IoT Security

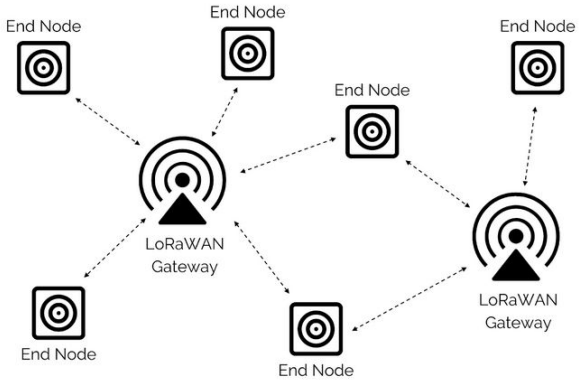
LoRa IoT

PV285

Václav Oujezský, Bacem Mbarek, Karel Slavíček,Tomáš Pitner

LoRa

- LoRa was formed by the composition of the words “Long Range” and is a **proprietary technology of Semtech**.
- the LoRa network is matched to the **star topology** in which the IoT end device is connected to the central network server via gateways.
- The minimum bandwidth is 125 kHz, which supports a maximum clutch loss of 157 dB.
- Proprietary, energy-efficient LoRa-based Chirp Spread Spectrum modulation is used to increase interference immunity.



https://www.thethingsnetwork.org/docs/lorawan/

MUNI
FI

LoRa

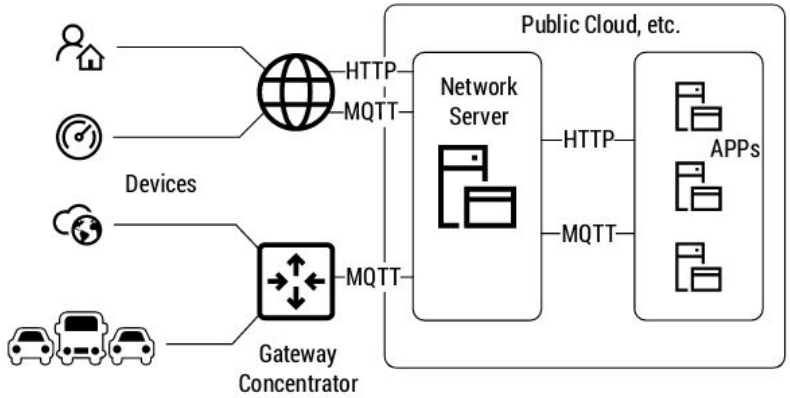
- LoRa symbols are modulated over an up-chirp of 125 kHz bandwidth and different orthogonal spreading factors are used based on data rate requirement and channel conditions.
- LoRa itself uses SF7 to SF12 spreading factors. LoRa modulation can be used in a wide range of frequencies from 137 MHz to 1020 MHz. This includes ISM series of license-free bands such as 169 MHz, 433 MHz, 868 MHz and 915 MHz.

LoRaWAN

- LoRaWAN network architecture is typically deployed in the star topology.
- In the LoRaWAN network, nodes are not associated with a particular gateway.
- Data transmitted by the node is typically received by multiple gates.
- Gateways here work as a transparent bridge that passes messages between end devices and a central network server.
- Gateways are connected to a network server via standard IP (Internet Protocol) connections, while end devices use wireless communication with LoRa radio connections.
- All endpoint communication is generally bi-directional, but also supports operations such as multicast.

LoRaWAN

- **MQTT** (Message Queuing Telemetry Transport) **provider** is a server that collects MQTT Publishing / Subscribing commands and sends data accordingly. It provides standard authentication mechanisms that only allow authorized users access to the data.
- The **application server** is a server that interacts with application resources published by the network server. Data received from an MQTT provider are processed by a specific application. The API is mostly based on MQTT with JSON encoding.



