VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Arttu Myllyniemi

NB-IOT AND LORA TECHNOLOGY EVALUATION AND PROTOTYPE IMPLEMENTATION

Technology and Communication
2020

VAASAN AMMATTIKORKEAKOULU
Tietotekniikka

TIIVISTELMÄ

Tekijä	Arttu Myllyniemi
Opinnäytetyön nimi	NB-IoT and LoRa Technology Evaluation and Prototype Implementation
Vuosi	2020
Kieli	englanti
Sivumäärä	30 + 1 Liite
Ohjaaja	Jukka Matila

Tämä opinnäytetyö tehtiin Wapice Oy:lle yhtiön sisäisenä tutkimusprojektina. Tämän opinnäytetyön tarkoituksena oli vertailla NB-IoT ja LoRa LPWAN-tekniikoita ja toteuttaa löydösten perusteella prototyyppi valittua tekniikka hyödyntäen.

Tekniikoiden vertailussa hyödynnettiin niiden spesifikaatioita ja aikaisempien tutkimuksien tuloksia.

Prototyyppi päätettiin toteuttaa käyttäen NB-IoT-tekniikkaa ja sen toteutuksessa hyödynnettiin Wapicen aikaisempaa Wi-Fi prototyyppiä. Suurin osa alussa suunnitelluista toiminnallisuuksista saatiin toteutettua onnistuneesti tämän opinnäytetyön aikana.

Wapice voi tulevaisuudessa hyödyntää tässä lopputyössä saatuja tuloksia uusien IoT-laitteiden kehittämisessä. Prototyypin kehitys jatkuu tämän opinnäytetyön jälkeen puuttuvien toiminnallisuuksien toteuttamisella.

Avainsanat IoT, LPWAN, NB-IoT ja LoRa

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Tietotekniikka

ABSTRACT

Author	Arttu Myllyniemi
Title	NB-IoT and LoRa Technology Evaluation and Prototype Implementation
Year	2020
Language	English
Pages	30 + 1 Appendix
Name of Supervisor	Jukka Matila

This thesis was done for Wapice Ltd as the company's internal research project. The purpose of this thesis was to compare NB-IoT and LoRa low-power wide-area network technologies and based on the findings implement a prototype using one of them. The outcomes of this thesis can be employed when developing future IoT applications.

The comparison between the technologies was done by combining data from specifications and earlier studies on the matter.

It was decided to implement the prototype using NB-IoT technology. An earlier Wapice Wi-Fi prototype was utilized in the making of the NB-IoT prototype. Most of the initially planned functionality was successfully implemented during this thesis.

The prototype will be developed further to implement the missing functionalities.

Keywords IoT, LPWAN, NB-IoT and LoRa

TABLE OF CONTENTS

TIIVISTELMÄ
ABSTRACT
1 INTRODUCTION 9
2 TECHNOLOGIES 11
2.1 LoRaWAN 11
2.1.1 LoRa Physical Layer 11
2.1.2 LoRaWAN Link Layer 11
2.2 Cellular for IoT 13
2.2.1 GSM – 4G LTE 13
2.2.2 3GPP Releases 13 – 15 13
2.2.3 NB-IoT 14
2.3 MQTT 16
2.4 Zephyr RTOS 17
3 TECHNOLOGY EVALUATION 18
3.1 Security 18
3.2 Range & Device Capacity 18
3.3 Power Consumption 20
3.4 Latency & Data Rate 21
4 PROTOTYPING 23
4.1 LPWAN Technology Selection 23
4.2 Modem Selection 23
4.3 Development Board 24
4.4 Zephyr 25
4.5 Implementation 25
4.6 Setbacks 28
5 CONCLUSIONS & FUTURE WORK 30
REFERENCES 31

