Long-range disruption of industrial processes using Drones and LoRaWAN

Ioannis Stavrou

Security Researcher

LPWAN Technology

- **LoRaWAN**[1] is a technology that falls in the area of Low Power Wide Area Networks (LPWAN)
- Other similar technologies include **Sigfox**, **NB-IoT** and **LTE-M**
- LPWAN technologies focuses on **long range** (up to 15km) and **low consumption** wireless devices (up to 10 years of battery life)
- A key additional advantage is the **low subscription costs**, with the caveat of low data rates

LPWAN Market[2] (2019)

LoRaWAN and the other three technologies are the **main players** in LPWAN field

The LPWAN market is currently **growing > 100%**

Asia-Pacific is the largest adopter of LPWAN technologies

Utilities remain the major market segment in the LPWAN market

HackInBo Winter 2021 Edition
17ª EDIZIONE

LPWAN Applications

Sigfox

- In Japan, **NICIGAS** is retrofitting **850,000 gas meters** with Sigfox connectivity.
- In Germany, **DHL** is equipping **250,000 roll cages** with Sigfox trackers.

LoRa

- In France, **Birdz** operates **400,000 LoRa-connected smart meters**.
- In Brazil, **MaxTrack** has equipped **1 million vehicle trackers** with LoRa connectivity.

NB-IoT & LTE-M

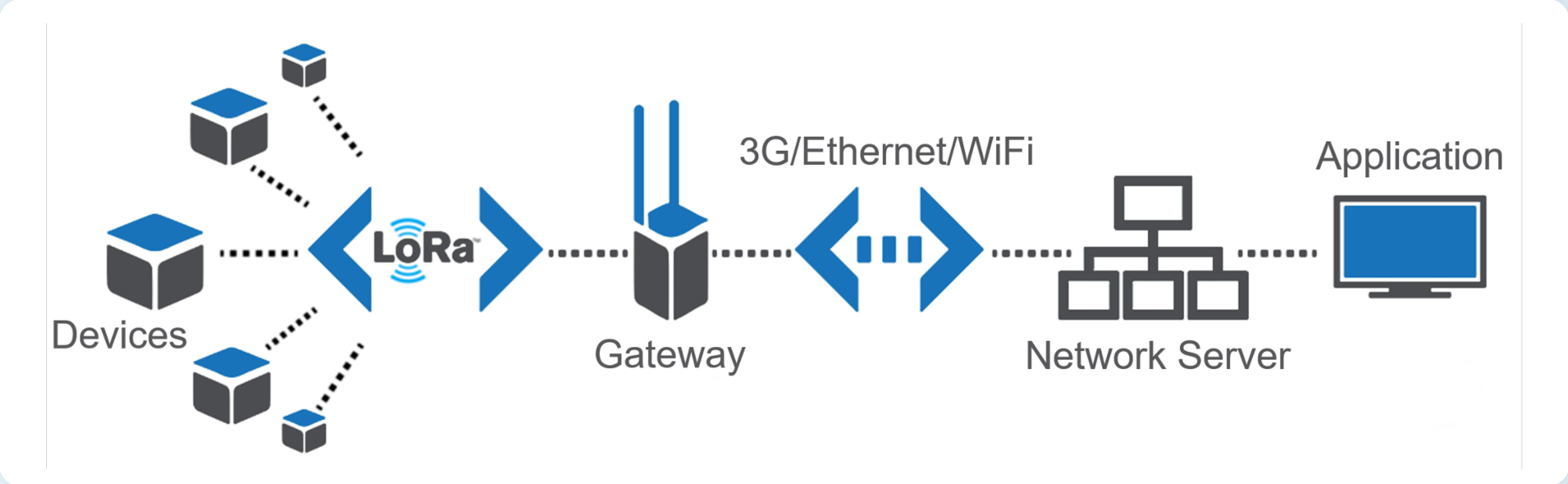
- In China, **NB-IoT** is used to track **1 million electric bikes** in Zhengzhou.
- In Sweden, over **2 million smart electricity meters** are being equipped with both NB-IoT and LTE-M radios.