LoRaWAN Network Stack

- The network stack of LoRaWAN is defined by the LoRaWAN specification.
- It starts with the Radio PHY layer. The PHY layer is created by preamble, which is 8 bytes of 0x34 for EU863-870 MHz ISM Band, a header **PHDR** and payload **PHYPayload**, followed by CRCs. The PHYPayload starts with a MAC header MHDR followed by the MAC Payload and an integrity check value MIC.
- User's data are included in the MAC header and payload. The MAC Payload is composed of Frame Header FHDR, Frame Port **FPort**, and Frame Payload **FRMPayload**. The FPort denotes if the message contains only MAC commands, or application specific data.

https://lora-developers.semtech.com/documentation/tech-papers-and-guides/sending-and-receiving-messages-with-lorawan/sending-and-receiving-messages

MUNI
FI

Security and LoRaWAN

- LoRaWAN considers **two security layers**, one for the network and the other for the applications.
- The LoRaWAN solution comes with an authentication and security framework and a framework based on the AES-128 (Advanced Encryption Standard) encryption algorithm.
- The AES-128 encrypts the trustworthy framework and generates the Message Integrity Code (MIC) for integrity.
- Each end device has an assigned key from the device manufacturer or application owners.
- Authentication and encryption are segregated, so authentication of packets can be ensured and integrity protected.

MUNI
FI

Security and LoRa

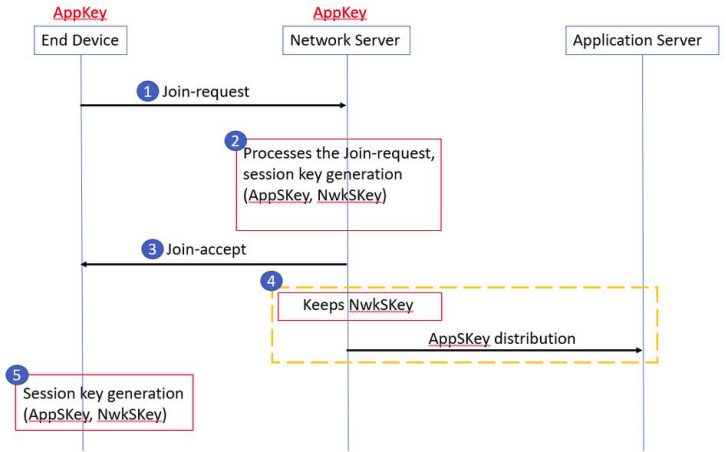
How the symmetric keys are distributed depends on how a node joins the network.

There are two following types:

- **Over-The-Air-Activation (OTAA)**
- **Activation by Personalisation (ABP)**

Security and LoRa - OTAA

- Nodes contain a unique 128-bit application key **AppKey** and this key is sent with a join request message.
- The message is signed by the key, but not encrypted.
- The join request includes an unique application identifier **AppEUI** and globally unique device identifier **DevEUI** value and randomly generated two byte value of **DevNonce**.
- All three values are signed with a 4 byte **MIC**.



MUNI FI

Security and LoRa - ABP

- Nodes are shipped with the **DevAddr** and session keys **NwkSKey** and **AppSKey**.
- The nodes can begin communicating with the network server without the join message, as they already have the keys.