APPENDICES

LIST OF FIGURES AND TABLES

Figure 1. NB-IoT “stand-alone” deployment. /9/ 15
Figure 2. NB-IoT “in-band” and “guard-band” deployments. /10/ 16
Figure 3. LTE IoT 2 Click expansion board by MikroElektronika /23/ 24
Figure 4. STM32 NUCLEO-F411RE development board /24/ 24
Figure 5. Zephyr IoT prototype 25
Figure 6. Zephyr modem driver connection procedure 26
Figure 7. Zephyr IoT-Ticket client MQTT publish procedure 28
Figure 8. IoT-Ticket prototype program flow 28

Table 1. Comparison of 3GPP Release 13 RAT features. /9, 10, 12/ 14

LIST OF APPENDICES

APPENDIX 1. Zephyr network stack architecture

GLOSSARY

IoT	Internet of Things
LPWAN	Low-Power Wide-Area Network
NB-IoT	Narrowband Internet of Things
LoRa	Long Range
ARM	Advanced RISC Machine
CSS	Chirp Spread Spectrum
ISM	Industrial, Scientific and Medical
ETSI	European Telecommunications Standards Institute
3GPP	3rd Generation Partnership Project
RAT	Radio Access Technology
GSM	Global System for Mobile Communications
4G LTE	4th Generation Long Term Evolution
5G NR	5th Generation New Radio
ISP	Internet Service Provider
FDD	Frequency Division Duplex
TDD	Time Division Duplex
MCL	Maximum Coupling Loss
PRB	Physical Resource Block
SMS	Short Message Service

GPIO	General Purpose I/O
TCP	Transmission Control Protocol
TLS	Transport Layer Security
MQTT	Message Queuing Telemetry Transport
HTTP	Hypertext Transfer Protocol
QoS	Quality of Service
RTOS	Real-Time Operating System
OS	Operating System
BSD	Berkeley Software Distribution
API	Application Programming Interface
AES	Advanced Encryption Standard
SIM	Subscriber Identity Module
PER	Packet Error Rate
SF	Spreading Factor
PSM	Power Save Mode
eDRX	Extended Discontinuous Reception
EGPRS	Enhanced General Packet Radio Service
DNS	Domain Name System
APN	Access Point Name
GCC	GNU Compiler Collection

1 INTRODUCTION

The Internet of things (IoT) is one of the fastest growing technological markets in the world to date. At the end of 2019 there were estimated nearly 5 billion commercial and industrial IoT devices deployed around the world. By the end of 2020, that number is estimated to reach nearly 6 billion. Most of today's IoT devices are deployed in either utility or security applications and building automation is expected to be the biggest growing sector in 2020. /1/

With the growth of commercial and industrial IoT, a demand has surfaced for low power long ranged communications. To meet this demand, several new communication technologies have been released in the last years. These low-power wide-area networks (LPWAN) offer ranges of up to tens of kilometres while keeping power usage and costs at a minimum mostly by compromising data rate. The transfer speeds of these technologies are in the ranges of tens of kilobits per second; enough for embedded sensor devices but insufficient for nearly everything else. /2/

Wapice Ltd is a Finnish full-service software company founded in 1999. Wapice provides a wide variety of hardware and software related services to advance industrial digitalization for its customers around the world. One of Wapice's successful products is their IoT-Ticket cloud service allowing easy prototyping and cloud integration of IoT solutions. /3/

Wapice has developed a prototype of an IoT device with information gathering and limited control capabilities. The wireless communication of this prototype was implemented using Wi-Fi, which is not suitable for long distance communications. To further advance the prototype, there was a need to investigate and implement long ranged connectivity using an LPWAN technology.

The purpose of this thesis was to compare two of the available LPWAN technologies and implement a prototype using the better suited one. Narrow Band IoT (NB-IoT) and Long Range (LoRa) were selected as the interesting options for Wapice when defining the boundaries of this thesis project. The prototype was

implemented using a cheap low power ARM microcontroller running a Zephyr real-time operating system (RTOS). The previous Wi-Fi prototype was used as a starting point and was expanded upon in the implementation phase of this project.