LoRaWAN

- The LoRaWAN specification is a **Low Power**, **Wide Area** (LPWA) **networking protocol**
- Is designed to **wirelessly connect battery** operated ‘things’ to the internet in regional, national or global networks
- Targets key Internet of Things (IoT) requirements such as:
    - bi-directional communication
    - end-to-end security
    - mobility and localization services

LoRaWAN Architecture

- **LoRa** devices are operating in a star network topology and communicate with a **LoRa** Gateway
- The Gateway uses a **common transmission technology** (3g/Ethernet/WiFi) to send the information to the application server



HackInBo Winter 2021 Edition
17ª EDIZIONE

Threatening LoRaWAN

The goal is to **disrupt the industrial process** by exploiting the nature of the LoRaWAN protocol.

We will explore how we can **practically impact any process** that is based on the LoRa technology

Threatening LoRaWAN

We will challenge LoRa with the following two strategies:

- **Locate** the LoRaWAN sensors
  - We implemented a method to locate the LoRa sensors. The goal is to be able to locate sensors in long distances like in a pipeline.
- **Disrupt** the LoRa signal
  - We implemented a method to disrupt the signal from the sensor. This will lead the gateway to miss valuable packets.

HackInBo® Winter 2021 Edition
17ª EDIZIONE

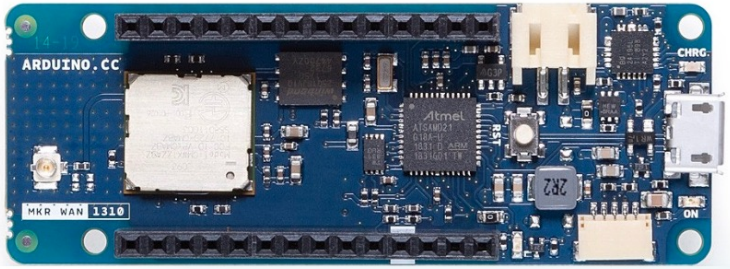
LoRaWAN – Lab Equipment

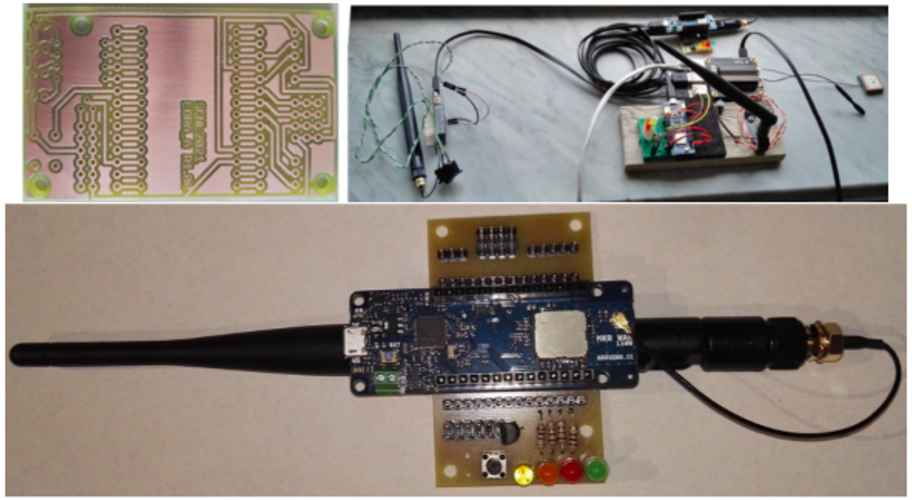
- For this project we used a number of **low-cost hardware**.
- **HackRF** is an affordable solution for a software-defined radio project.
- Can be **programmed** to **produce** or **receive LoRa signals** and process them.

HackInBo Winter 2021 Edition
17ª EDIZIONE

LoRaWAN – Lab Equipment

- We constructed the Gateway using an **Arduino MKR WAN 1310**
- The Gateway is **able to receive** lora packets
- Its is connected to a PCB and can be **remotely controlled** with a raspberry via a serial port.





