Report Date: 10/28/2022
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

LoRaWAN Network was deployed with the RAK as a basic station. Since the main objective of this week was to design a hacking scenario and try jamming and packet sniffing with SDR device. Jamming the LoRaWAN using HackRF, USRP-B200 and Canopy was the first thing that could be tried. HackRF and SDR can make a radio frequency (902MHz~928MHz) to conduct jamming with GNU Radio. This jamming radio frequency was detected by spectrum analyzer.

What 454P completed this week:

- Set up Local LoRaWAN as basic station

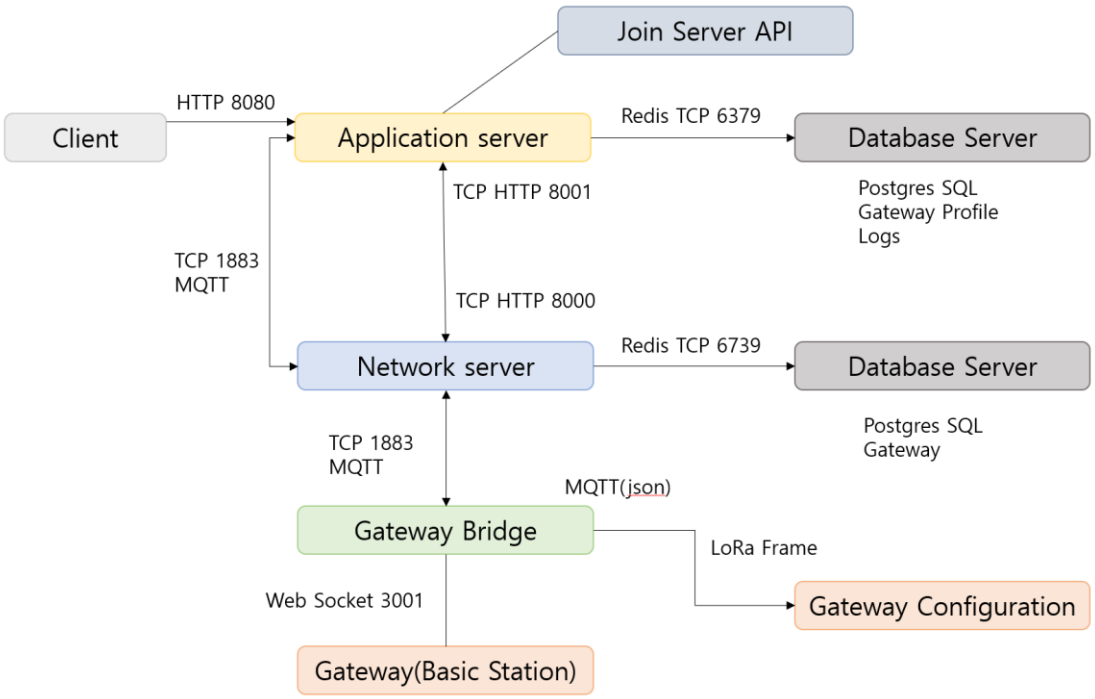

Fig. 1. Diagram of local LoRaWAN

To design a local LoRaWAN, join server is needed to run in a local environment. For other cloud base LoRaWAN services, join server is provided as a cloud's websocket server[1], which should be avoided for the local setup. Thus, using join server Application Programming Interface (API)[2] from ChirpStack and a direct connection of websocket of gateway bridge to own redis server of application server is established via MQTT. Using PostgreSQL[3] and a redis server[4], from 3001 port of gateway bridge, end devices can be queried into join server, which ends up with join accept message sending down to the gateway or just a failure that does not do anything. Thus, local LoRaWAN with basic station as a backend is accomplished as Fig. 1 shows.