2 TECHNOLOGIES

2.1 LoRaWAN

The terms LoRa and LoRaWAN are used almost interchangeably while the former is a physical layer modulation and the latter is an LPWAN standard. This section was split to avoid the confusion.

2.1.1 LoRa Physical Layer

LoRa is a proprietary radio frequency modulation for low power and long-range connectivity owned by a French company Semtech. The original developer of the modulation scheme was a French start-up called Cycleo, which Semtech bought in 2012. Semtech offers a broad overview of the modulation scheme and its features but does not distribute its technical specification. LoRa modulation resembles chirp spread spectrum (CSS) modulation where error tolerance can be adjusted by altering the data transfer rates while keeping the bandwidth constant. In CSS modulation, an ultra- narrow band signal is spread over a wide bandwidth to increase its error tolerance and reach. /4/

2.1.2 LoRaWAN Link Layer

LoRaWAN is an open standard LPWAN technology built on top of the proprietary LoRa modulation scheme. The standard is maintained by LoRa Alliance, an international non-profit association founded by Semtech. The objective of LoRa Alliance is to develop the standard and encourage LoRaWAN's usage across the globe. /5/

LoRaWAN operates on unlicensed Industrial, Scientific, and Medical (ISM) radio frequencies. The ISM bands vary depending on geographical location and their usage is restricted by the local standards authority. In Europe ISM band restrictions are set by the European Telecommunications Standards Institute (ETSI). /6/

In Europe LoRaWAN has two valid frequency ranges, 433 MHz and 868 MHz, where it operates on either 125 kHz or 250 kHz channel. A single LoRaWAN message may contain up to 243 bytes of payload data. The transmissions on the ISM bands are restricted to 1% duty cycle, meaning a single device may only transmit 1% of the time. The duty cycle restrictions also affect the network base stations so downlink messages from the network to the end devices should be kept at a minimum. /6, 7/

Anyone may set up their own LoRaWAN network. A single LoRaWAN device does not attach to a specific base station and all base stations within transmission range will hear every message. Multiple base stations may be connected to form a LoRaWAN network. The position of a device can be triangulated if multiple stations belonging to the same network hear the devices messages. All LoRaWAN devices have a unique identifier which base stations use to determine if they should process the received message or not. In Finland Digita offers a nation-wide coverage with its commercial LoRaWAN network. /7, 8/

LoRaWAN standard specifies three device classes: A, B and C. All LoRaWAN devices must fill the requirements of a class A device. Class A device is the most simple and low power one. It mostly sleeps and only periodically wakes up to send its messages to the network. It may only receive data in set receive intervals after it has sent its own message. Class A device is not reachable from the network side until it autonomously wakes up and sends its message. Class B device synchronizes itself with beacon frames sent by the network base station. It negotiates a receive window relative to the beacon signal and wakes for every window to listen for incoming messages. The beacon signal repeats every 128 seconds and the time between is split into 30ms time slots. A device may negotiate the use any number of time slots with the network base station. Class C device keeps its receiver always open and only momentarily closes it while transmitting its own messages. This leads to the lowest delay from the network side, but the power consumption of the device increases drastically. /7/

2.2 Cellular for IoT

2.2.1 GSM – 4G LTE

Cellular connectivity has been utilized in IoT data transmissions from the beginning but is ill suited for many IoT applications due to its excessive power consumption and bad reception particularly indoors. In addition, the higher data rates provided by the later generation cellular networks do not provide anything of value for the majority of IoT applications. A widespread deployment of cellular IoT devices in an area would only cause excessive load on the cellular infrastructure and cause a degradation of service for everyone. /9/

2.2.2 3GPP Releases 13 – 15

In Release 13 in 2016 the 3rd Generation Partnership Project (3GPP) specified three new Radio Access Technologies (RAT) better suited for IoT applications: EC-GSM-IoT, LTE-M and NB-IoT. LTE-M and NB-IoT received further improvements in Releases 14 and 15 in 2017 and 2019 respectively. From the upcoming Release 16 onwards both LTE-M and NB-IoT are incorporated into 3GPP's 5G plan for massive machine type communications. /9, 10, 11/