HackInBo®
Winter 2021 Edition
17ª EDIZIONE

LoRaWAN Localization

Each LoRa sensor is emitting a signal to be able to communicate with the gateway

We can get **valuable information** even if the signal is **encrypted**

We can understand how **strong or weak** the signal is

And we can make an estimation about the **distance of the sensor** from the point of measurement

LoRaWAN Localization

- A radio signal receiver, produces the **Received Signal Strength Indicator** (RSSI)
- The RSSI value is measurement of the **power of the signal**
- Its measurement to know if we can get a **good wireless connection**
- The received signal power is in **milliwatts** and is **measured in dBm**.
- Is measured in **negative values** and the **closer to 0** the better the signal
- For LoRa the **minimum value is -120 dBm.**

HackInBo Winter 2021 Edition
17ª EDIZIONE

LoRaWAN Localization

- The RSSI can provide an **estimation of the distance from a node**

- The following mathematical formula can provide **the RSSI**

$$RSSI = -10 \cdot n \cdot log10d + A$$

Where:

- A: received power when the distance between the two antennas is 1 m.
- n: the loss parameter or loss exponent which depends on the environment conditions
- d: Is the distance from the measuring point

HackInBo® Winter 2021 Edition
17ª EDIZIONE

LoRaWAN Localization

- We can solve the equation for the distance

$$d = 10^{\frac{A-RSSI}{10n}}a$$

- We can infer the value A and n with an approximate value

$$n = 3.74A$$
$$= -35.8\ dBm$$