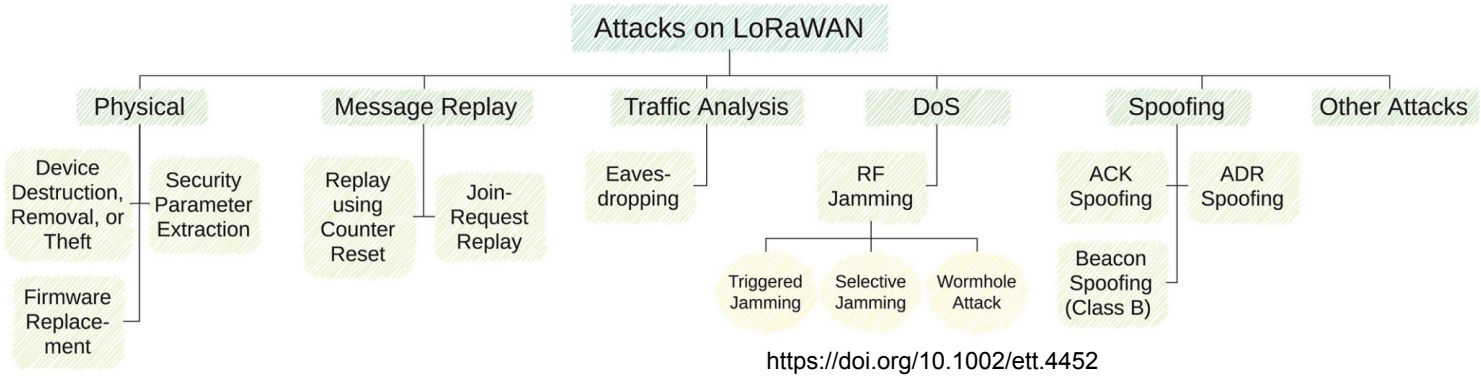
MUNI FI

Security and LoRa - message encryption

- Encryption of messages is performed using AES 128.
- The **NwkSKey** is used if the **FPort** is set to 0, if not, the **AppSKey** is used.
- In LoRa, counters for sent messages **FCntUp** and received messages **FCntDown** ***never repeat***.
- It is very important feature, because those counters are used to produce a decrypted or encrypted key-stream. More precisely, the key-stream includes those non repeated values and all the key-stream is than XOR'd with the **FRMPayload** to decrypt or encrypt data.

IoT Attacks

- If the IoT is taken in general, it is possible to classify attacks into individual categories.
- These categories include physical attacks, network attacks, software attacks, encryption attacks.
- Attacks can be node manipulation, RFID interference, node lock in wireless sensor network, malicious node deployment, physical damage, social engineering, traffic analysis, DoS (Denial Of Services) execution, RFID spoofing, messaging, man in the middle attack, router attack, virus attacks, side channel attacks, crypto-analysis and others



https://doi.org/10.1002/ett.4452

MUNI FI

Attacks on the LoRaWAN Network

Examples for the lab exercises:

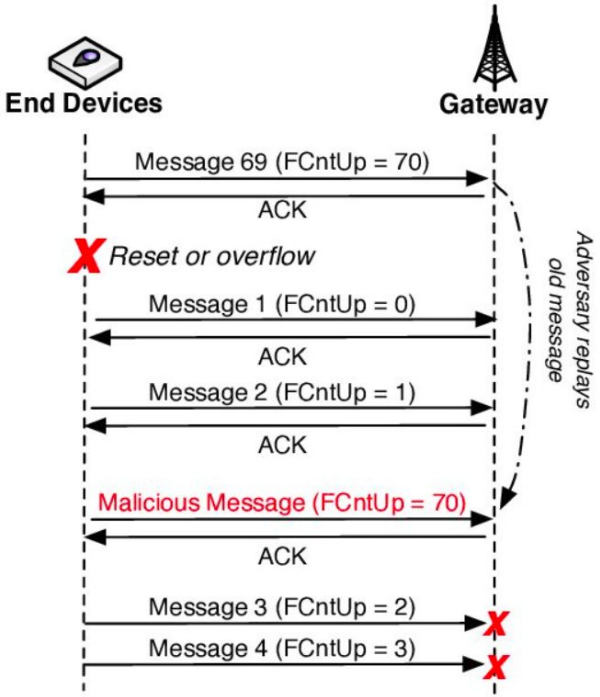
- Re-play attack for ABP activated nodes
- Bit Flipping Attack with own Network server

Re-play attack for ABP activated nodes

The network server may receive a malicious message that complies with the following requirements:

- The session keys are the same as one accepted end device.
- DevAddr is the same as one accepted end device.
- If the counter value is acceptable.

More detailed information:
https://ieeexplore.ieee.org/document/8631198



Yang, Xueying & Karampatzakis, Evgenios & Doerr, Christian & Kuipers, Fernando. (2018). Security Vulnerabilities in LoRaWAN. 129-140. 10.1109/IoTDI.2018.00022.

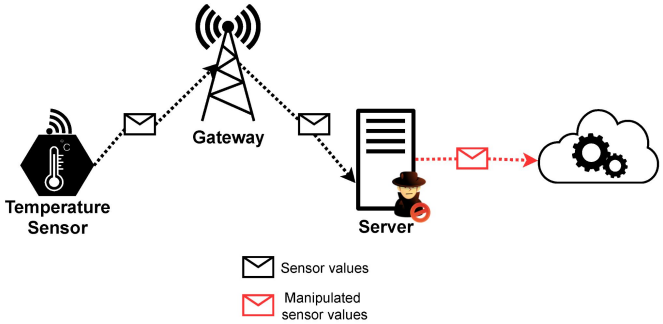
MUNI FI

Bit Flipping Attack

The goal of the lab is to test whether the integrity between the network server and the application server is protected. The hypothesis is, **If an attacker has the ability to capture traffic (on network server or between network and application server)**, there is no way the application server can detect whether the message is from the attacker or the network server.

unencrypted text ⊕ *key* = *encrypted text*
encrypted text ⊕ *key* = *unencrypted text*

The open text position corresponds to the same ciphertext position. An attacker aims to modify the given encrypted text to affect the open text.
More detailed information:
https://ieeexplore.ieee.org/document/8631198



(a) Bit-Flipping attack example.

