Report Date: 10/06/2022
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 purpose of this week was to set up a local LoRaWAN network with Chirpstack. Several problems occurred while building the network, but it was confirmed that data was being transmitted to uplink and downlink normally from the end device to the application server. Also, based on the feedback received at the meeting for the paper review on Monday, team members revised the format of the paper and refined the introduction section. The writing of the literature review started with analyzing the prior attack methods of LoRaWAN and other wireless networks.

What 454P completed this week:

- Establish a connection between the application server and the network server

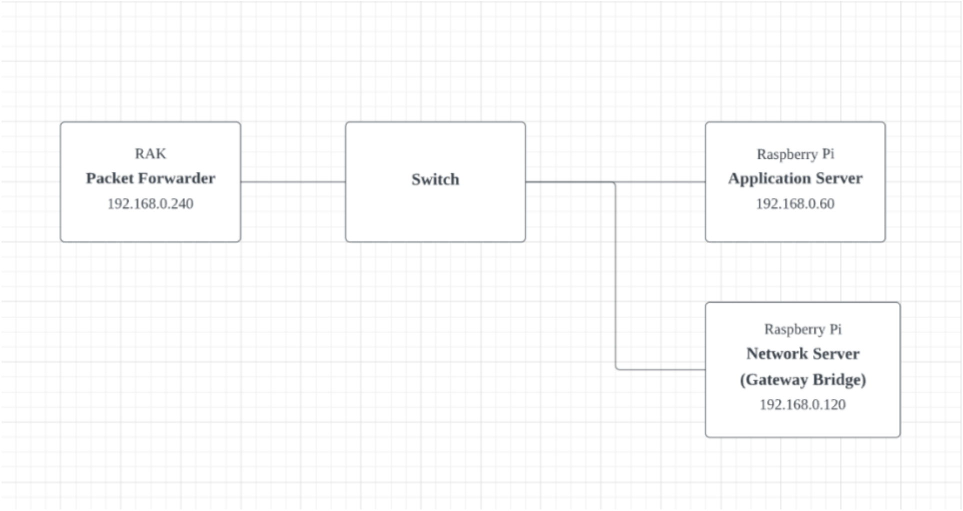


Fig. 1. LoRaWAN network architecture designed this week

To set up the local LoRaWAN network with ChirpStack, local LAN is constructed with two Raspberry Pis using Raspbian OS. One of the Raspberry Pis is set as a network server using Chirpstack v3, and another one is set as an application server using Chirpstack v4. By constructing the servers in this way, it is easier to monitor our servers if anything happens, since the connection is separated into two modules. By using the vanilla Chirpstack server, the connection between the network server and the application server could not be established, since they used different IP addresses and the vanilla Chirpstack configuration does not support different IP addresses rather than localhosts. By changing all the configuration files, the connection was established, but other issues were raised.

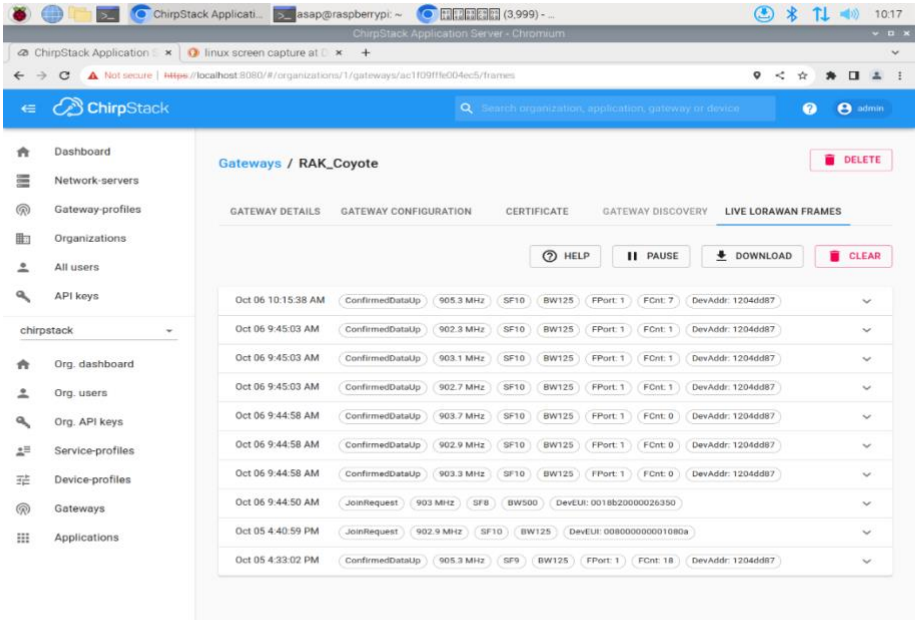
- SSL/TLS Connection between the application server and the network server

