Multi-network Technology Cloud-Based Asset-Tracking Platform for IoT Devices

Francesco Lubrano[1](✉), Davide Sergi[2], Fabrizio Bertone[1], and Olivier Terzo[1]

[1] LINKS Foundation, via Boggio 61, Turin, Italy
{francesco.lubrano,fabrizio.bertone,olivier.terzo}@linksfoundation.com
[2] ST Microelectronics, via Olivetti 2, Agrate Brianza, MB, Italy
davide.sergi@st.com

Abstract. Nowadays a huge number of different devices and sensors generate information of every type. The data collected, even from long distances, can be used to support decision making, prevent losses and maximize asset utilization rates. Thus, the possibility to track assets is getting attention and raising interest worldwide. The heterogeneity of such sensors as well as the multitude of different application fields led to the development of new communication protocols, network technologies and low-power connected devices. This wide range of possibilities introduces the need to integrate in a unique platform the provisioning and management of different device types as well as data ingestion mechanisms, ensuring security and data segregation. Moreover, the need to accommodate the growing demand to provide ready-to-use solutions is leading to the development of adapters and interoperable platforms that can communicate with each others. This paper presents an analysis of some of the most common wireless technologies used by low-power connected devices and describes a cloud-based platform that integrates different device types and network providers. The aim of the proposed platform is to provide a unique interface for the user, through which he can manage connected devices and visualize data coming from them, regardless of their network technology.

1 Introduction

Nowadays the wide spread of IoT devices is changing our lives. New paradigms such as smart buildings, smart cities, smart agriculture, etc. rely on a huge number of sensors and connected devices that communicate with each others and send data into centralised or distributed platforms or network servers. Currently, IoT devices leverage on different network technologies to transmit data and this depends on diverse connectivity requirements in terms of range, data throughput, energy efficiency and cost. Focusing on energy, the overall consumption of an IoT device is greatly influenced by the technology used for transmitting data [1,2]. Indeed, the transmitter state, the network overhead, the power needed to receive and transmit data are characteristics of primary importance to ensure energy efficiency and decrease power consumption. Taking into account the general scenario of asset-tracking it is clear that depending on the specific use

L. Barolli et al. (Eds.): CISIS 2020, AISC 1194, pp. 344–354, 2021.
https://doi.org/10.1007/978-3-030-50454-0_33

case there are different needs in terms of communication and therefore of power consumption. In several use cases, such as smart building or home automation, there is a energy source that can be considered unlimited. In this cases a high energy efficiency and long range are of secondary importance and often network technologies like WiFi [4] or Bluetooth LE [5] are chosen [3]. On the contrary, other scenarios such as smart agriculture have more strict requirements regarding power consumption. In this use case, it's common to have low power devices relying on batteries to sense and communicate. This forces the use of low power communication technologies, such as Low-Power Wide-Area Network (LPWAN) [7], Near-Field Communication (NFC) or Radio-frequency Identification (RFID) [6], depending on the range required by the use case.

Just by looking at the two example provided, it is clear that there is a big number of alternatives concerning how devices can communicate and this lead to a big number of applications and platforms a user might use to interface with his devices. Aiming to provide a unique interface for the user to manage his devices, this paper presents the work done to develop a cloud-based platform and an application front-end able to manage devices that communicate with different technologies, from WiFi to LPWAN networks.

2 State-of-the-Art

This section provides a description of actual technologies implied in IoT, with a focus on two of the most widespread LPWAN networks: Sigfox [8] and LoRa [9]. Figure 1 provides a comparison of networks largely used in IoT. Networks are compared by their range, their bit rate and their cost. While technologies like RFID or NFC provide a moderate bit rate at the expense of the range, that is quite low (centimeters in the case of NFC), LPWAN networks provide long range communication with an extremely low throughput. WiFi and cellular networks ensure a high range and high bit rate, but in these cases the cost of the device in terms of money as well as its power consumption is really significant. In the middle, there is a compromise among range, bit rate and cost, represented by BLE and Zigbee [12].

