Report Date: 10/21/2022
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 switch the packet forwarder to the basic station. Unlike the packet forwarder, the basic station needs the certification of a node device. It caused the necessity of the "join server process. Team members discussed the hacking plan last week. The first step was jamming. Team members learned how to utilize the R&S®FSP spectrum analyzer with the hacking plan. Based on the feedback received at the meeting with the TA on Monday, team members revised the paper architecture and corrected the format error. The materials were prepared for the next week midterm presentation.

What 454P completed this week:

- Learn how to use GNU Radio

  GNU Radio is a program that can control SDR(Software Defined Radio) [1], [2]. To utilize GNU Radio Osmosdr [3], LoRa connection [4], [5], Scapy [6], and HackRF [7] configuration problems were solved [8]. Team members learned how to use GNU Radio for batching the signal of the LoRaWAN packet forwarder and jamming LoRaWAN signals. Tests were conducted to analyze the spectrum in specific frequency bands, including 902.3MHz, 914.2MHz, and 927.5 MHz. However, these frequency bands did not work. The key reason was that the tests were conducted in a single channel while LoRa has multiple channels. Whenever LoRa sends a packet, it sends a packet through a different channel. For this reason, utilizing multi-channel was mandatory for the following tasks. Therefore, researching and applying various methods for multi-channel are planned.

- Configure the RAK as a basic station

  Last week, configuring the packet forwarder was conducted. However, the basic station is widely utilized in the real life. Team members decided to connect the RAK as a basic station [9]. Building the network as a basic station was completed. However, the joining process had a problem. The node device was not enrolled to either server or gateway and the uplink was not processed.

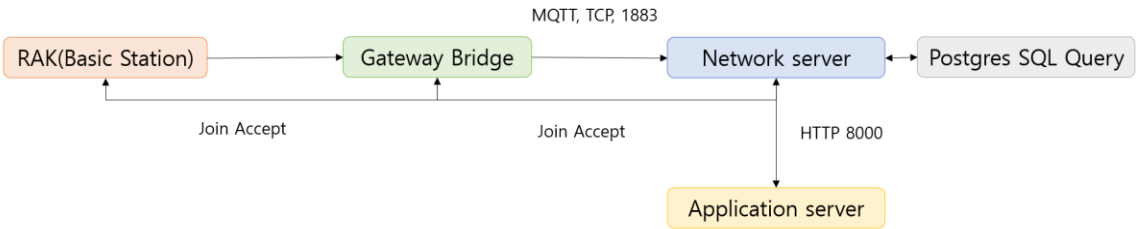

Fig. 1. Flowgraph of local LoRaWAN

- Learn how to use R&S®FSP spectrum analyzer

  Using the official manual [10], team members learned about each function of the device and considered how to apply it. The machine was capable of analyzing signals like frequency, bandwidth, amplitude, and so on. Utilizing this analyzer and canopy, which is a kind of transmitter, more fine analysis and jamming wider area was enabled.

Things to do by next week

- Preparing for mid-term presentation
- Specifying the hacking scenario and methodology
- Analyzing the difference between the join server of LoRaWAN and the program associated with PostgreSQL

Problems or challenges:

The SX1301/0 did not support ChirpStack. The network server and the application server were built on ChirpStack. For this reason, 1301/0 cannot be used for the project.

Rak is configured as a basic station this week. However, sending data through uplink and downlink was not processed properly. The join request message was refused repeatedly since there was no join server to process data. Making new join server or using PostgreSQL to make query for join requests were planned.

References

[1] Ryanvolz, "Radioconda", *GitHub*. [Online]. Available: https://github.com/ryanvolz/radioconda#hackrf [Accessed: 17-Oct-2022]
[2] Gnuradio, "Gnuradio", GitHub. [Online]. Available: https://github.com/gnuradio/gnuradio/ [Accessed: 17-Oct-2022]
[3] Osmocom, "Gr osmosdr", GitHub. [Online]. Available: https://github.com/osmocom/gr-osmosdr [Accessed: 17-Oct-2022]
[4] PentHertz, "LoRa Craft", GitHub. [Online]. Available: https://github.com/PentHertz/LoRa_Craft [Accessed: 17-Oct-2022]
[5] Rpp0, "Gr LoRa", GitHub. [Online]. Available: https://github.com/rpp0/gr-lora [Accessed: 17-Oct-2022]
[6] Scapy, "Build your own tools.", scapy.readthedocs.io, https://scapy.readthedocs.io/en/latest/extending.html (accessed Oct. 17, 2022).
[7] HackRF, "HackRF Compatible Software.", hackrf.readthedocs.io, https://hackrf.readthedocs.io/en/latest/software_support.html (accessed Oct. 18, 2022).
[8] Bistromath, "Gr air modes", GitHub. [Online]. Available: https://github.com/bistromath/gr-air-modes [Accessed: 17-Oct-2022]
[9] RAK, "RAK7249 WisGate Edge Max.", docs.rakwireless.com, https://docs.rakwireless.com/Product-Categories/WisGate/RAK7249/Overview/#product-description (accessed Oct. 17, 2022).
[10] Rohde & Schwarz, "R&S® FSP Spectrum Analyzer Quick Start Guide", *www.rohde-schwarz.com*, https://www.rohde-schwarz.com/us/manual/r-s-fsp-quick-start-guide-manuals-gb1_78701-28742.html (accessed Oct. 19, 2022).