Connected Bus Monitor

Francesco Crinò
Constanta Efros

CONCEPT

Francesco Crinò
Constanta Efros

PROBLEM

- Air Quality on ground transport (Safety issues)
  - Elevated **CO2 concentration** leads to drowsiness, lethargy, fatigue, headaches, breathing problems
  - Higher **Relative Humidity** levels (> 60%) can encourage the growth of mold and mildew. Dust mites, bacteria and fungi all thrive under humid conditions
  - Lower RH levels (< 30%) can cause eye or nose irritation
  - Low RH levels (< 30%) can also lead to increased survival of some viruses, thereby increasing the spread of viral infections
  - Ambient temperature

Francesco Crinò
Constanta Efros

IDEA: BRIEF RECAP

- Monitor ground transport air quality
  - Temperature (°)
  - Relative Humidity (%)
  - CO2 concentrations (ppm)
- Provide aggregated indicators of air quality

Francesco Crinò
Constanta Efros

REQUIREMENTS SPECIFICATION

- The system shall ensure ground transport air quality monitoring as well as a normalized air quality indicator based on
  - Temperature
  - Humidity
  - CO2 concentrations
- The system shall enforce security policies
  - Data Integrity
  - End-device Authentication
  - Data Confidentiality
- The system shall provide updates in a near real-time offset
- The system shall be efficient in terms of energy consumption

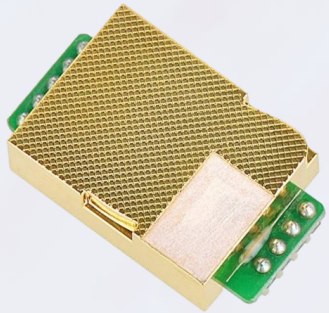
Francesco Crinò
Constanta Efros

HARDWARE
AND
CLOUD BACK-END

24/05/2022

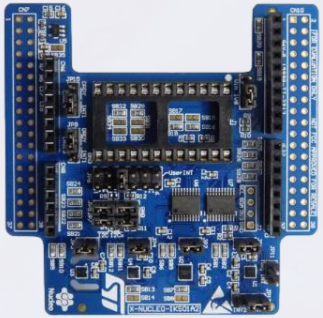
Francesco Crinò
Constanta Efros

HARDWARE COMPONENTS



MH-Z19C:

- Non-Dispersive InfraRed (NDIR) CO2 sensor
- Detection range CO2 [200, 5000] ppm



X-NUCLEO-IKS01A2:

- Motion MEMS and environmental sensor
- HTS221: capacitive digital relative humidity and temperature

