Léonard de Vinci

PROJECT LORAWAN
-
SECURE LORA LAN

Groupe 1 - TD IOS 2
LEDOUX Alexis - MARCHAL Baptiste - MEROLLA Mathis - NIVESSE Charles

Année universitaire 2020/2021

SUMMARY

INTRODUCTION

The idea of the project is to make a small local area network with LORA. We want to set up a gateway that can be used by multiple LORA modules.

For this project, we used 3 SODAQ Explorer boards. One board functions as the gateway and the others functions as modules which can send and receive data from the gateway. We also used two temperature sensors which will provide data to be sent to the gateway. Finally, we used a mobile application to visualize the end node data.

SCENARIO

Within all these requirements, we established a scenario which describes the problem best.

FIRST SCENARIO

materials needed :

- 1 phone
- 1 gateway
- 2 modules
- 2 temperatures sensors

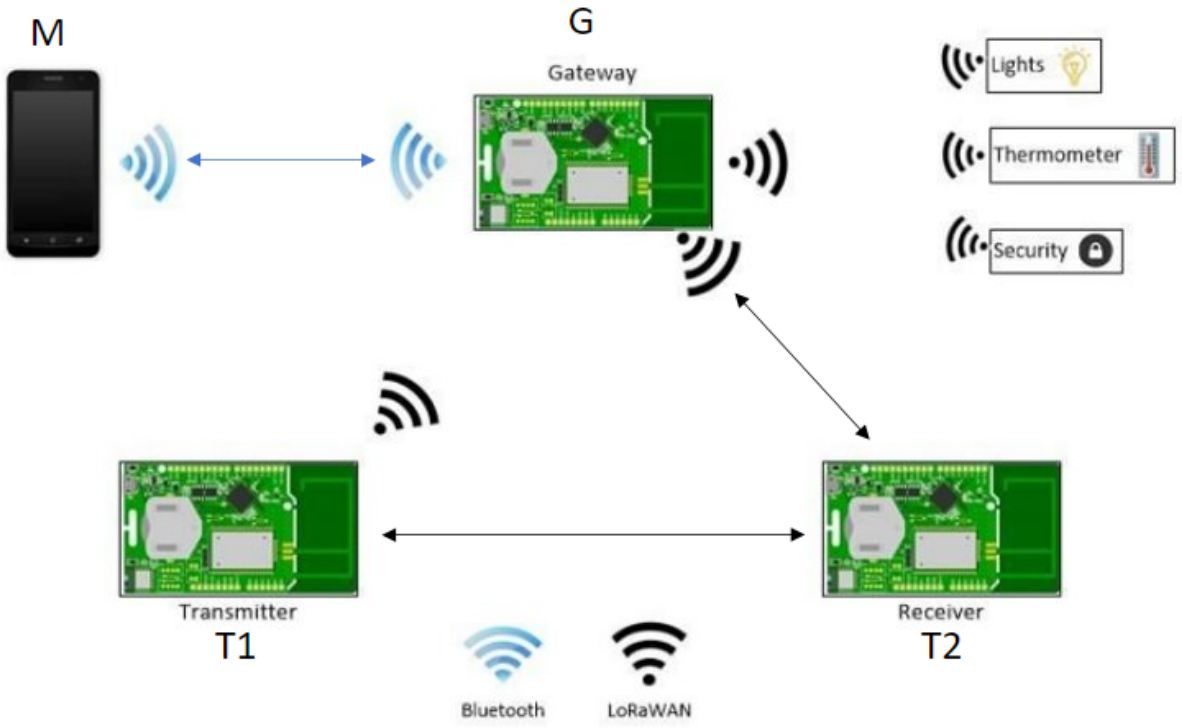

FIGURE 1 : Scenario 1 schema

A user will use a button on the app on his mobile M. Then the gateway G will ask the card T2 of the network to wake up. Then T2 will do the same for the card T1. Once T1 is awake it will get the temperature θ1 around him with its sensors and send the value to T2 before going back to sleep. T2 will do the same, getting the temperature θ2 and then sending both θ1 and θ2 values to the gateway before going back to sleep too.
Hence the gateway will send θ1 and θ2 to the mobile by bluetooth and it will be shown on the screen.