EC-GSM-IoT is an extension to the archaic GSM standard that allows existing GSM networks to be better utilized in IoT applications. It adds new power classes for reduced power consumption and improves security to match that of 4G LTE. The changes are compatible with existing GSM infrastructure and its deployment only requires a software update from the Internet Service Provider (ISP). /9, 10/

LTE-M is a toned-down version of LTE that is better suited for IoT applications. It uses a narrower channel and limits the data rate to achieve enhanced network coverage while keeping most of the LTE features intact. It is the first 3GPP standardized RAT that fulfills the LPWAN requirements for long distance communications and high device density. LTE-M is compatible with current LTE infrastructure and its deployment only requires a software update from the ISP. /9, 10/

NB-IoT is a completely new RAT based on LTE but with most features either cut out or redone to minimize power consumption. NB-IoT offers a vastly superior range and battery life compared to regular LTE, but it has a very limited data rate and a long and variable latency. NB-IoT was developed as a direct competitor for other ultra low power LPWAN technologies in the ISM bands. A comparison between the features of the three different RATs can be seen in Table 1. /9, 10/

Table 1. Comparison of 3GPP Release 13 RAT features. /9, 10, 12/

	EC-GSM-IoT	LTE-M	NB-IoT
Channel access method	TDMA/FDMA (As in GSM)	DL: OFDMA UL: SC-FDMA (As in LTE)	DL: OFDMA UL: SC-FDMA (Minor differences to LTE)
Signal modulation	GMSK/8PSK (As in GSM)	16-QAM (As in LTE)	QPSK (As in LTE)
Channel	200 kHz carrier (As in GSM)	1,4 MHz channel (LTE 3-20 MHz) 15kHz subcarriers (As in LTE)	180 or 200 kHz channel 15 or 3,75 kHz subcarriers
Minimal spectrum usage	FDD 2x 600 kHz	TDD 1.4 MHz FDD 2x 1.4 MHz	FDD 2x 180 kHz or 2x 200 kHz
User Equipment power class	23 / 33 dBm	20 / 23 dBm	14 / 20 / 23 dBm
MCL (LTE 144dB)	164 dB at 23 dBm	161 dB at 23 dBm	164 dB at 23 dBm

2.2.3 NB-IoT

The development of NB-IoT started in 2015 when operators worldwide began refarming old GSM spectrum for newer 3G and LTE applications. NB-IoT was designed with that background in mind, which led to the use of approximately equal channel widths to ease the spectrum planning and conversion from GSM to NB-IoT. NB-IoT features three distinct deployment options to achieve maximum

flexibility for both spectrum refarming and coexistence with LTE and in the future 5G NR alike. /9/

In “stand-alone” deployment a NB-IoT channel can be placed in any available spectrum. For example, two GSM channels can be replaced with a single NB-IoT channel in the middle of GSM spectrum without the neighbouring channels interfering with each other. Although NB-IoT and GSM channels are of equal width, there is a need for additional guard bands between RAT boundaries. An illustration of “stand-alone” deployment can be seen in Figure 1. /10/