For the gateway to connect to the network server, certification files must be set from the network server and the gateway, so that they could connect securely. Thus, setting up an SSL/TLS connection is also needed between the application server and the network server since the network server will open the ports with SSL/TLS connection. For this reason, creating PEM files to configure secure connections was mandatory. There was already an existing program to make the certification files[6], however, the program was written in Golang[1], and as Golang does not support root access naturally since golang is made to use dockers without root permission[2], giving Golang root permission to generate certification files was the first challenge. By adding a root directory into the PATH environment and switching the directory of GOROOT and GOPATH[3], Golang and cfssl could be used in root permission, thus generating the PEM files, which were distributed to both the application and network server.

- CN

As the vanilla Chirpstack starts with a localhost-based network and application server, the Common Name (CN) of the PEM file was localhost (127.0.0.1), which ended up causing problems. Searching about x509 certification[4], and looking through cfssl's official documentation[5], manipulation of the configuration file of the ChirpStack certification generator[6] was executed, which changed all of the CN to 192.168.0.120 and 192.168.0.60, which is the address of network and application server respectively. By doing so, the connection between the network server and the application server was secured with SSL/TLS protocol, and ready for new gateways to connect through this pipe.

- Connecting RAK gateway into the network server



```
Oct 06 10:15:38 AM  ConfirmedDataUp  905.3 MHz  SF10  BW125  FPort: 1  FCnt: 7   DevAddr: 1204dd87
Oct 06 9:45:03 AM   ConfirmedDataUp  902.3 MHz  SF10  BW125  FPort: 1  FCnt: 1   DevAddr: 1204dd87
Oct 06 9:45:03 AM   ConfirmedDataUp  903.1 MHz  SF10  BW125  FPort: 1  FCnt: 1   DevAddr: 1204dd87
Oct 06 9:45:03 AM   ConfirmedDataUp  902.7 MHz  SF10  BW125  FPort: 1  FCnt: 1   DevAddr: 1204dd87
Oct 06 9:44:58 AM   ConfirmedDataUp  903.7 MHz  SF10  BW125  FPort: 1  FCnt: 0   DevAddr: 1204dd87
Oct 06 9:44:58 AM   ConfirmedDataUp  902.9 MHz  SF10  BW125  FPort: 1  FCnt: 0   DevAddr: 1204dd87
Oct 06 9:44:58 AM   ConfirmedDataUp  903.3 MHz  SF10  BW125  FPort: 1  FCnt: 0   DevAddr: 1204dd87
Oct 06 9:44:50 AM   JoinRequest  903 MHz  SF8  BW500  DevEUI: 0018b20000026350
Oct 05 4:40:59 PM   JoinRequest  902.9 MHz  SF10  BW125  DevEUI: 008000000001080a
Oct 05 4:33:02 PM   ConfirmedDataUp  905.3 MHz  SF9  BW125  FPort: 1  FCnt: 18  DevAddr: 1204dd87
```

Fig. 2. Demonstration of RAK gateway connected to the application server

Multitech had an issue from udhcpc.d daemon[7], Dragino router[8] cannot be set up as a gateway, and SX1262[9] cannot be set up as a gateway either. So, giving a shot for the RAK gateway[10] from another team (Team Coyote) was the last option, since there was no more gateway to use until the new ones are delivered. By connecting the RAK gateway to the local LAN and setting it as a packet forwarder[11], while setting up a new gateway bridge with a modified configuration file for the network server, the RAK gateway successfully connected to our network and application server. Since it is a packet forwarder, the basic commands for the gateway cannot be sent into the RAK gateway, but uplink and downlink packets of signals tested by a LoRa tester was successfully showed up on the application server as Fig. 2.

- Writing the literature review of the paper

  Research is conducted to write the LoRaWAN security parts of the paper by analyzing similarities or differences in both structure and vulnerabilities, of LAN and WAN, through the Wi-Fi and other wireless networks' hacking cases[12]. Also, reviewing LoRaWAN attack methods such as bit-flipping attack[13], replay attack[14], and jamming[15] is conducted. The Literature review includes LoRaWAN's network architecture, authentication methods, and the novelty of this study, which is different from previous studies.