Eventually, we failed to use one of the modules, which appeared to not function properly. We came up with an alternative scenario which is still relevant to the initial problem.

SECOND SCENARIO

materials :

- 1 phone
- 1 gateway
- 1 module
- 1 temperature sensor

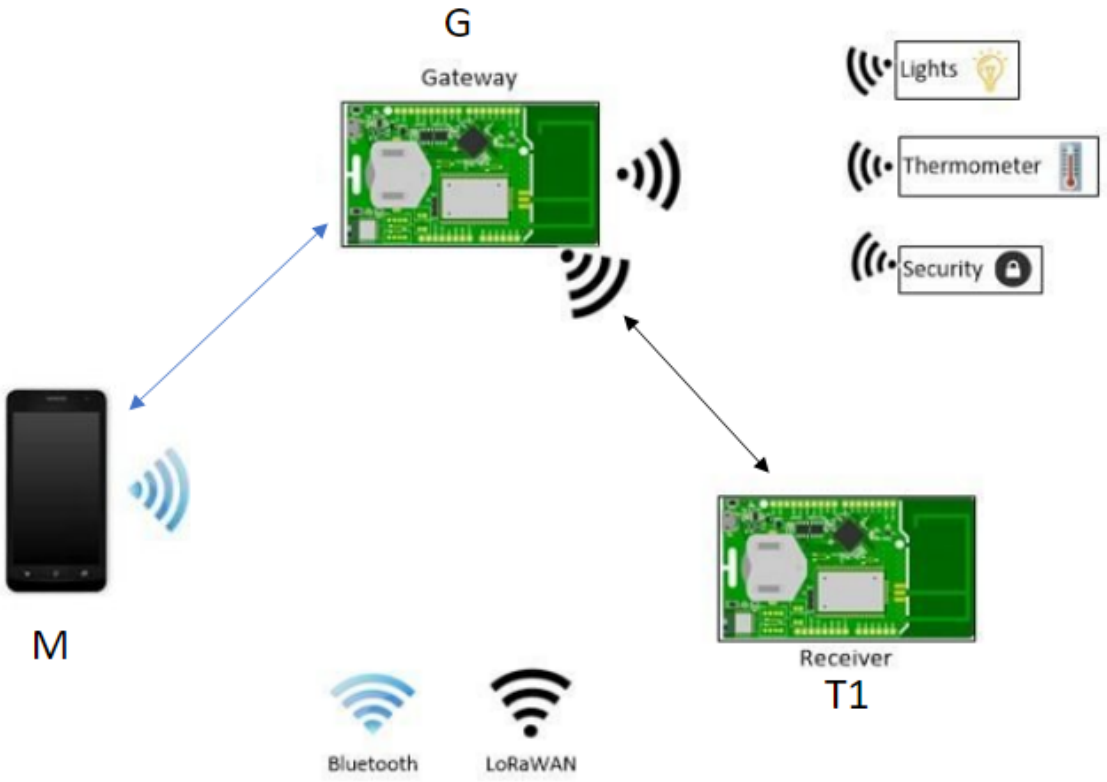

FIGURE 2 : Scenario 2 schema

A user will use a button on the app on his mobile M. Then the gateway G will ask the card T1 of the network to wake up. Once T1 is awake it will get the temperature θ1 around him with its sensors and send the value to the gateway before going back to sleep.
Hence the gateway will send θ1 to the mobile by bluetooth and it will be shown on the screen.

SLEEP

This LoRa protocol needs to be designed to function with low-power transmission at a moderate bit-rate and low duty-cycle.
In order to operate longer periods of time without access to energy sources, low-power optimized operation is a design requirement: this is where sleep modes come into play: energy savings are created by putting the sensors to sleep.