- They have been estimated by experimentation with the outdoor environment

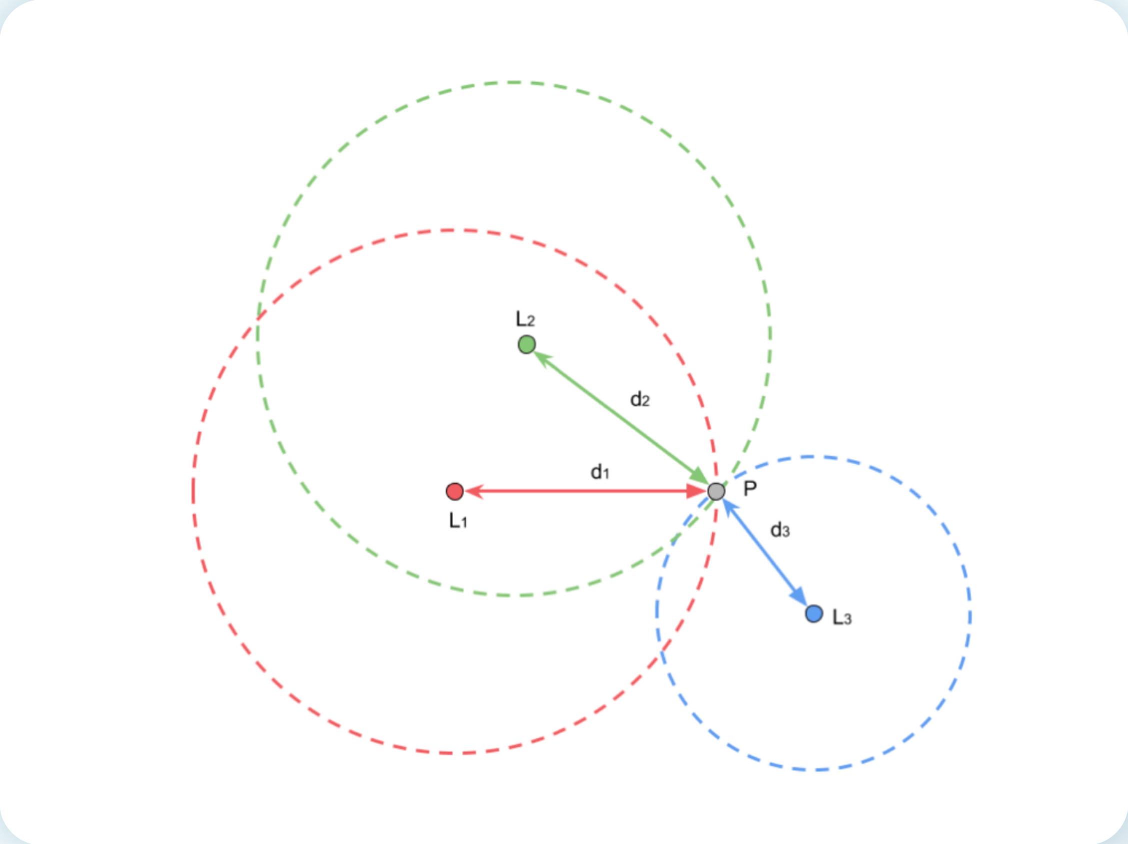
LoRaWAN Localization

Having the distance from one point **is not enough**

- We can use the Trilateration Algorithm to estimate the precise position of the device P from the estimated distance.
- It is a geometry-based algorithm where a set of circles (at least three) are drawn having the known position of the gateway as the center L and the estimated distance as radius d.

LoRaWAN Localization

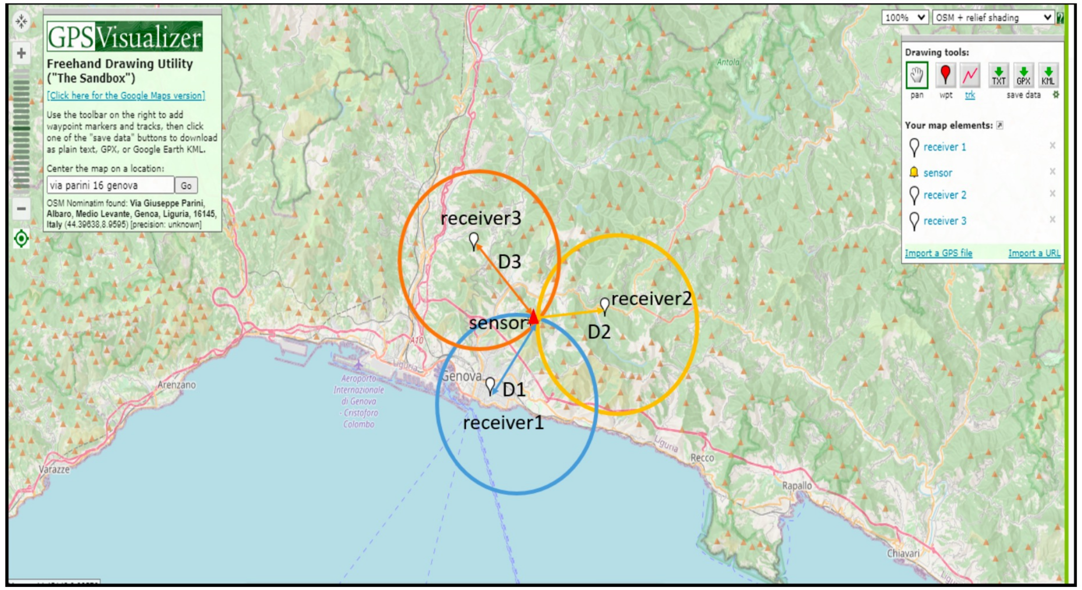
- Having the distance of three different random locations we can create three circles where the center for each circle is the point of measurement
- The point where all the circles intersect each other is the location of **the sensor**



HackInBo Winter 2021 Edition
17ª EDIZIONE

LoRaWAN Localization

- We can use **GPS coordinates** to make the actual calculations
- Depending on the terrain the **accuracy can be variable**
- We had **better results** in **open flat areas**



HackInBo® Winter 2021 Edition
17ª EDIZIONE

LoRaWAN Jammer

The goal here is to **intercept the LoRa traffic** and **create DoS state**

The attack targets to **interrupt the radio signal** coming from the sensor

The gateway will **fail to receive the packet** and **the message will be lost**

LoRaWAN Jammer

- Radio jammers use a powerful signal to **disrupt the demodulation** of the original signal
- That makes them **noisy**
- They are also **uncontrollably disruptive**
- And **easily detectable**