2.1 Cellular Networks

Cellular networks or mobile networks are almost omnipresent in urban environment. This type of network offers a reliable broadband communication, enough to support video streaming applications besides classical voice calls. Despite the widespread of these networks, they are not the most suitable for IoT battery-powered devices, because of the high power consumption of the communications but they are viable for some specific use cases. The high throughput and pervasive presence of such networks are requirements for application like connected vehicles, traffic routing, advanced driver assistance systems (ADAS), etc. The 5G, next-gen of mobile networks, will have an important impact on IoT. Ensuring ultra-low latency, 5G is considered an enabling technology for several use cases with real-time requirements.

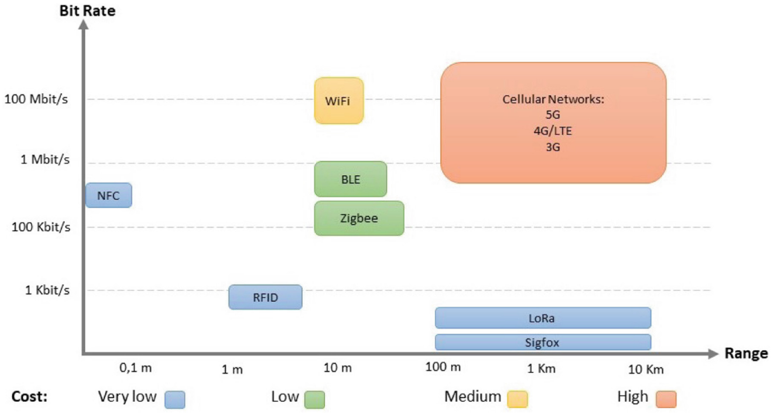


Fig. 1. Network technologies comparison

2.2 Low-Power WAN (LPWAN)

LPWANs are wireless networks designed to allow low-power and long-range communications among connected devices such as sensors, typically operated on a battery. LPWAN networks are based on distributed gateways, that receive messages by the devices and provide them to users. A LPWAN may be a private wireless sensor network, but nowadays multiple providers offer LPWAN as a service, allowing end users to deploy their devices in the field without investing in infrastructure. Two of the most popular LPWAN technologies are Sigfox and LoRa. Both of them use unlicensed ISM radio bands to transmit messages, typically centered on 868 MHz or 915 MHz. ISM bands usage is generally regulated and limited by specific set of rules (e.g [15] in Europe and [16] in the USA).

2.2.1 Sigfox

Sigfox is the name of a global LPWAN network-and the corresponding owner company- that covers a fair portion of the inhabited lands, especially in Europe, including at the time writing about 70 Countries and counting. Coverage is provided by licensed operators that deploy base stations on the territory and the access to the network requires the payment of a periodic fee.

Sigfox uses Ultra NarrowBand (UNB) techniques to transmit information [17]. As the name suggests, UNB concentrates the power on a very narrow band (100 Hz), allowing good resilience to interference even at far distances of reception, with an efficient energy usage. The protocol does not provide medium access control mechanisms in order to reduce complexity on the device, hence saving battery. The consequence is that multiple devices can transmit at the same time without coordination. In order to increase the chances of correct reception and avoid collisions between the transmissions of different devices, the same message is sent three times in a short sequence, centered on a different pseudo-random radio frequency each time (frequency hopping). Sigfox protocol uses Differential Binary Phase-Shift Keying (DBPSK) modulation for its radio communications.

The available payload for each message is limited to 12 bytes, while an additional 12 bytes header includes the device ID and other metadata. Communication can be bi-directional (i.e. devices can receive control messages from the network), but it is necessarily initialized by the device itself, so that for the most of time it is in sleep-mode (i.e. it does not listen to the network).

When base stations receive a message, they forward it to the Sigfox Cloud, a centralized cloud service that handles the whole Sigfox network. Customers can connect their IT infrastructure to the Sigfox cloud in order to manage messages and devices. This is done by implementing callbacks and REST APIs, in order to process received messages and administrate the devices' fleet [18].

2.2.2 LoRa and LoRaWAN

LoRa - Long Range
LoRa is the physical layer or the wireless modulation utilized to create the long range communication link. It is based on chirp spread spectrum modulation ensuring low power long range transmissions [13]. The device transmission frequency depends of the regional spectrum allocations and regulatory requirements adopted.

LoRaWAN - Long Range WAN
LoRaWAN is a LPWAN completely designed to optimize battery lifetime, network bandwidth, communication range, and cost, accommodating needs of sensors and applications that send asynchronously small amounts of data over long distances a few times per hour from varying environments [10].