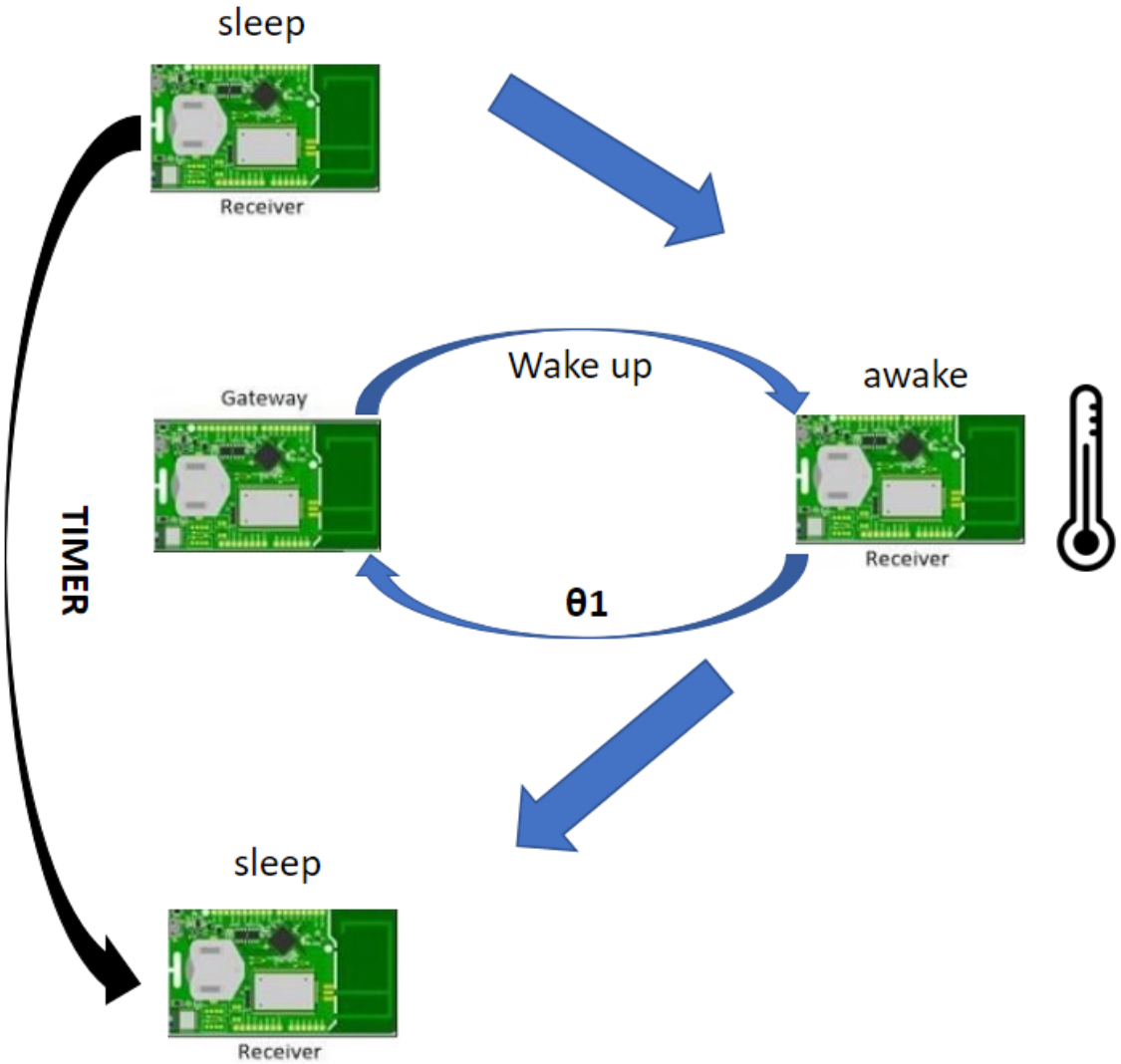

FIGURE 3 : Sleep schema

P2P

The main goal is to create a P2P with LORA. We needed here to establish the P2P connection between the gateway and the module board.

To use the P2P functionality of the Lora with the Sodaq Explorer, we use the radio feature. It is basically a broadcast in the Lora network, that everyone can access and read. So, it makes transmission easy and accessible, but it is a big concern for security, as everyone can make a “Man in the Middle attack” and access every single Data with send. (cf refer to crypto part).

We used some basic code that was given in the sodaq support page (an Rx and an Tx Example).