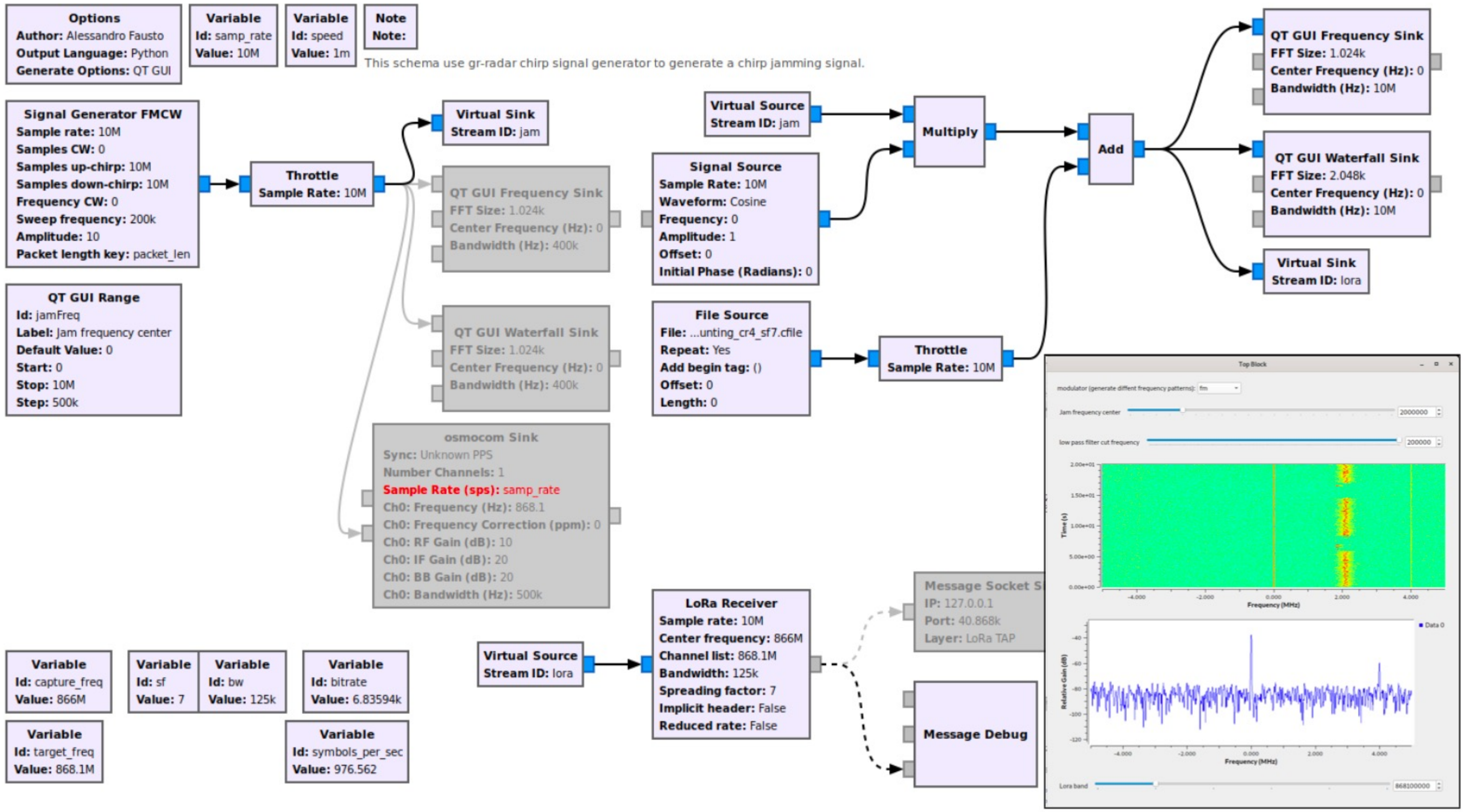
LoRaWAN Jammer

To avoid these issues, we implemented a "selective" jammer

- It activates itself when it detects a LoRa signal and deactivates itself when the transmission is over
- It monitors multiple LoRa channels at the same time to defeat the frequency hoping counter measure
- By activating the jammer during the transmission window, we can destroy part of the lora signal
- This results in invalidating the CRC of the packet. If the packet is even able to be demodulated