PlainText : {ID: 001, humidity: 13}
CipherText : 00BN12JH54BF45NM66JJEO78CB94KJ40EN00F30B

CipherText : 00BN12JH54BF45NM66JJEO78CB94KJ40EN00F60B
PlainText : {ID: 001, humidity: 43}

(b) Sensor data manipulation.

Torres, N.; Pinto, P.; Lopes, S.I. Security Vulnerabilities in LPWANs—An Attack Vector Analysis for the IoT Ecosystem. Appl. Sci. 2021, 11, 3176. https://doi.org/10.3390/app11073176

MUNI FI

Lab exercises

Equipment:

RFM95 module + STM32 https://www.hoperf.com/modules/lora/RFM95.html

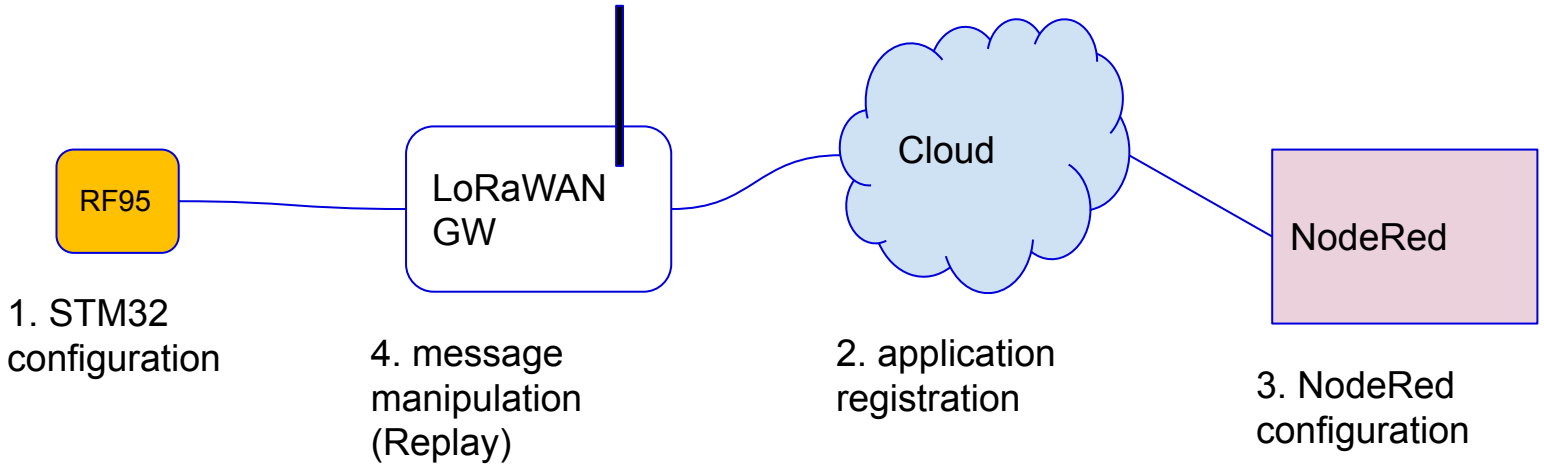
LoRaWAN: GW ic880a + raspberry pi

TheThingsNetwork Cloud https://www.thethingsnetwork.org/

NodeRed https://nodered.org/

MUNI
FI

Lab Scenario



MUNI FI

Lab Scenario - source code

Package IBM lmic for Arduino IDE STM : #include <lmic.h>

Source code .ino
https://drive.google.com/drive/folders/1xgMEBZPpAkQBz3QL7ETpPqWmE0n-Wmp0?usp=sharing

Source code NodeRed
https://drive.google.com/file/d/1tOLFdOWkzoWF-hqIwfSLPW_ur4ot0Vcg/view?usp=share_link

Python tools
https://drive.google.com/drive/folders/1Rd1cOLvYx-8OHUPE2OlAetvP2hSRtwqG?usp=share_link

This document and the code is for educational purposes only.

MUNI
FI