Francesco Crinò
Constanta Efros

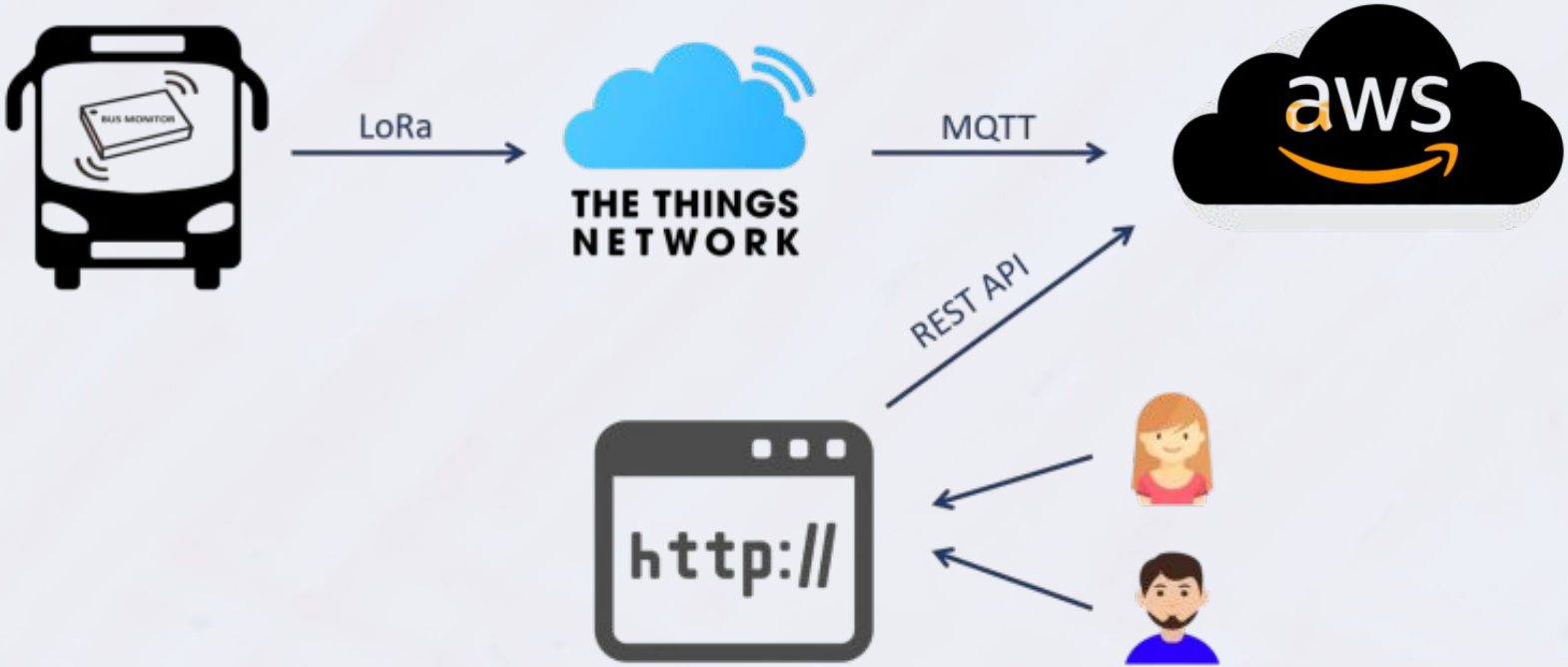
HARDWARE COMPONENTS

B-L072Z-LRWAN1 Discovery kit:

- Embedded ultra-low-power STM32L072CZ MCU, based on Arm® Cortex®-M0
- LoRaWAN™ Class A certified
- LoRa® (+ Sigfox™ compatibility)
- Embedded SX1276 transceiver
- Frequency range: 860 MHz - 930 MHz