LoRaWAN Jammer

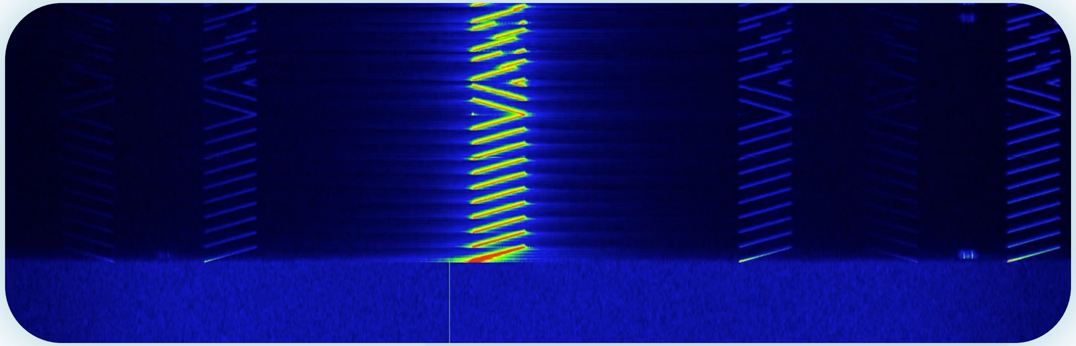
- To implement the jammer, we used a **common SDR with GNU Radio**



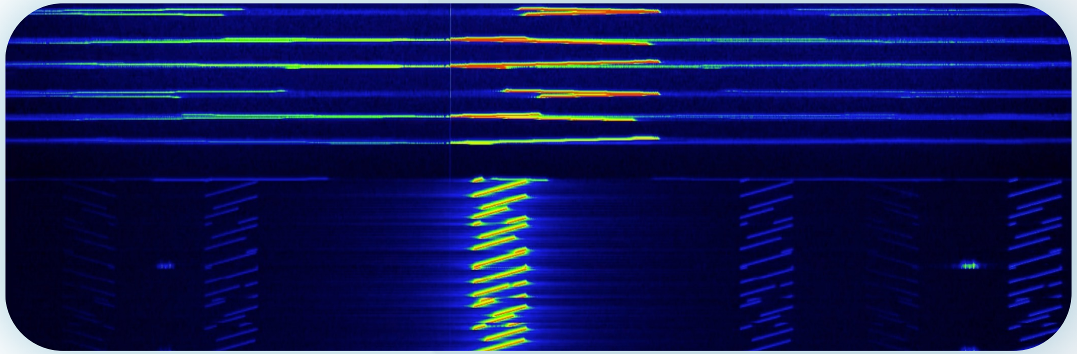
Winter 2021 Edition
17ª EDIZIONE

LoRaWAN Jammer

- The sensor send the LoRa signal. Here we see the start of the transmission:



- The Jammer activates during the transmission sending powerful pulse that distorts the signal



Execution

- Having implemented a method to locate a sensor and a method to disrupt it, now we need **a method to execute**
- LoRa has **several idiosyncrasies** that we must take into consideration
- We need to be able to **transfer a lab experiment to the real world**
- The goal is to **understand the limitations** and **practicalities** of the approach

Execution - Idiosyncrasies

LoRa is a long-range radio technology. That means to locate **the sensor we must be able to move in the order of hundred of meters**

Because of the long distances, **terrain can be a factor in our localization tactic**. Different terrain might impact the value of RSSI giving inaccurate values

Our approaches uses selective jamming. We need to be close to the sensor to be able to get the signal before the gateway is able to demodulate it

