Report Date: 09/16/2022
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

Our team decided on the topic of the project this week and studied related the topic. We were interested in cyber security and networking. Therefore, we took LoRaWAN hacking as a topic of the project through the meeting with Professor Anthony Smith. We heard an explanation of the topic from the professor and decided on the direction of how to research. After that, we studied basic knowledge necessary for the project, such as networking and LoRaWAN. We also went to the professor's lab to get some devices we need to construct LoRaWAN network by our own.

What 454P completed this week:

- Research on LoRa and LoRaWAN

  LoRa is an RF modulation technology for LPWANs, which uses Chirp Spread Spectrum to send a signal between devices [1]. LoRaWAN is a network of LoRa devices. In short, LoRa is a physical layer, while LoRaWAN is a MAC layer.

- Research on LoRaWAN network architecture

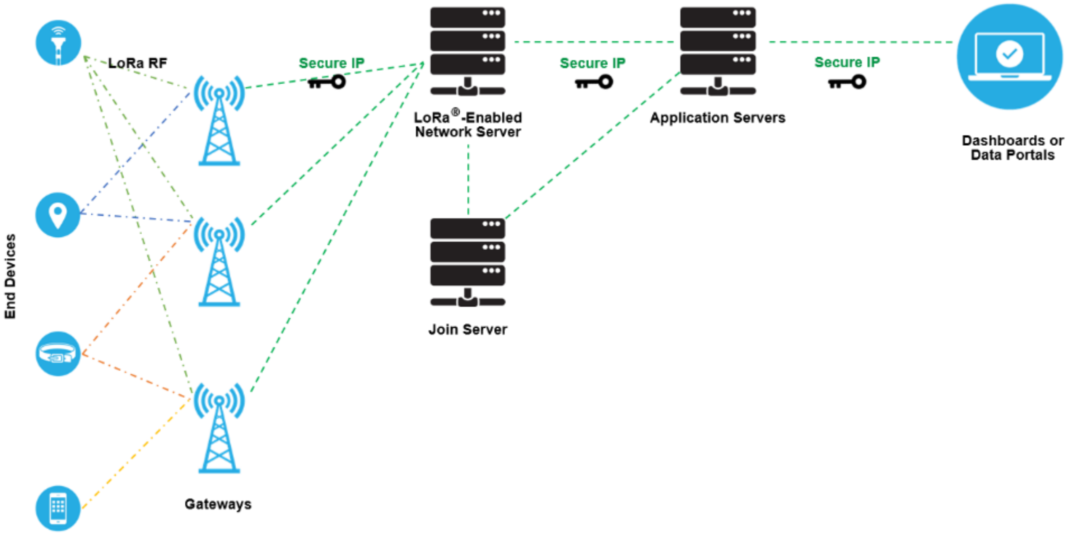

Fig. 1. Typical LoRaWAN network implementation [1]

LoRaWAN's network uses gateways as a connector from the end node to the LoRa network server. From there, the join server checks the join request message and sends information about the sensor to application servers, then sends the join accept message to the LoRa network server which distributes that message back to the end node [2]. We found several paths to break into this connection. If possible, hacking into the application servers would be the most impactful way. However, the most vulnerable path we thought was the end node to gateways since they do not exchange the application keys [3]. We will further investigate this.

- Reasons why LoRaWAN security is important

  The wireless network is always vulnerable to packet sniffing because the way it communicates is public and shared information [4]. As LoRaWAN is used for many IoT devices, especially for farming, because it is able to do the long-range communication between devices, hacking successfully into LoRaWAN can cause serious problems for the users.

Things to do by next week

- Set up the LoRaWAN network [5].
- Check packet communications of the established LoRaWAN network and learn how LoRaWAN exchanges packets.
- Sniff some packets from the other sources if possible, using the MCU.

Problems or challenges:

We need to study GoLang to understand how LoRaWAN works or to use LoRAWAN API because it is written in GoLang [6]. We have two people in our group who have experience in GoLang, however, all our team members might need to study it.

References

[1] Semtech, "What are LoRa® and LoRaWAN®?," *lora-developers.semtech.com*, https://lora-developers.semtech.com/documentation/tech-papers-and-guides/lora-and-lorawan (accessed Sep. 14, 2022).

[2] Makerdemy, Chennai, Tamil Nadu, IND. *What is LoRa? (2020) | Learn Technology in 5 Minutes*. (Feb. 25, 2020). Accessed: Sep. 15, 2022. [Online Video]. Available: https://www.youtube.com/watch?v=WdJxXzSE9Gs

[3] Semtech Corporation. *LoRaWAN: Providing Secure and Reliable Connectivity.* (Apr. 2, 2020). Accessed: Sep. 9, 2022. [Online Video]. Available: https://www.youtube.com/watch?v=WdJxXzSE9Gs

[4] S. Vinjosh Reddy, K. Sai Ramani, K. Rijutha, S. Mohammad Ali and C. Pradeep Reddy, "Wireless hacking - a WiFi hack by cracking WEP," *2010 2nd International Conference on Education Technology and Computer,* 2010, pp. V1-189-V1-193, doi: 10.1109/ICETC.2010.5529269.

[5] Multitech, "Dot box and EVB Software," *multitech.net*, http://www.multitech.net/developer/software/dot-box-and-evb-software (accessed Sep. 14, 2022).

[6] “Lorawan,” Nov. 22, 2015 [Online] Available: https://github.com/brocaar/lorawan (accessed Sep. 14, 2022).