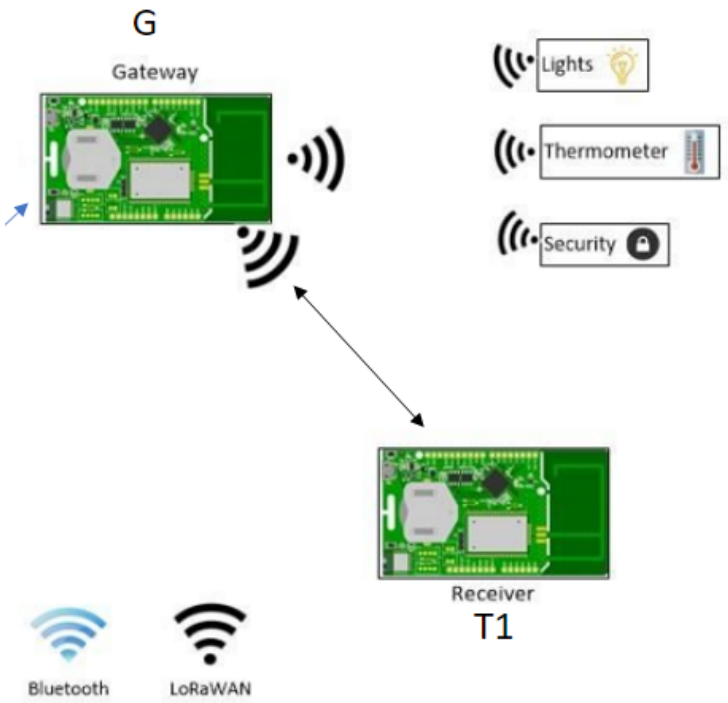

FIGURE 4 : P2P LORA

CRYPTO

To securise the connection, we first thought to do an asymmetrical encryption.

Asymmetric Encryption uses two distinct, yet related keys. One key, the Public Key, is used for encryption and the other, the Private Key, is for decryption. As implied in the name, the Private Key is intended to be private so that only the authenticated recipient can decrypt the message.

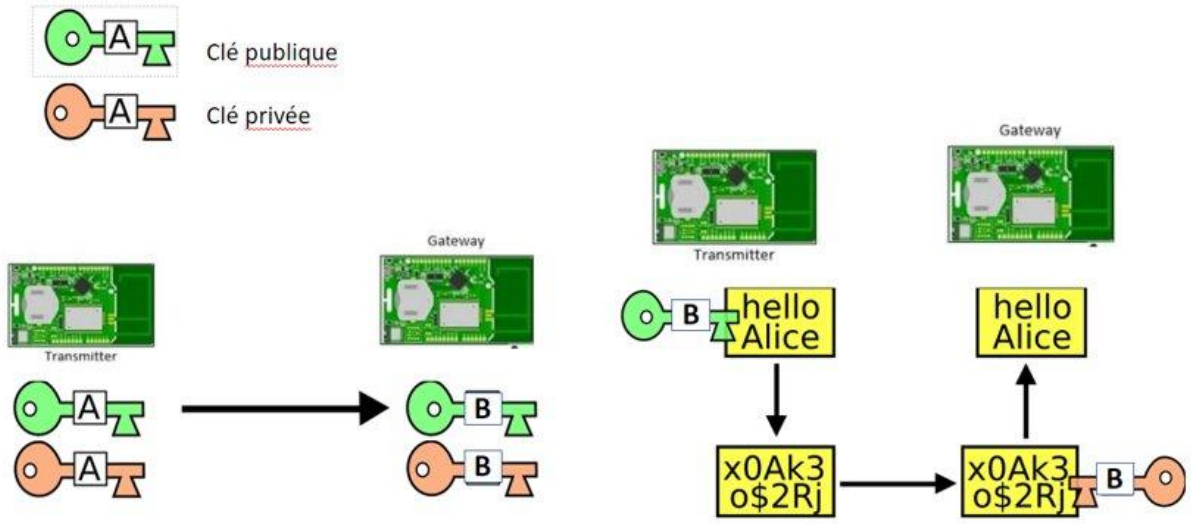

FIGURE 5 : Asymmetrical encryption

Here in the example, we use the public key of the gateway to encrypt the data we want to send to the gateway, then the gateway uses its private key to decrypt it.