Things to do by next week

- Analyze LoRaWAN hacking cases to derive methodologies
- Set LoRaWAN using Dragino LSP8N[16] and SX1302[17]
- Make certificates for the gateway
- Set up a LoRaWAN gateway as a basic station instead of the packet forwarder

Problems or challenges:

A packet forwarder serves to replay packets from one network segment to another[18]. A gateway is a computer or software that enables the communication between networks using different protocols [19]. Although a network connection from the packet forwarder to the application server was established this week, implementing an environment that is more realistic with a gateway connected to the application server is crucial for a real-life hacking scenario. Therefore, changing the device connected by a packet forwarder to a gateway will be conducted next week.

References

[1] Go, "Get started with Go.", *go.dev*, https://go.dev/ (accessed Oct. 3, 2022).
[2] *Golang Armbuilds.* (2016). Hypriot. https://github.com/hypriot/golang-armbuilds Accessed: Oct. 4, 2022.
[3] *Golang Armbuilds.* (2016). Hypriot. https://github.com/hypriot/golang-armbuilds/issues/6 Accessed: Oct. 4, 2022.
[4] SSL, "X.509 Certificate.", *ssl.com*, https://www.ssl.com/faqs/what-is-an-x-509-certificate/ (accessed Oct. 4, 2022).
[5] *CFSSL*. (2014). Cloudflare. https://github.com/cloudflare/cfssl Accessed: Oct. 4, 2022.
[6] *ChirpStack certificates.* (2018). Brocaar. https://github.com/brocaar/chirpstack-certificates Accessed: Oct. 4, 2022.
[7] Debian, "Udhcpc Manpages.", *manpages.debian.org*, https://manpages.debian.org/stretch/udhcpc/udhcpc.8 (accessed Oct. 5, 2022).
[8] Docker, "Install Docker Desktop on Linux.", *docs.docker.com*, https://docs.docker.com/desktop/install/linux-install/ (accessed Oct. 5, 2022).

[9] Waveshare, “Pico-LoRa-SX1262”, *waveshare.com*, https://www.waveshare.com/wiki/Pico-LoRa-SX1262 (accessed Oct. 5, 2022).
[10] RAK, “RAK7249.”, *rakwireless.com*, https://www.rakwireless.com/en-us/products/lpwan-gateways-and-concentrators/rak7249 (accessed Oct. 5, 2022).
[11] RAK, “Amazon Web Services.”, *rakwireless.com*, https://docs.rakwireless.com/Knowledge-Hub/Learn/Amazon-Web-Services/ (accessed Oct. 5, 2022).
[12] 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.
[13] JungWoon Lee, DongYeop Hwang, JiHong Park and Ki-Hyung Kim, "Risk analysis and countermeasure for bit-flipping attack in LoRaWAN," 2017 International Conference on Information Networking (ICOIN), 2017, pp. 549-551, doi: 10.1109/ICOIN.2017.7899554.
[14] SeungJae Na, DongYeop Hwang, WoonSeob Shin and Ki-Hyung Kim, "Scenario and countermeasure for replay attack using join request messages in LoRaWAN," 2017 International Conference on Information Networking (ICOIN), 2017, pp. 718-720, doi: 10.1109/ICOIN.2017.7899580.
[15] E. Aras, N. Small, G. Sankar Ramachandran, S. Delbruel, W. Joosen, D. Hughes, "Selective Jamming of LoRaWAN using Commodity Hardware," 14th EAI International Conference on Mobile and Ubiquitous Systems, 2018, doi:10.4108/eai.7-11-2017.2273515
[16] Dragino, “LPS8N Indoor LoRaWAN Gateway.”, *dragino.com*, https://www.dragino.com/products/lora-lorawan-gateway/item/200-lps8n.html (accessed Oct. 6, 2022).
[17] Semtech, “SX1302.”, *semtech.com*, https://www.semtech.com/products/wireless-rf/lora-core/sx1302 (accessed Oct. 6, 2022).
[18] The Things Network, “Packet Forwarders.”, *thethingsnetwork.org*, https://www.thethingsnetwork.org/docs/gateways/packet-forwarder/ (accessed Oct. 6, 2022).
[19] The Things Network, “Gateways.”, *thethingsnetwork.org*, https://www.thethingsnetwork.org/docs/gateways/ (accessed Oct. 6, 2022)