LoRaWAN defines the communication protocol and system architecture for the network where the nodes are not associated with a specific gateway. In fact, data sent by a node are typically received by multiple gateways which will forward the received packet from to the cloud-based network server via cellular, Ethernet, satellite or Wi-Fi. The network server will be responsible for filtering redundant received packets, performing security checks and eventually forwarding them to the application server (Fig. 2).

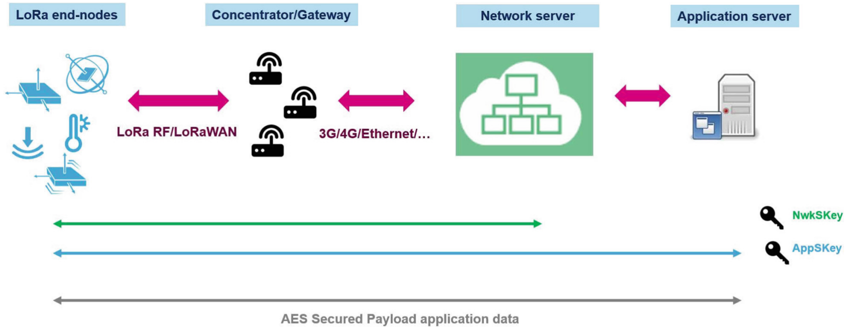


Fig. 2. LoRaWAN network: architecture and security

In a LoRaWAN network there are three device classes - A, B and C - which define how network server and end-node perform downlink communication. These classes are designed to fit end-nodes requirements in terms of power consumption.

In terms of network security, LoRaWAN uses two types of symmetric key, typically unique for each device: the network session key (NwkSkey) and the application session key (AppSkey). The NwkSkey provides data integrity between end-node and network server, while AppSkey provides data confidentiality among end-nodes and the application server [10].

End-nodes get these keys through a process called *join*. Two different procedures can be identified for this process:

- *OTAA (Over-the-Air-Activation)*: end-node and network server derive session keys starting from a pre-shared key called AppKey;
- *APB (Activation by Personalization)*: session keys are set manually by the user in both end-node and network server side.

Although a user could decide to implement its own network server, there are many public cloud hosted network servers that can handle the management of gateways, end-nodes and data. Examples of these network service provider are TTN[1], Loriot.io[2], MachineQ[3], etc.

All of these provides similar features, enabling users to integrate custom applications, cloud hosted or on-premises.

2.2.3 A Comparison Among Sigfox and LoRa Transmissions

As described in previous sections, LoRa and Sigfox have two different approach for transmitting data. LoRa signal is based on chirp spread spectrum modulation while Sigfox use Ultra Narrow Band techniques to transmit information. The simplified graph, depicted in Fig. 3, shows the difference among these two different approach. Sigfox emission is concentrated in a really small bandwidth and in the graph it appears like a spike. Instead, in LoRa the signal requires more bandwidth.

2.3 NFC - Near-Field Communication

Near-field communication (NFC) is a protocol for P2P wireless device communication over a distance of the order of centimeters [11]. It offers a low-speed connection (around 0.5 Mbps) that can be used to carry out from the simplest applications such as small files sharing and device configuration, to the most complex such as contactless payment.

NFC is based on Radio-frequency identification (RFID), a technology that leveraging on electromagnetic fields can identify and track the so called tags,

[1] https://www.thethingsnetwork.org/.

[2] https://www.loriot.io/.

[3] https://machineq.com/.