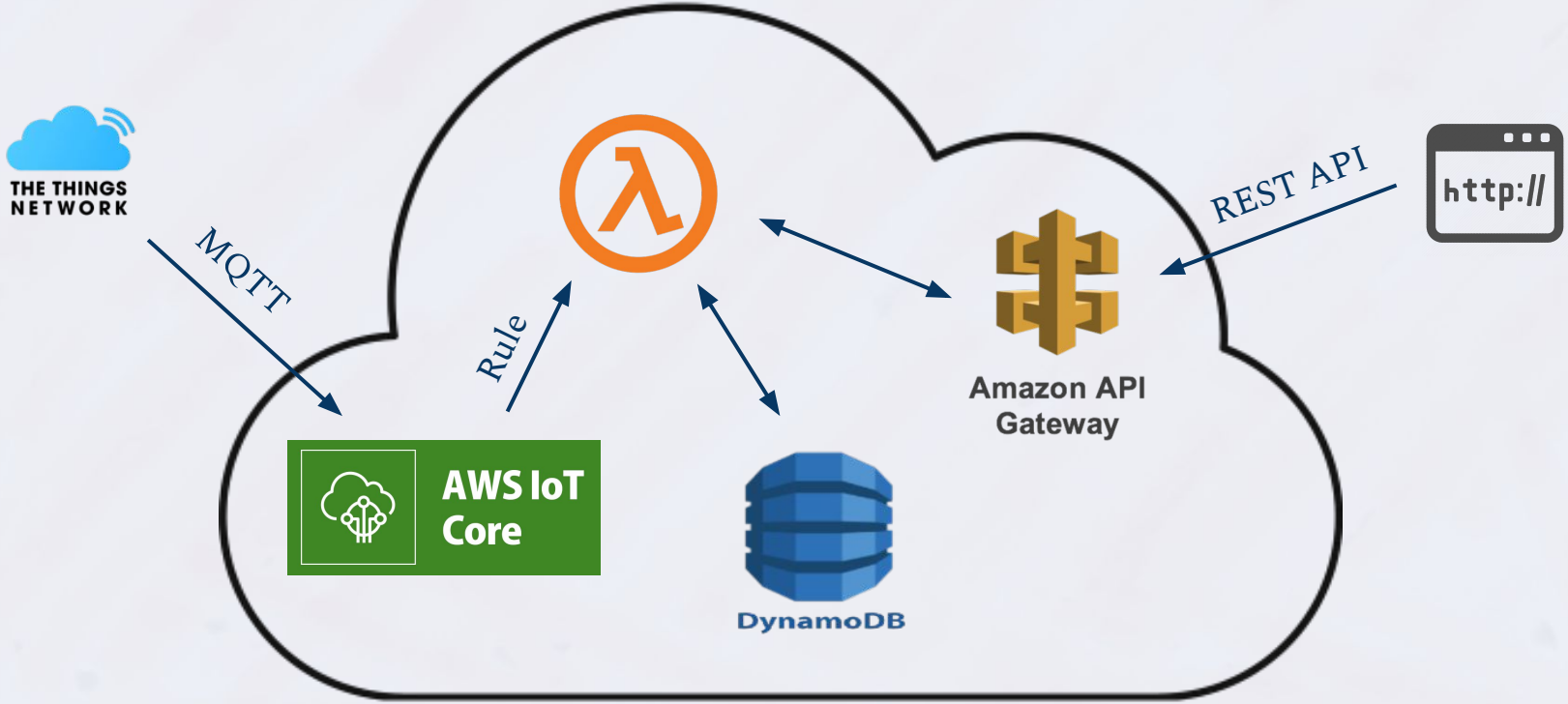
Francesco Crinò
Constanta Efros

ARCHITECTURE



Francesco Crinò
Constanta Efros

CLOUD BACK-END



Francesco Crinò
Constanta Efros

STORE THE DATA

- AWS IoT Core receives the data with topic lorawan/devID/uplink
- A rule sends the incoming message to a lambda function
- Lambda function:
  - get the arrival time of the form Y-m-dTH:M:S
  - computes the timestamp
  - get the payload
    - decodes the payload (base64)
    - decrypts the payload
    - get busID
    - get air parameters

timestamp	bus	date	payload
1653132476	11	2022-05-21T11:27:56	{"humidity": 29.5, "temperature": 31.5, "co2": 400}

Francesco Crinò
Constanta Efros

API GATEWAY

Two APIs are supported: /bus and /bus/id

1. The web page invokes the api and sends a request to the cloud
2. The API Gateway forwards the request to a lambda function
3. The lambda computes and sends back a response
4. The API Gateway forwards the response to the web page