- Conduct jamming with HackRF, USRP-B200 and Canopy

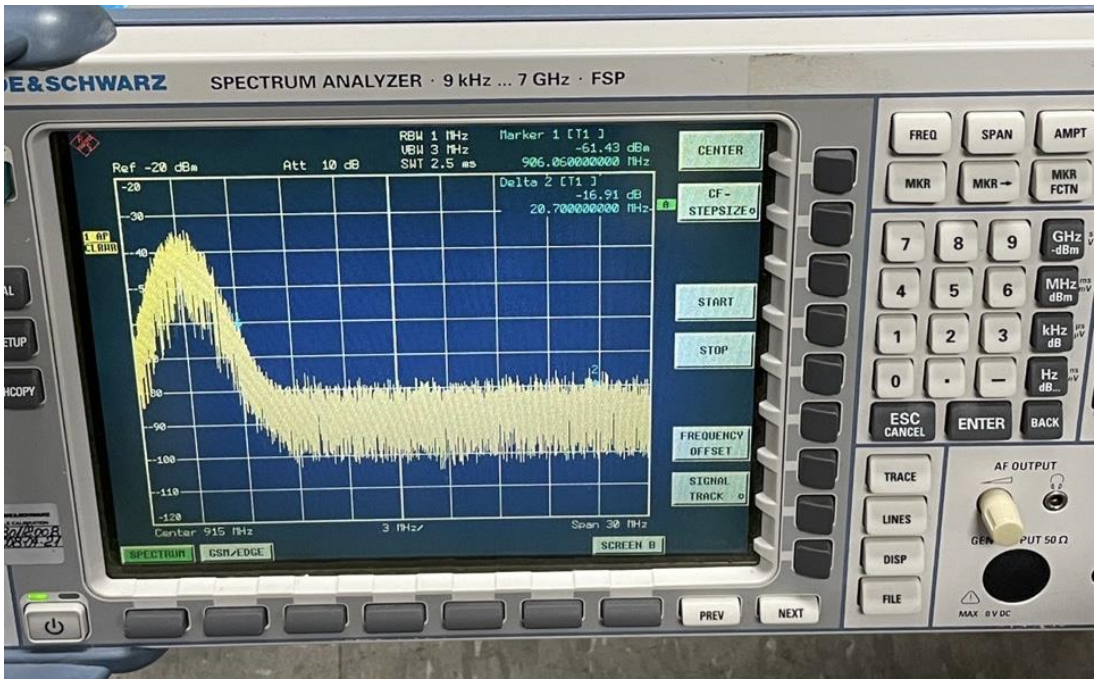

Fig. 2. Result of jamming using HackRF on spectrum analyzer

After discussing the way of approaching the hacking the LoRaWAN, the conclusion was conducting the jamming is the first to try. It could be done easily than any other method because jamming is the physical layer hacking method. There were two Software Defined Radio (SDR) which are HackRF[5] and USRP-B200[6] that can generate radio frequency to conduct jamming. However, both devices could not generate sufficient amplitude to conduct jamming successfully, which is shown at Fig. 2, therefore, amplifier would be required to jam with SDRs. However, Motorola Canopy devices[7] are introduced as that can make a big amplitude radio frequency. Canopy could interfere with the LoRa network communication, and with a single set of Canopy devices with 906.1Mhz setting for radio frequency, these devices can jam from 902Mhz to 914Mhz, which is a LoRaWAN network's frequency domain. The lack of power to jam in 915Mhz and further up can be solved by using another new Canopy.

- Conduct packet sniffing

The second method was packet sniffing with HackRF. Packet sniffing can be done using HackRF as a listener and translating the digital radio signal into LoRa packets. The translation is processed using gr-lora[8] which change analog Chirp Spread Spectrum (CSS)[9] signals to digital and LoRa_Craft[10] which consumes up that digital signal into LoRa packets by uploading that digital signal to Scapy[11] by UDP port.

Things to do by next week

- Set up several Canopy devices to conduct jamming
- Find a precise jamming boundary that can be done successfully jamming by Canopy.
- Optimize the number of Canopy devices needed to complete jamming.
- Using HackRF as a multichannel listening device.
- Replay attack using HackRF and GNU radio.

Problems or challenges:

Generating big size radio frequencies is illegal in the US. Because of this reason, every SDR device's

power is not sufficient to succeed in jamming.

Discussing this problem with prof. Smith, Canopy could make sufficient radio frequencies. After figuring out this device and connecting the appropriate antenna, huge size of radio frequencies are detected in spectrum analyzer.

References

[1] Brocaar, “Chirpstack-api”, *GitHub.* [Online]. Available: https://github.com/brocaar/chirpstack-api [Accessed: 24-Oct-2022]

[2] The Things Stack, “The Things Join Server.”, *www.thethingsindustries.com,* https://www.thethingsindustries.com/docs/getting-started/cloud-hosted/tti-join-server/ (accessed Oct. 24, 2022).

[3] PostgreSQL, “What is PostgreSQL?.”, *www.postgresql.org*, https://www.postgresql.org/ (accessed Oct. 25, 2022).

[4] Redis, “Introduction to Redis.”, *https://redis.io/,* https://redis.io/ (accessed Oct. 24, 2022).

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

[6] Ettus Research, “USRP Hardware Driver and USRP Manual.”, *files.ettus.com,* https://files.ettus.com/manual/page_usrp_b200.html (accessed Oct. 25, 2022).

[7] manualslib, “Canopy 900 MHz Subscriber Module User manual.”, *www.manualslib.com,* https://www.manualslib.com/manual/449781/Motorola-9000sm-Canopy-900-Mhz-Subscriber-Module.html (accessed Oct. 25, 2022).

[8] Rpp0, “Gr LoRa”, *GitHub.* [Online]. Available: https://github.com/rpp0/gr-lora [Accessed: 26-Oct2022]

[9] B. Reynders and S. Pollin, "Chirp spread spectrum as a modulation technique for long range communication," 2016 Symposium on Communications and Vehicular Technologies (SCVT), 2016, pp. 1-5, doi: 10.1109/SCVT.2016.7797659.

[10] PentHertz, “LoRa Craft.”, *GitHub.* [Online]. Available: https://github.com/PentHertz/LoRa_Craft [Accessed: 26-Oct-2022]

[11] Scapy, “Build your own tools.”, *scapy.readthedocs.io,* https://scapy.readthedocs.io/en/latest/extending.html (accessed Oct. 26, 2022).