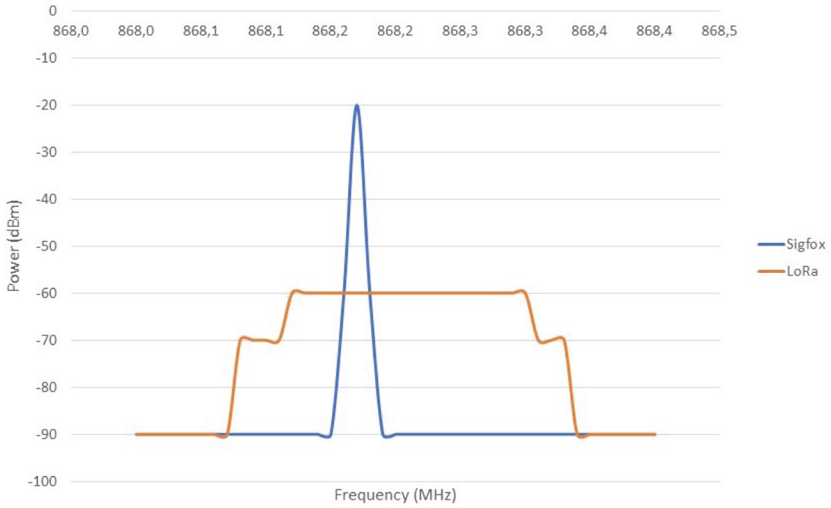


Fig. 3. Comparison among Sigfox and LoRa signal emissions

often attached to objects. Tags are simply tiny transponders, that can receive and transmit radio signals. To read the content of a tag, the reader generates a electromagnetic pulse, triggering the tag that transmits its identification and other information to the reader. It can be identified three different tag types based on the power source:

- *Passive*: powered by energy from the RFID reader's interrogating radio waves;
- *Battery-assisted passive*: has a small battery on board and is activated when in the presence of an RFID reader;
- *Active*: powered by a battery and thus can be read at a greater range from the RFID reader (up to hundreds of meters).

Tags can also be read-only, the information is written at building time, or can be rewritable, where object-specific data can be written into the tag by the user. Field programmable tags may be wrote once and read multiple times; blank tags may be written with an electronic product code by the user.

3 Asset Tracking Platform

The asset tracking platform is a cloud application based on AWS services[4] that allows users to collect, visualize and analyze data streamed by IP and no-IP devices tailored to monitor environmental condition and to perform geo-tracking in a centralized way. The heart of the asset-tracking platform is deployed through AWS services involving computation, storage, data management, networking,

[4] https://aws.amazon.com/.

development tools, monitoring, security, notification services, and so on, for a fully functional asset-tracking application. The asset-tracking dashboard is the graphical browser interface through which user can monitor and control the status and the activity of his devices and analyze incoming data.

3.1 Architecture

The end-to-end solution from user devices to web dashboard used to provision and monitor devices is depicted in the Fig. 4.

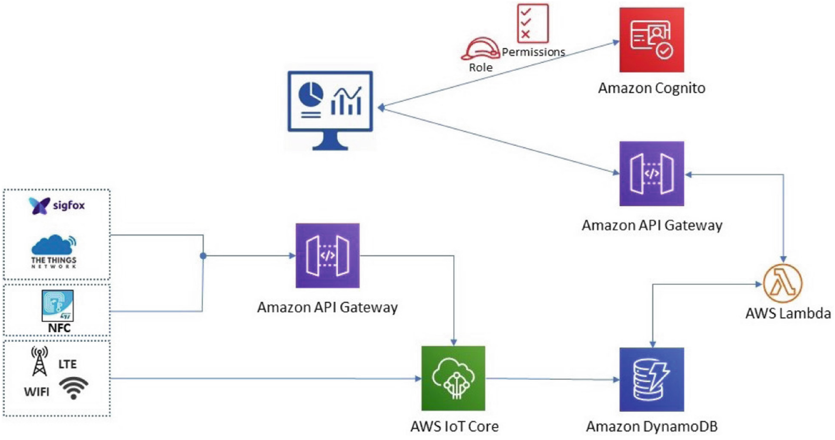


Fig. 4. Asset tracking platform architecture

Devices able to communicate through WI-FI or mobile networks, can directly send data to the AWS IoT Core using MQTT protocol. Such devices authenticate themselves through X.509 certificates [14]. While WI-FI and LTE devices can communicate directly on IP networks with the AWS IoT Core, no-IP devices require a third party, acting as an intermediate operator, that can receive data from devices and re-transmit them via Internet. In the asset tracking platform, Sigfox and LoRa network server providers are the central hub where messages and information from devices are stored. Both operators allow to create a link among network operators and the asset-tracking dashboard platform using the common network protocols available (e.g. HTTP). Indeed, in the case of devices that use a LPWAN network to communicate, there is an adapter layer made by express API developed through the AWS API Gateway. This API allows network servers to send data coming from physical devices via HTTP. This API is secured by using a pre-shared secret, generated as token by the dashboard at device registration time and it is set in the integration function on the network service provider side.