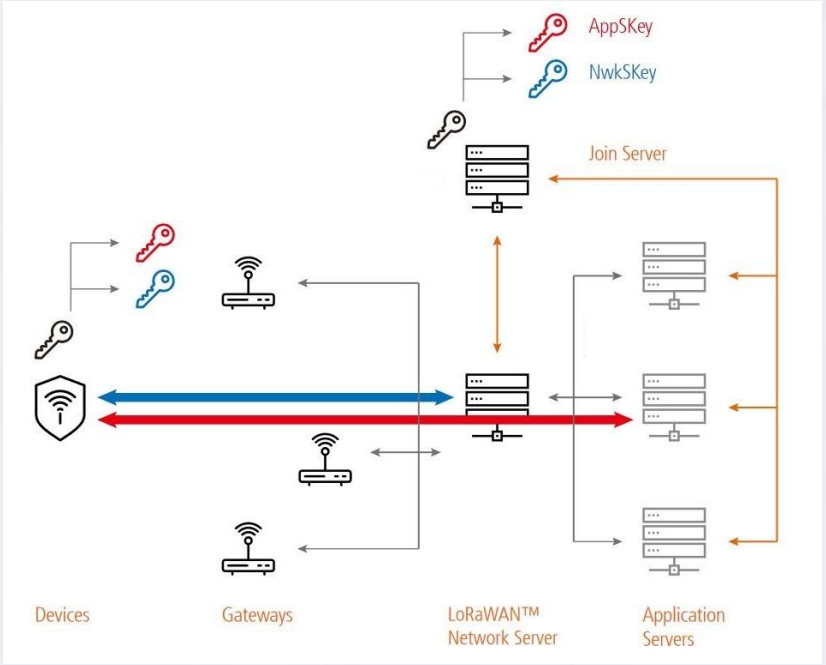
Francesco Crinò
Constanta Efros

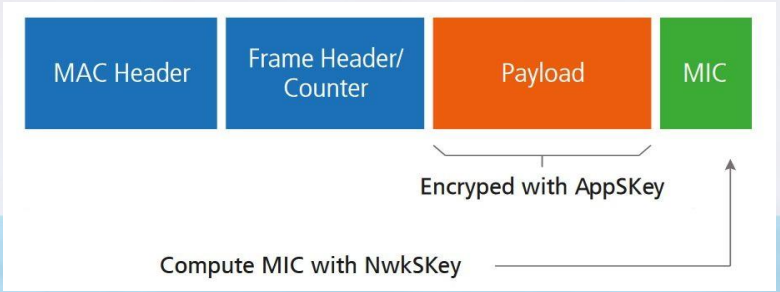
SECURITY

Francesco Crinò
Constanta Efros

LoRaWAN ENCRYPTION

- All LoRaWAN traffic is protected using two session keys.
- The payload is encrypted by AES-CTR and carries a frame counter (to avoid packet replay)
- Message Integrity Code (MIC) computed with AES-CMAC (to avoid packet tampering).





Francesco Crinò
Constanta Efros

LoRaWAN ENCRYPTION

- Over-The-Air Activation

Francesco Crinò
Constanta Efros

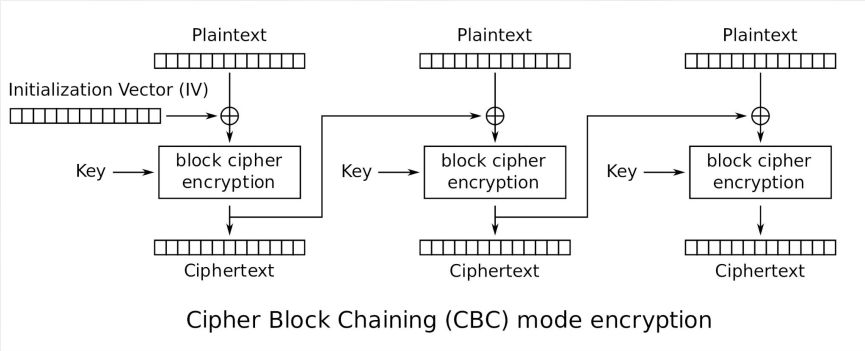
OVERALL SEC

- Bus-TTN is secured by LoRaWAN
- What about TTN-AWS?

Francesco Crinò
Constanta Efros

DATA ENCRYPTION

- To assure confidentiality in all the path bus-aws we encrypt the data using AES-CBC



Cipher Block Chaining (CBC) mode encryption

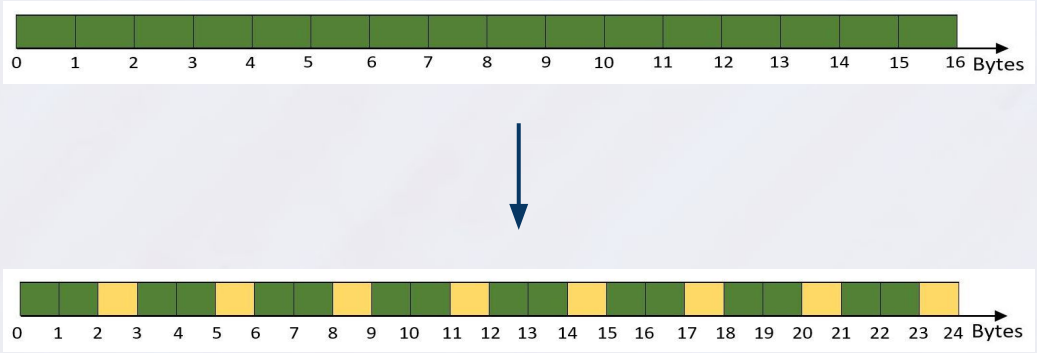
- We need:
  - 16 bytes key
  - 16 bytes IV

- On RIOT:
  - module random to generate random key and IV
  - module crypto to perform AES-128

Francesco Crinò
Constanta Efros

HIDDEN KEY

- In order to let AWS be able to decrypt the message we need to sends the key and the IV
- We can send the IV in clear but protecting the key