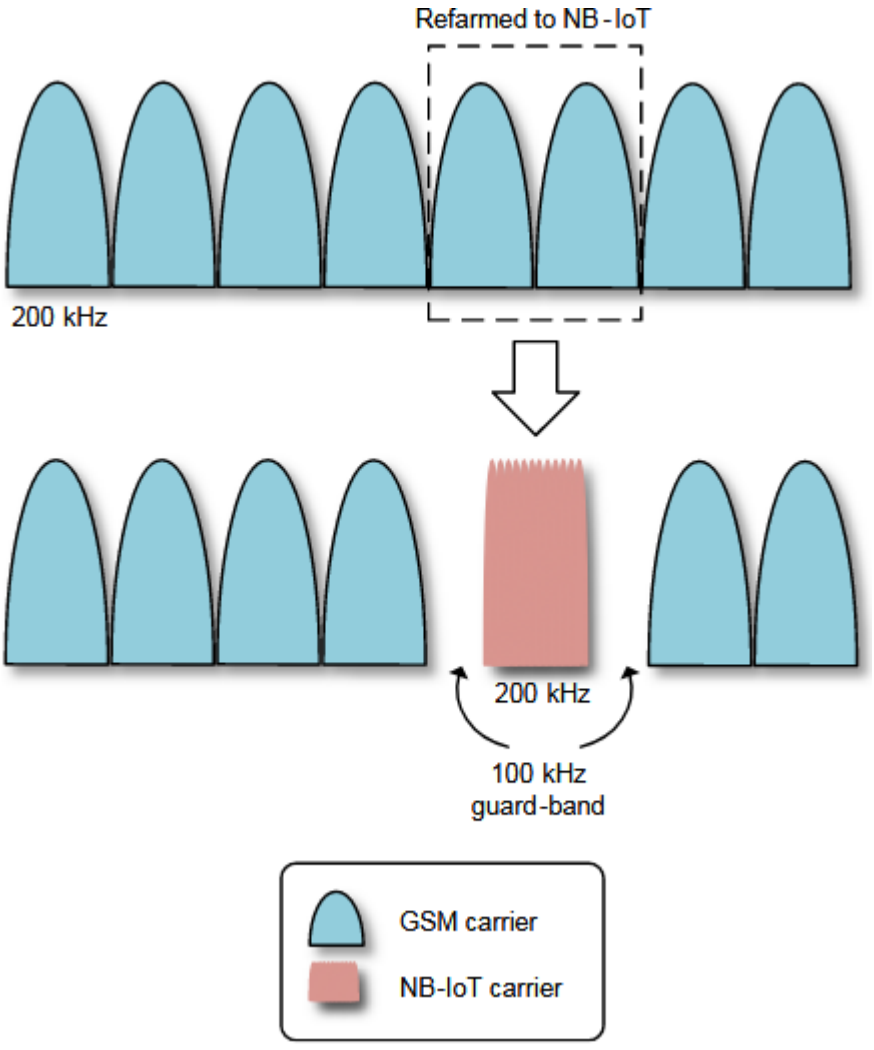

Figure 1. NB-IoT “stand-alone” deployment. /9/

In “in-band” and “guard-band” deployment modes NB-IoT channels can be deployed utilizing existing LTE channels. In “in-band” deployment NB-IoT

channel replaces one of LTE channels un-used Physical Resource Blocks (PRB). A guard band is not needed in this case due to NB-IoT PRBs being orthogonal to LTE PRBs and as such do not cause interference. In “guard-band” deployment NB-IoT is deployed in the guard band of an existing LTE channel, utilizing otherwise un-used spectrum. An illustration of “in-band” and “guard-band” deployments can be seen in Figure 2. /9/