Finally, the asset-tracking platform supports NFC devices. In this case, the end-user reads the data collected over time by the device and send them directly to the cloud dashboard through the ST NFC Sensor application. User must authenticate itself through mobile app before proceeding to send data.

Leveraging on AWS cross-service features, the API gateway can automatically republish messages into the MQTT Broker implemented in the AWS IoT Core service. Thanks to this behaviour, all the device data are concentrated on the AWS IoT Core and the same policies apply. If policies are satisfied, data are stored in a document-oriented database. Once data are stored, through a dedicated API, the user can retrieve his data using the dashboard.

3.2 Devices: Hardware and Software

The physical devices used to develop and test the asset-tracking platform are STM32 Nucleo development boards combined with X-NUCLEO expansion boards and running Function Packs stack as firmware. STM32 ODE Function Packs are set of function examples developed within the Open Development Environment (ODE)[5], a development environment offered by STMicroelectronics[6], for the realization and prototyping of applications based on the STM32 family of 32-bit microcontrollers. These microcontrollers, combined with other ST components state-of-the-art connected by means of expansion boards, allow to realize most common application cases built by leveraging the modularity and interoperability of STM32 Nucleo development boards and expansions.

LPWAN devices involved within the asset-tracing platform, runs the FP-ATR-LORA1 and the FP-ATR-SIGFOX1 Function Packs. These software have been designed specifically for asset-tracking and fleet management purposes and are capable to get data from environmental and motion sensors, retrieve geo-position from GNSS and send collected data via LoRaWAN and Sigfox connectivity. The packages implements low power profiles and related transitions to ensure long battery autonomy.

Regarding the NFC device, FP-SNS-SMARTAG1 has been used. Coupled with a NFC enabled reader such as a mobile phone or a tablet and the NFC Sensor mobile application, developed by ST, it provides motion and environmental sensor data. This package supports energy harvesting (enabled by NFC) and battery operated use cases.

4 Asset-Tracking Dashboard

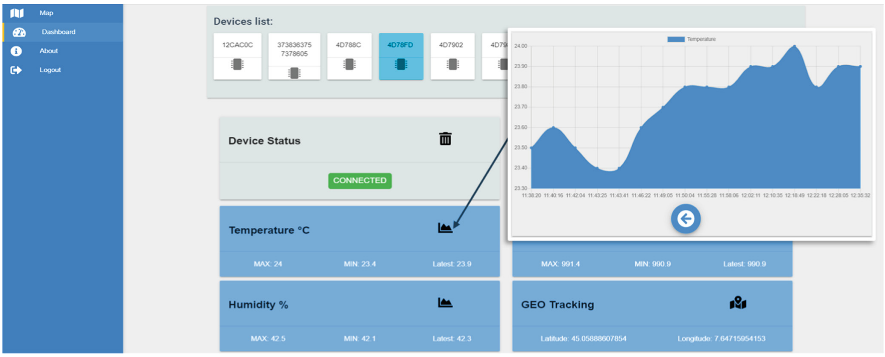
As described in the previous sections, the asset-tracking cloud platform mainly acts as a concentrator for data coming from different devices. Such data are standardized in a unique data model inside the database and can be accessed through appropriate APIs by the asset-tracking web dashboard. This dashboard is an interface that provides several features ranging from provisioning, management and deletion of devices, to the visualisation of device data, position

[5] https://www.st.com/en/ecosystems/stm32-open-development-environment.html.
[6] https://www.st.com/.

and events. Furthermore, the dashboard has a dedicated section that provides all the needed information to create a device, depending on its communication technology.

Users can access or register a new account through the dashboard, proper configured to interact with the AWS Cognito service, that manages user accounts, authentication flow and user rights.

Once the user logged-in, the dashboard shows all the devices belonging to that user in a map, reporting the last position of each device. This main page can be considered as a global dashboard where the user can control the position and the status of all the device he owns in a single view.