HackInBo Winter 2021 Edition
17ª EDIZIONE

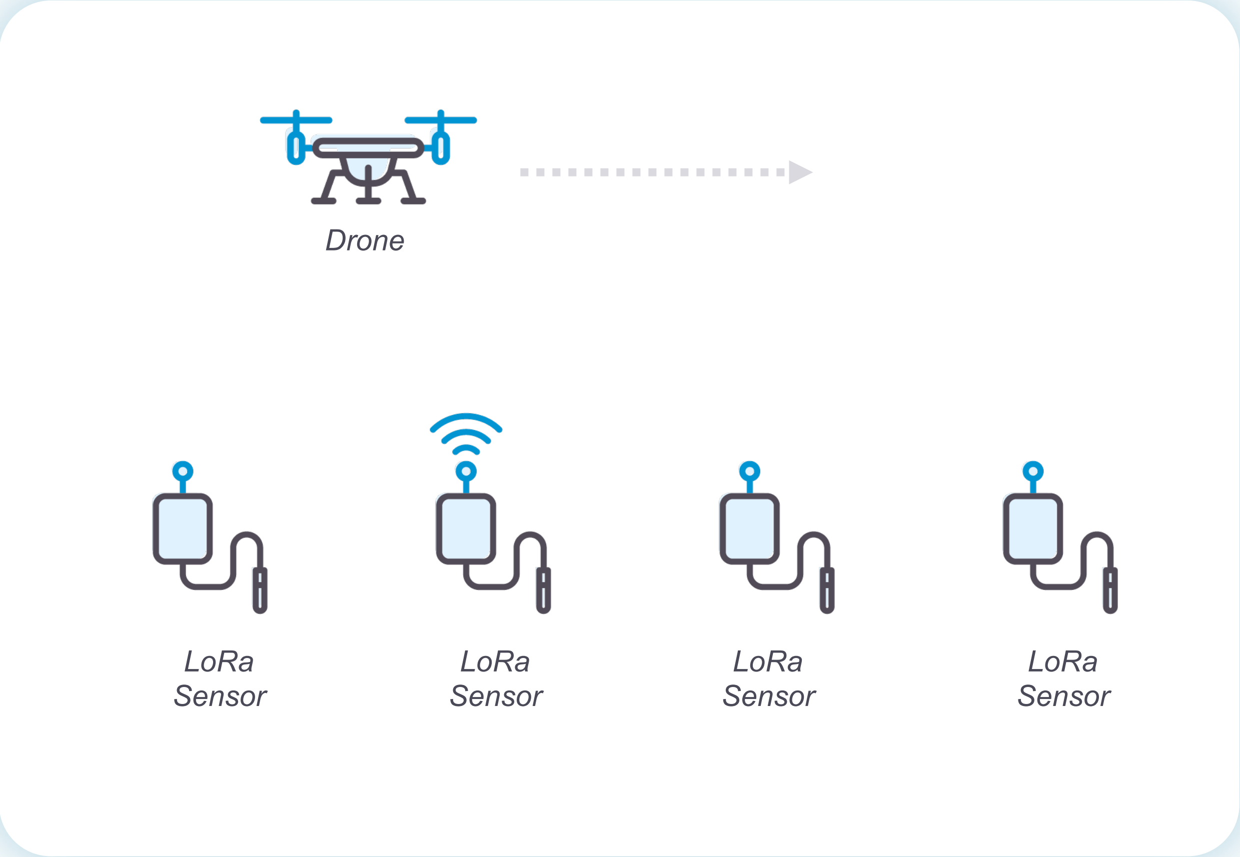
Execution - Drones

- Our solution is to **use drones or other UAV solutions**
- A drone can move in **any terrain**, and it can also **gain adequate altitude to receive the signal**
- The **RSSI can be quite accurate** after a few measurements in the same location by averaging the values