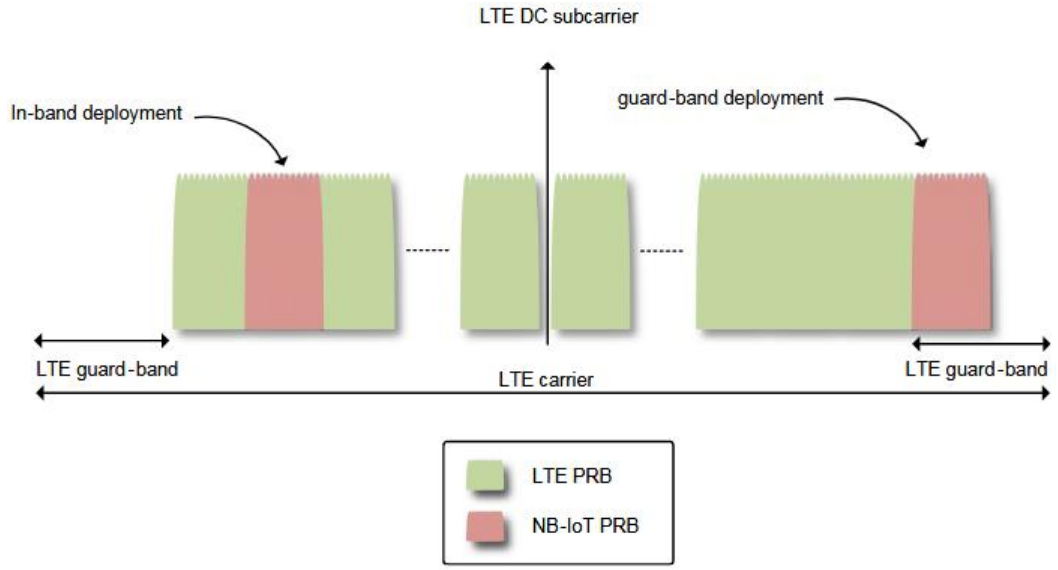

Figure 2. NB-IoT “in-band” and “guard-band” deployments. /10/

The flexible deployment options allow for deployed NB-IoT channels to persist through changes in the surrounding spectrum from GSM to LTE and in the future to 5G NR. With additions done in 3GPP Releases 14 and 15 NB-IoT now includes features for simple handover between cells and positioning of the device. NB-IoT does not support voice calls but supports SMS messaging. /9/

2.3 MQTT

Message Queueing Telemetry Transport (MQTT) is a lightweight OASIS-standardized publish-subscribe communication protocol. MQTT operates over a TCP connection and is designed for reliable transfer of small amounts of data, such as sensor data. In MQTT, messages are organized by using hierarchical topics which are implemented with text strings. MQTT is not a secure protocol but security can be achieved by using Transport Layer Security (TLS) for the

underlying TCP connection or by encrypting the data payloads so that only the desired parties can make sense of the data. /13/

MQTT communication has three parties: a publisher, a broker, and a subscriber. When a publisher sends its message to a topic on a broker, the broker then distributes the message to every subscriber of that topic. An MQTT client can operate as both publisher and subscriber simultaneously. Clients and the broker can agree on various quality of service (QoS) levels for their messaging. Using a higher QoS level leads to an increased resource consumption as more messages need to be transferred. /13/

2.4 Zephyr RTOS

Zephyr is an open source real-time operating system (RTOS) developed under the Linux Foundation initially released in 2016. It is designed primarily for resource constrained embedded devices. Zephyr aims to be hardware agnostic; the same Zephyr application can be run on multiple hardware architectures with minimal changes. /14/

Zephyr provides all the basic OS functionalities, such as multithreading, thread priorities and synchronization primitives. The footprint of the kernel is minimized by only compiling in the features the application requires. Zephyr supports a wide variety of peripherals such as GPIO, flash memory and various serial protocols. All the various memory buffers are allocated statically at compile time to reduce the risk of memory errors caused by dynamic memory management in long running embedded applications. /14, 15/

Zephyr has a highly versatile networking stack with support for variety of protocols and technologies. It supports both TCP and UDP traffic over both IPv4 and IPv6 as well as several higher-level protocols such as HTTP and MQTT. The OS also provides a BSD style socket API the application developers may utilize for easier network related development. TLS and DTLS capabilities for the Zephyr socket API are provided by the bundled Mbed TLS library. The full Zephyr network stack architecture can be seen in Appendix 1. /15/

3 TECHNOLOGY EVALUATION

3.1 Security

Security is an important factor when developing commercial or industrial IoT applications. Communication security is often difficult to get right and is frequently neglected in IoT applications. Neglecting the security aspect of IoT will lead to more widespread malware such as the Mirai botnet back in 2016 /16/.

