Report Date: 11/04/2022
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 goal of this week was to determine the direction of the project. At the beginning of this week, studying multi-channel packet sniffing on LoRaWAN and checking whether it is possible through hackRF was conducted. This is because if multi-channel sniffing is possible, a replay attack could be attempted. However, it was important to start the experiment with a more certain topic for the paper. Team members decided to proceed with the experiment with the jamming attack first. Accordingly, the necessary research was conducted, and the structure and the direction of the paper were changed. In addition, the design of experiments for jamming attack was decided and configuration for the outdoor experiments were proceeded.

What 454P completed this week:

- Learn how to sniff multi-channel packets of LoRaWAN through hackRF
  Using gqrx[1] and GNU-Radio[2], as well as hackRF[3], researching and deploying a set up for multi-channel sniffing was conducted. Using gqrx, the team can now receive the LoRaWAN's data in multi-channel. However, because of the lack of references about translating the RF signal that uses Chirp-Spread-Spectrum (CSS)[4] to bytes, works to connect gqrx into gr-lora[5] still remained.

- Use hackRF as a LoRaWAN frame transmitter

  As gr-lora[5] only supports receiving data and translating the data to bytes, changing gr-lora into gr-lora_sdr[6] was conducted as gr-lora_sdr supports RX/TX transmissions, thus sniffing and sending packet could be conducted.

- Design the experiments for jamming attack on LoRaWAN

  A total of three experiments, outdoor, indoor, and general, were planned. The indoor experiment was designed to find out whether the jamming attack is possible in a building despite obstacles such as walls and doors. The outdoor experiment was designed to determine the range of jamming attacks by measuring distances on the farm. Lastly, the general experiment will be jamming next to the gateway. The detail information about the experimental setting and design will be written in the paper.

- Set up the devices for experiments

  For the experiments that reflect real life, LoRaWAN testers like MTDOT-Box[7] were not suited for the purpose since the testers' power of transmitting the data is too strong compared to actual

LoRa sensor devices. Thus, the usage of ESP32[8] had been arisen. ESP32's LoRa chip is used in many LoRa sensors and has a lot less power to transmit the data, so jamming transmission of these devices are not only much easier but also makes the experiments more based on reality. As ESP32 uses Arduino[9] code to run, by using team Coyote (IoT)'s code that transmits a packet every 5 seconds, the team successfully set up the ESP32 as a packet transmission tester.

- Changing local LoRaWAN settings into The Things Network[10]
  To reflect a real-life environment, changing local LoRaWAN into cloud server LoRaWAN was needed. With the experience of configuring local LoRaWAN, connecting RAK gateway[10] into The Things Network has been conducted, therefore managing the LoRaWAN in the remote distance can be easily done by signing into the cloud server

- Research on experiments of LoRaWAN and jamming attacks

  Since the subject of the project was decided, it is necessary to slightly modify the introduction and abstract written before the midterm. Researching and organizing the prior studies [12], [13], [14] on experiments of LoRaWAN and jamming attacks were conducted to write the sections of methods and experiments.

Things to do by next week

- Design the details of experiments
- Conduct outdoor demo experiments of jamming attack at KNOY.
- Make the draft of experiment section of the paper
- Make the code that measures Packet Delivery Rate (PDR)[13] for ESP32[8]
- Automate The Things Network[10] for calculating PDR

Problems or challenges:

While trying to set up an experiment environment, several problem statements havebeen been raised, such as which distance we would be modifying between canopies and sensors, or what methods would be used to calcthu elate the effect of jamming, et cetera. Our challenge for next week is to ensure our methods of outdoor experiments, as well as set up indoor experiments and environmental conditions to control.

References

[1] Gqrx SDR, "Welcome to gqrx.", *gqrx.dk*, https://gqrx.dk/ (accessed Nov. 4, 2022).
[2] GNURadio, "Usage Manual". *gnuradio.org*, https://www.gnuradio.org/ (accessed Nov. 4, 2022).
[3] Great scott gadgets. [Online]. Available: https://greatscottgadgets.com/sdr/. [Accessed: 14-Oct-2022]
[4] "IEEE Draft Standard for Local and Metropolitan Area Networks - Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs) Amendment - Physical Layer (PHY) Specifications for Low Energy, Critical Infrastructure Monitoring Networks (LECIM)," in IEEE P802.15.4k/D3, November 2012 , vol., no., pp.1-133, 10 Jan. 2013.
[5] Rpp0, "Gr LoRa", *GitHub*. [Online]. Available: https://github.com/rpp0/gr-lora [Accessed: 26-Oct2022]
[6] Tapparelj, "Tapparelj/gr-LORA_SDR," *GitHub*. [Online]. Available: https://github.com/tapparelj/gr-lora_sdr. [Accessed: 03-Nov-2022].

[7] MULTITECH, “MultiTech mDot™ Box MTDOT-BOX-G-915-B.”, *multitech.com*, https://www.multitech.com/models/99999211LF (accessed Nov. 4, 2022).
[8] ESPRESSIF, “ESP32.”, *espressif.com*, https://www.espressif.com/en/products/socs/esp32 (accessed Nov. 4, 2022).
[9] Arduino, “Home,” *Arduino.cc*. [Online]. Available: https://www.arduino.cc/. [Accessed: 04-Nov-2022].
[10] The Things Network, “The things network,” *thethingsnetwork.org*. [Online]. Available: https://www.thethingsnetwork.org/. [Accessed: 05-Nov-2022].
[11] RAK, “RAK7249.”, rakwireless.com, https://www.rakwireless.com/en-us/products/lpwan-gatewaysand-concentrators/rak7249 (accessed Oct. 5, 2022).
[12] E. Bout, V. Loscri and A. Gallais, "Energy and Distance evaluation for Jamming Attacks in wireless networks," 2020 IEEE/ACM 24th International Symposium on Distributed Simulation and Real Time Applications (DS-RT), 2020, pp. 1-5, doi: 10.1109/DS-RT50469.2020.9213652.
[13] D. Yim et al., "An experimental LoRa performance evaluation in tree farm," 2018 IEEE Sensors Applications Symposium (SAS), 2018, pp. 1-6, doi: 10.1109/SAS.2018.8336764.
[14] A. I. Petrariu, A. Lavric and E. Coca, "LoRaWAN Gateway: Design, Implementation and Testing in Real Environment," 2019 IEEE 25th International Symposium for Design and Technology in Electronic Packaging (SIITME), 2019, pp. 49-53, doi: 10.1109/SIITME47687.2019.8990791.