HackInBo Winter 2021 Edition
17ª EDIZIONE

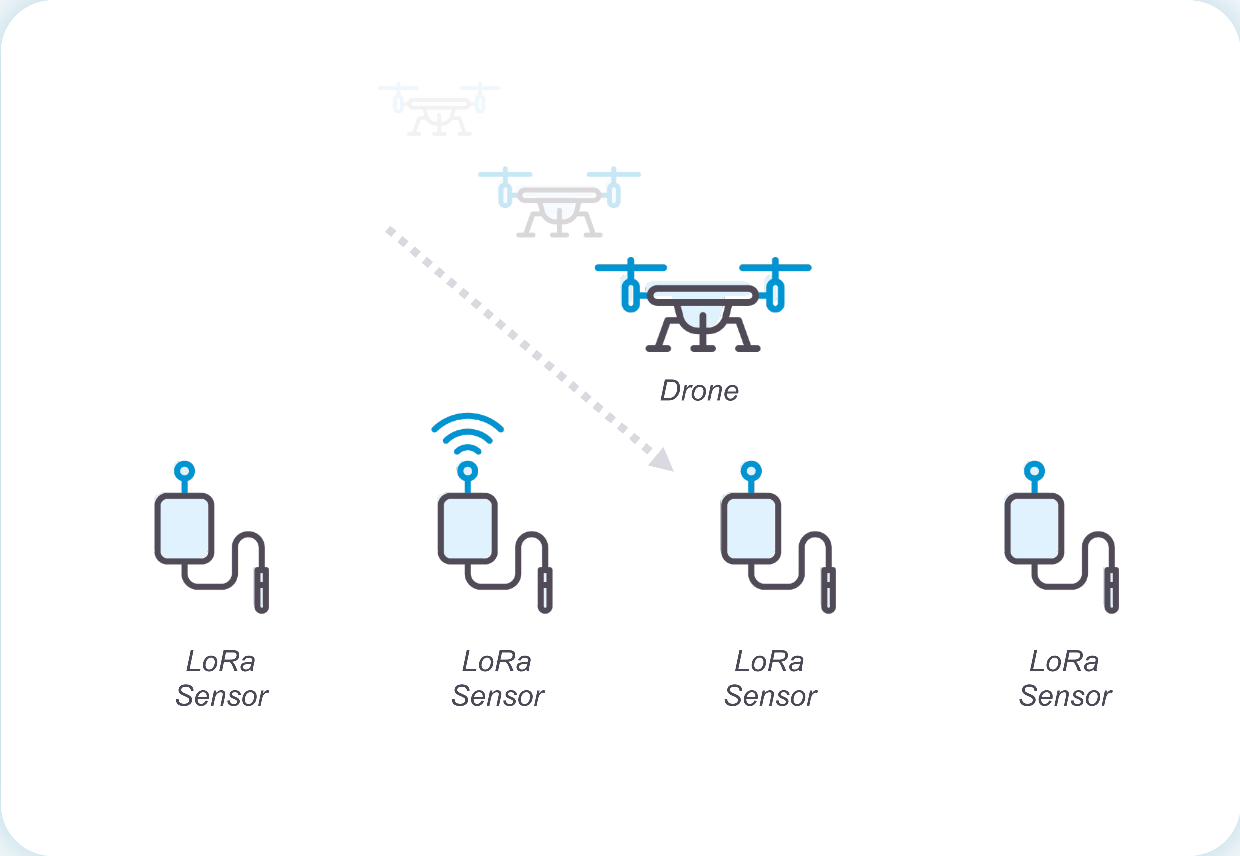
Execution - Localization

- Select a random location **close to the facility**. That could be 10km radius area.
- For a single location **take 4-5 measurements** of the RSSI
- **Move arbitrary** to 2 other locations
- **Calculate** the location of the sensor



Execution - Jamming

- **Approach the sensor** and land into a close location
- Enable **the jamming attack**



HackInBo Winter 2021 Edition
17ª EDIZIONE

Execution - Results

The localization and disruption parts were successful.

- We were able to verify that the advantages of the drone provided better signal detection and RSSI values. Ground measurements were inadequate behind terrain (trees, small cliffs, etc.). Accuracy of the localization tactic can be improved with more advanced techniques like time difference of arrival (TDoA) and others.
- The main limitations were:
  - Weight that the drone can carry and battery life of the drone
  - Legalities considering flying the drone. We needed a pilot while the whole process could be completely automated
- Both limitations are irrelevant from an APT perspective

Takeaways

LoRaWAN is a technology that is **advancing further** into the market

Disruptions can be a possible attack vector

Drone technology can be used to deliver such attacks

The **physical** and **regional security** should be an aspect when deploying such a solution in critical infrastructure

References

1. https://lora-alliance.org/about-lorawan
2. https://iot-analytics.com/5-things-to-know-about-the-lpwan-market-in-2020/

HackInBo Winter 2021 Edition
17ª EDIZIONE