AES-128 key

fake AES-192 key

Francesco Crinò
Constanta Efros

ENC PAYLOAD

- The clear payload has dimension between 54 and 60 bytes
- To be encrypted with AES-128 it is padded to 64 bytes
- The encrypted payload to send is 94 bytes long

Francesco Crinò
Constanta Efros

FRONT-END

Francesco Crinò
Constanta Efros

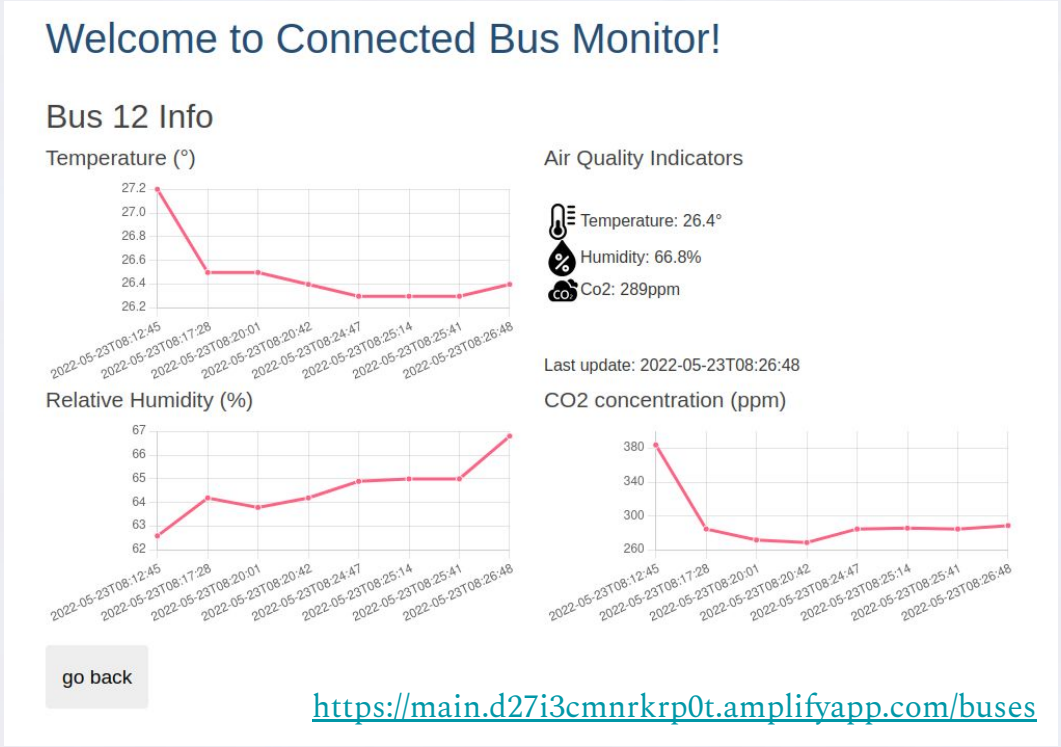
WEB DASHBOARD

Angular application

- ng2-charts

Get bus IDs

Get bus air quality data



https://main.d27i3cmnrkrp0t.amplifyapp.com/buses

Francesco Crinò
Constanta Efros

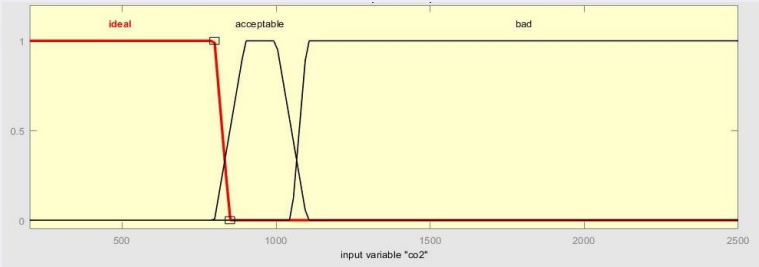
EVALUATION

Francesco Crinò
Constanta Efros

AIR QUALITY INDEX (AQI)

