.html. [Accessed: 14-Oct-2022]

[3] A. Sârbu and D. Neagoie, "Wi-Fi jamming using software defined radio," *International conference KNOWLEDGE-BASED ORGANIZATION*, 01-Jun-2020. [Online]. Available: https://doi.org/10.2478/kbo-2020-0132. [Accessed: 14-Oct-2022]

[4] "The Free & Open Source Radio Ecosystem · Gnu Radio," *GNU Radio*. [Online]. Available: https://www.gnuradio.org/. [Accessed: 14-Oct-2022]

[5] “Get $WIFI analyzer and scanner from the Microsoft Store,” *Microsoft Apps*. [Online]. Available: https://apps.microsoft.com/store/detail/wifi-analyzer-and-scanner/9NBLGGH5QK8Q?hl=en-us&gl=us. [Accessed: 14-Oct-2022]
[6] timkim0713, “TIMKIM0713/RFJamming-FMRadio-SDR,” *GitHub*. [Online]. Available: https://github.com/timkim0713/RFJamming-FMRadio-SDR. [Accessed: 14-Oct-2022]
[7] YouTube, 2020 [Online]. Available: https://www.youtube.com/watch?v=EuTAmtMGdNU. [Accessed: 14-Oct-2022]
[8] “Scapy.contrib.loraphy2wan,” *scapy.contrib.loraphy2wan - Scapy 2.5.0 documentation*. [Online]. Available: https://scapy.readthedocs.io/en/latest/api/scapy.contrib.loraphy2wan.html. [Accessed: 14-Oct-2022]
[9] “Gateways,” *The Things Network*. [Online]. Available: https://www.thethingsnetwork.org/docs/gateways/. [Accessed: 14-Oct-2022]
[10] “Packet forwarders,” *The Things Network*. [Online]. Available: https://www.thethingsnetwork.org/docs/gateways/packet-forwarder/. [Accessed: 14-Oct-2022]
[11] “LPS8N Indoor lorawan gateway,” *Dragino*. [Online]. Available: https://www.dragino.com/products/lora-lorawan-gateway/item/200-lps8n.html. [Accessed: 14-Oct-2022]
[12] “The Websocket API (WebSockets) - web apis: MDN,” *Web APIs | MDN*. [Online]. Available: https://developer.mozilla.org/en-US/docs/Web/API/WebSockets_API. [Accessed: 14-Oct-2022]
[13] “Semtech Lora Cloud,” *Semtech LoRa Cloud*. [Online]. Available: https://www.loracloud.com/. [Accessed: 14-Oct-2022]
[14] “Eclipse mosquitto,” *Eclipse Mosquitto*, 08-Jan-2018. [Online]. Available: https://mosquitto.org/. [Accessed: 14-Oct-2022]
[15] “Documentation,” *Eclipse Mosquitto*, 06-Jul-2020. [Online]. Available: https://mosquitto.org/documentation/. [Accessed: 14-Oct-2022]
[16] “Lorawan network server,” *LoRa Alliance®*, 25-Nov-2020. [Online]. Available: https://lora-alliance.org/lora_products/lorawan-network-server/. [Accessed: 14-Oct-2022]