The encryption in LoRaWAN communication is implemented using symmetrical Advanced Encryption Standard (AES) with 128-bit keys. LoRaWAN devices employ two distinct encryption keys: one for securing the network traffic and another for encrypting the message payloads. Before LoRaWAN specification version 1.1 only a single key was used for both which allowed the network provider to also decrypt the message payloads. /7/

NB-IoT employs the same security architecture as modern LTE and joining the network requires a valid Subscriber Identity Module (SIM) from the ISP. The SIM handles the cryptographic functionalities required for network connectivity. The keys used in LTE encryption are either 128-bits or 256-bits long and provide full authentication of connected parties, encryption of all sent data and protect the integrity of the message at all stages. /17/

From a security standpoint both LoRaWAN and NB-IoT are equally good choices for IoT connectivity. In LoRaWAN the security keys are device specific whereas in NB-IoT a valid SIM provided by the ISP must be used. Both technologies use adequately long keys with symmetrical AES encryption, which is expected to remain secure for the time being /18/.

3.2 Range & Device Capacity

The number of IoT devices utilizing both short- and long-range communications is growing rapidly. As more and more devices are deployed the limitations of the radio spectrum become increasingly apparent. Special attention must be paid to

the technology choices when designing an IoT applications for locations where there is a danger of congestion in the network. /2/

LoRaWAN claims to support up to 20 km radio links. In practice, the usable range varies from up to 10 km on rural deployments to around 1 km in urban areas. A single LoRaWAN base station can serve around 10 000 devices while maintaining an acceptable Packet Error Rate (PER). /7, 19/

LoRaWAN uses a pure ALOHA medium access which leads to problems when the device density under a single base station grows. In pure ALOHA any source may transmit at any given moment. This leads to frequent collision and a need to retransmit messages. The frequency of collisions is mainly affected by the length of the transmissions. /7, 19/

A LoRaWAN device adjusts its Spreading Factor (SF) to achieve fastest reliable communication channel. In worse signal conditions, it uses a bigger SF to compensate. A bigger SF means the message transmission is spread over a longer period for the receiver to have a better chance of receiving it successfully. This in turn makes the transmissions more susceptible for collisions. Interference from many devices can be mitigated by deploying more base stations as the devices will use the lowest required transmit power to reach the nearest station. /7, 19/

Susceptibility to collisions combined with restrictions set for ISM bands may make it challenging for a device in bad coverage to transmit its message. After a failed transmission, the duty cycle restriction can force the device to wait for a long period before it may try retransmission. This problem is especially apparent for downlink messages from the network base station to the end device. Additionally, any other application or technology may start using the same ISM bands at any moment, which can cause issues with LoRaWAN connectivity if such applications become widespread. /7, 19/

NB-IoT is deployed by the ISPs alongside regular LTE using mostly the same base stations. The coverage follows along the lines of current LTE coverage but reaches further from the stations due to NB-IoT’s greater maximum link budget.

The improved link budget is achieved mostly by using a simpler coding scheme and a much slower data rate. /9/

Based on a simulation used when designing the NB-IoT RAT a single NB-IoT carrier could support up to 67 000 devices simultaneously. 3GPP Release 14 added a possibility to designate a single NB-IoT carrier as an anchor channel the devices use when joining the network but then switch to transmit their data on a separate nonanchor carrier. This way up to 110 000 devices could communicate using the same nonanchor carrier. This multi carrier approach can satisfy the 5G requirement of 1 000 000 devices per square kilometre without excessive use of spectrum. /9/

Both LoRaWAN and NB-IoT are suitable for long range IoT communications and support high device densities. NB-IoT supports a higher number of devices per base station but LoRaWAN compensates by being easier to expand. Both are reliant on the network providers coverage unless a private network is established and maintained.