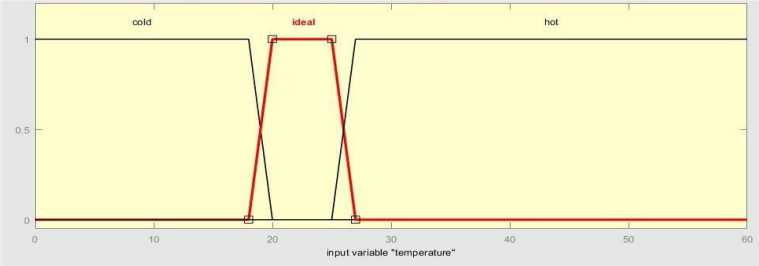
CO2 concentration thresholds [ppm]:

- Ideal: < 800
- acceptable: [800, 1110]
- bad: > 1100



Temperature thresholds [°C]:

- cold: < 20
- ideal: [20, 25]
- hot: > 25

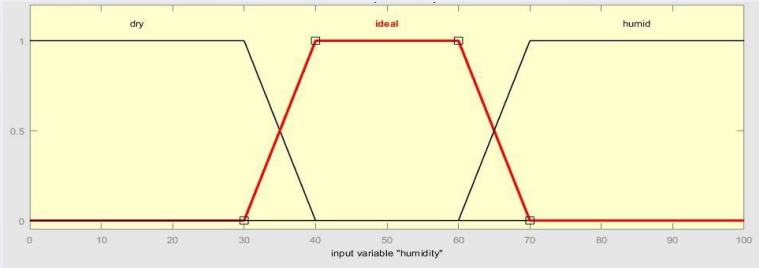


Francesco Crinò
Constanta Efros

AIR QUALITY INDEX (AQI)

Humidity thresholds [%]:

- Dry: < 40
- Ideal: [40, 60]
- Too humid: > 60



First strategy to compute AQI:

- AQI $\in [0, 3]$
- equivalent to the number of parameter in the ideal range

Francesco Crinò
Constanta Efros

AIR QUALITY INDEX (AQI)

Second strategy to compute AQI:

- AQI $\in [0, 3]$
- Normalized contribution of temp and hum

$$hum_{cont} = \begin{cases} 1 & \text{if } hum \in [40, 60] \\ \frac{hum}{40} & \text{if } hum < 40\% \\ \frac{100 - hum}{100 - 60} & \text{if } hum > 60\% \end{cases}$$

$$temp_{cont} = \begin{cases} 1 & \text{if } temp \in [20, 25] \\ \frac{temp - 5}{20 - 5} & \text{if } temp < 20°C \\ \frac{40 - temp}{40 - 25} & \text{if } temp > 25°C \end{cases}$$

$$co2_{cont} = \begin{cases} 0 & \text{if } co2 > 1100ppm \\ 1 & \text{if } co2 \in [200, 1100] \end{cases}$$

Francesco Crinò
Constanta Efros

AIR QUALITY INDEX (AQI)

Lets see the different outcomes of the two methods taking as examples the parameters:

- temp = 34°C
- hum = 21%
- co2 = 227 ppm

AQI with first method = 1
AQI with second method = 1.9

Francesco Crinò
Constanta Efros

SAMPLING FREQUENCY

The sampling frequency is strictly related to the transmission time bus-TTN since we need to respect the 1% duty-cycle.

Reminder: The payload is 94 bytes long

Data rate	Spreading factor	Channel bandwidth	Bit rate	Maximum payload size
0	SF12	125 kHz	250 bps	51 bytes
1	SF11	125 kHz	440 bps	51 bytes
2	SF10	125 kHz	980 bps	51 bytes
3	SF9	125 kHz	1.76 kbps	115 bytes
4	SF8	125 kHz	3.13 kbps	242 bytes
5	SF7	125 kHz	5.47 kbps	242 bytes
6	SF7	250 kHz	11 kbps	242 bytes

$$t_{trans} = \frac{PayloadSize_{bit}}{BitRate}$$

$$= \frac{PayloadSize_{byte} * 8}{BitRate}$$

$$= \frac{94\ bit * 8}{5470\ bit/s} = 0.137\ s$$

Transmission time bus-TTN: t_{trans} = 0.137 seconds

Francesco Crinò
Constanta Efros

SAMPLING FREQUENCY

Respecting the 1% duty-cycle, we can transmit each 14 seconds

Is SF=7 the best to use in our case?