However, we decided to use the AES algorithm to encrypt our data. Each time we send something over the Lora network, we encrypt the message before sending, so anyone sniffing the network can't get the value of what we want to send, if they don't have the Key.

AES is a symmetric encryption algorithm, which means that every board in the mesh should remember the same key, and this key must remain secret at all cost (otherwise the encryption is useless).

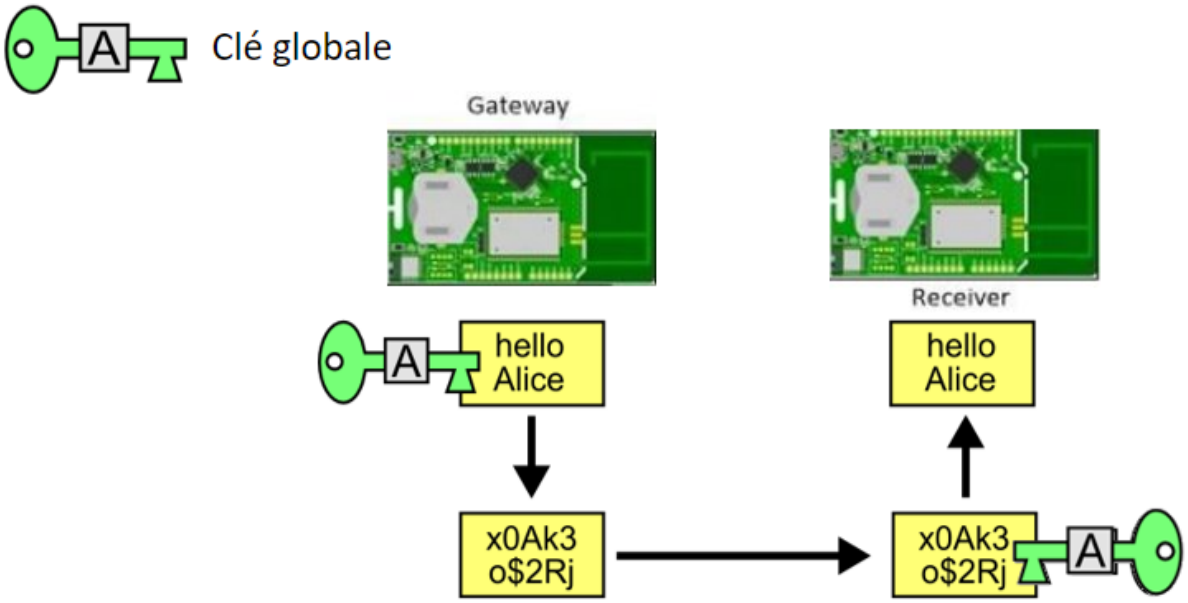

FIGURE 6 : AES crypto

Here in the example, we use the global key to encrypt the data we want to send, then use the same key to decrypt it.

BLUETOOTH

We tried here to connect the gateway to a mobile application to visualize the end node date.
Here, we used an application named Serial Bluetooth Terminal, downloaded from the Google Store.

We encountered some issues with the bluetooth connection on our android mobiles, so we tried to emulate a mobile on our computer.

After trying multiple emulators, we didn't succeed. :(

BIBLIOGRAPHY

Loenen, J. (2019). *LoRa peer-to-peer - SODAQ Support pages*. Support Sodaq. https://support.sodaq.com/Boards/ExpLoRer/Examples/lora_p2p/

Loenen, J. (2019). *Crypto Chip - SODAQ Support pages*. Support Sodaq. https://support.sodaq.com/Boards/ExpLoRer/Examples/crypto/

Bodin, P. (2017, 18 avril). *SODAQ ExpLoRer and Bluetooth – Systev*. systev. https://systev.com/sodaq-explorer-and-bluetooth/

Loenen, J.(2019). *MCU Deep Sleep - SODAQ Support pages*. Support Sodaq. https://support.sodaq.com/Boards/ExpLoRer/Examples/LoRaWAN_Deep_Sleep_v1_0.pdf

new AES library. (2012). Forum Arduino. https://forum.arduino.cc/index.php?topic=88890.0