Device Status

CONNECTED

Temperature °C

MAX: 24 MIN: 23.4 Latest: 23.9

MAX: 991.4 MIN: 990.9 Latest: 990.9

Humidity %

MAX: 42.5 MIN: 42.1 Latest: 42.3

GEO Tracking

Latitude: 45.05888607854 Longitude: 7.64715954153

Fig. 5. Asset tracking dashboard

As depicted in Fig. 5, the asset-tracking dashboard implements a second view, where the user can check all the information coming from his devices. In this view there are several cards that provide through graphs information related to the temperature, humidity and pressure data reported by each device. One of this cards is dedicated to the device positions. It reports, for a time frame inserted by the user, the positions of the devices and its interpolated path in a map. Regarding the asset-tracking, this feature is crucial because it allows to track the position of the device in the time, understanding its path. Finally, there is a card devoted to the event management, in which are reported all the events sent by the device, such as wake up, MEMS event and tilt event. Users can also set several thresholds, such as a maximum temperature, that when exceeded raises events displayed as notifications in the dashboard.

5 Conclusions

The wide-spread of IoT devices and their heterogeneity is a clear challenge for their management in the future and this work aims to tackle it, presenting a cloud-based platform capable to aggregate different network technologies and device types. At the same time the asset-tracking platform, leveraging on a customised dashboard and on external APIs, aims at providing an easy interface, through which users can provision and manage their devices. Considering the asset-tracking scenario, that involves a huge number of different use cases, the asset-tracking platform can be considered a starting point for a centralised management of this type of devices and will be extended to support other devices and other network technologies, providing at the same time easy to use. A modular and adaptive graphic user interface, automatic device provisioning, wide support to most used network server providers and heterogeneous devices are the challenges that we are facing to provide a comprehensive platform for asset-tracking.

References

1. Mahmoud, M., Auday, M.: A study of efficient power consumption wireless communication techniques modules for internet of things (IoT) applications. Adv. Internet Things (2016). https://doi.org/10.4236/ait.2016.62002
2. Gray, C., Ayre, R., Hinton, K., Tucker, R.S.: Power consumption of IoT access network technologies. In: 2015 IEEE International Conference on Communication Workshop (ICCW), London, pp. 2818–2823 (2015)
3. Samuel, S.S.I.: A review of connectivity challenges in IoT-smart home. In: 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), Muscat, pp. 1–4 (2016)
4. IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, in IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012), pp.1–3534, 14 December 2016
5. Heydon, R., Hunn, N.: Bluetooth low energy. CSR Presentation, Bluetooth SIG (2012). https://www.bluetooth.org/DocMan/handlers/DownloadDoc.ashx
6. Want, R.: Near field communication. IEEE Pervasive Comput. **10**(3), 4–7 (2011)
7. Farrell, S.: Low-power wide area network (LPWAN) overview. IEEE (2018). https://buildbot.tools.ietf.org/html/rfc8376
8. Zuniga, J.C., Ponsard, B.: Sigfox system description. LPWAN@IETF97, 14th–25 November (2016)
9. Sornin, N., et al.: Lorawan Specification. LoRa Alliance (2015)
10. A Technical overview of LoRa® and LoRaWAN^{TM}, Technical Marketing Workgroup 1.0 (2015)
11. Faulkner, C.: What is NFC? Everything you need to know. Techradar.com. Accessed 30 Nov 2015
12. Gislason, D.: Zigbee Wireless Networking. Newnes (2008)
13. Reynders, B., Pollin, S.: Chirp spread spectrum as a modulation technique for long range communication. In: Symposium on Communications and Vehicular Technologies (SCVT), Mons, pp. 1–5 (2016)
14. Myers, M., Adams, C., Solo, D., Kemp, D.: Internet X. 509 certificate request message format. Request for Comments, 2511 (1999)
15. European Commission: Commission Implementing Decision (EU) 2017/1483 (2017)

16. Federal Communications Commission: Code of Federal Regulations Title 47 (Telecommunication) Part 15: RADIO FREQUENCY DEVICES - § 15.247 - Operation within the bands 902-928 MHz, 2400-2483.5 MHz, and 5725-5850 MHz
17. Sigfox connected objects: radio specifications. In: Sigfox Device Radio Specifications. https://build.sigfox.com/sigfox-device-radio-specifications. Cited 30 Mar 2020
18. Sigfox Cloud Integration. https://build.sigfox.com/backend-callbacks-and-api. Cited 30 Mar 2020