SF	BitRate [Kbit/s]	T_{trans} [s]	Transmission Period [s]	Range[km]
7	5,47	0,137	14	2
8	3,13	0,240	24	4
9	1,76	0,427	43	6

For our purposes it is better to use SF=9:

- The range is tripled
- We can sample each 43 seconds

Francesco Crinò
Constanta Efros

ENERGY CONSUMPTION

All major bus manufacturers foresee the presence of USB ports in the new buses

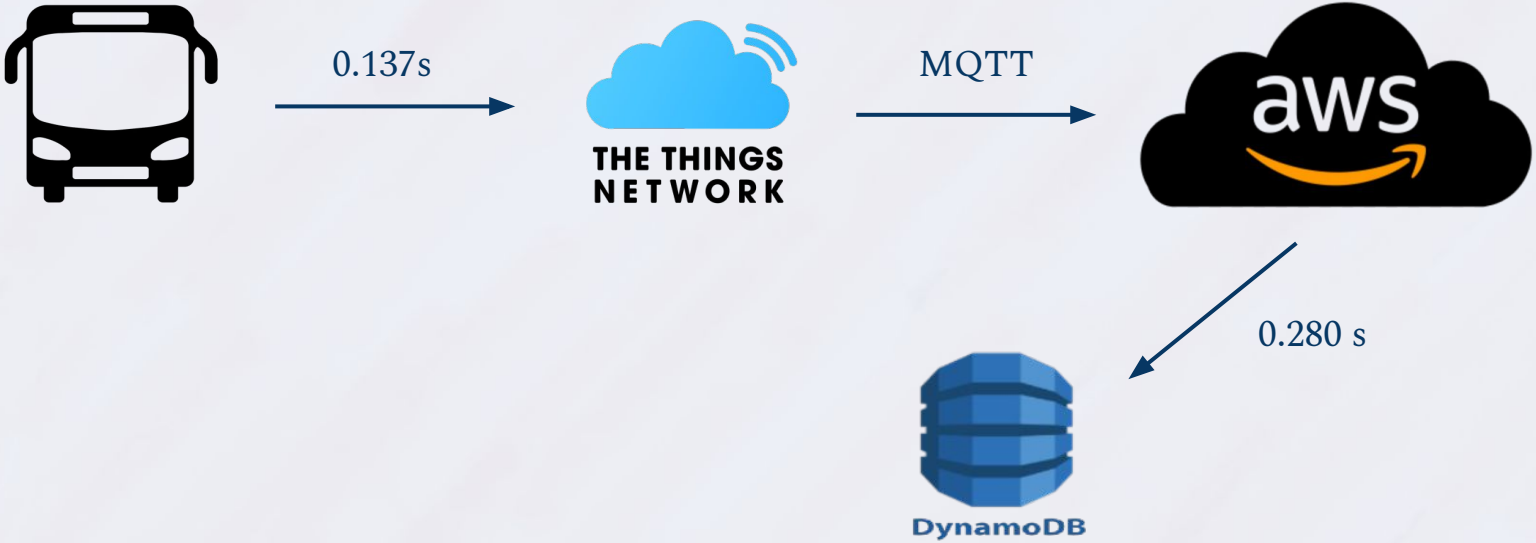
→ The CBM can be plugged to the bus through USB

We wanted to maintain the device on also while the bus is powered off (terminus) to do not re-calibrate the co2 sensor

→ We have experienced that the CO2 sensor takes around 10 minutes to give stable values, that is acceptable for our purposes

Francesco Crinò
Constanta Efros

STORE DELAY



Francesco Crinò
Constanta Efros

FUTURE PLANS

Francesco Crinò
Constanta Efros

POTENTIAL ADDITIONAL HARDWARE

- Exploit the MEMS sensor for supplying data (acceleration and inclination) in order to assess city traffic conditions
- Include a Volatile Organic Compounds (VOC) sensor
- Noise sensor for additional pollution metrics
- Supplement an already existent GPS system combining heterogeneous information

Francesco Crinò
Constanta Efros

POTENTIAL SOFTWARE DEVELOPMENTS

- Analytics
  - Provide an approximation of the number of people onboard
  - Ground transport statistics (conditions, degree of usage)

Francesco Crinò
Constanta Efros

THANKS FOR YOUR ATTENTION

github.com/FrancescoCrino/ConnectedBusMonitor

Francesco Crinò
Constanta Efros