3.3 Power Consumption

In wireless communications, device power consumption is mostly dictated by the transmission times. The more a device keeps its transceiver active the more it consumes power and thus shorter its battery life. IoT devices are often designed to be autonomous and battery powered while they are expected to operate several years even in remote locations. /2/

LoRaWAN devices negotiate the optimal transmission power and SF with their nearest base station. This leads to minimal power consumption and helps reduce interference between nearby devices and networks. Class A LoRaWAN device uses the least amount of power due to it keeping its receiver inactive until it itself transmits to the network. /7/

In a perfect scenario a simple class A LoRaWAN device transmitting sensor data could operate up to five years with a small 3 Wh battery. If the device expects the network to acknowledge the transmitted messages the expected lifetime already

drops to four years. Frequent retransmits combined with bad reception can drop the autonomous time down to just a few months. A typical LoRaWAN sensor device can be expected to remain operational for around four years. /20/

The power consumption of NB-IoT depends on mostly the same criteria as LoRaWAN, but NB-IoT has some addition power drain due to network synchronization and enforced QoS. Additionally, NB-IoT has expanded functionality for two LTE power saving techniques. In Power Saving Mode (PSM) the device only attaches itself to the network once and can shut down its transceiver for extended periods of time without dropping from the network. While in PSM the device only opens the communication channel periodically to exchange messages. This can be combined with Extended Discontinuous Reception (eDRX) where the device periodically toggles its reception while remaining active on the network. /9, 21/

In a perfect scenario an NB-IoT device can autonomously send sensor data for over 20 years with a 5 Wh battery. In the worst-case scenario the device is expected to operate only just over 1 year. A typical NB-IoT sensor device can be expected to remain operational for over 5 years. /9/

Both LoRaWAN and NB-IoT are suitable for use in battery powered IoT application. In good reception, both technologies can comfortably hit a 5-year device lifetime using small batteries. In bad reception NB-IoT performs better due the network enforced QoS which leads to less unnecessary retransmissions.

3.4 Latency & Data Rate

Most of the low-power IoT applications do not require low latency or high throughput connectivity. Latency is only relevant for the fraction of the applications that implement controlling of the device from the network. Data rate is of importance only for applications that must frequently transmit large amounts of data.

The latency to reach a LoRaWAN device depends mostly on its class. Class A device is not reachable from the network until it first wakes and transmits to the

network. Class B employs the beacon time slots for downlink connectivity. The delay to a class B device varies depending on the current beacon phase and demand for the time slots. The delay can be expected to remain under the 128s the full beacon cycle takes. Class C device keeps its receiver always open, which leads to minimal downlink delay but increased power consumption. LoRaWAN data rates vary between 150 bps and 10 kbps depending on used channel and SF. Newer LoRa modules also support 50 kbps GFSK modulated signals in good reception. /7, 19/

The latency to reach an NB-IoT device utilising the PSM and eDRX functionalities is comparable to a class B LoRaWAN device. The length of the cycles can be configured from seconds to up to 3 hours for eDRX and several days for PSM. Both the device and the base station must agree on the PSM and eDRX configurations before they can be used. The signalling delay in good reception is under 1 second while in bad reception it can take up to 8. /9/

NB-IoT data rate varies depending on deployment type and how many subcarriers are available for the device to utilize. Average downlink speeds are around 25 kbps while uplink speeds vary from 5 kbps to 60 kbps. After 3GPP Release 14 data rates on a nonanchor carrier can reach up to 120 kbps and 200 kbps for downlink and uplink respectively. /9/

Neither of the technologies are suited for applications that require real-time control capabilities due to both having long and variable latencies. NB-IoT supports higher data rates compared to LoRaWAN and the maximum amount of data one can transmit over a period is limited by their agreement with the ISP regardless of chosen technology. NB-IoT is more flexible with the sleeping configurations for when there is a need to both send and receive data periodically.

4 PROTOTYPING

4.1 LPWAN Technology Selection

After the evaluation part, it was decided the prototype would be implemented using NB-IoT. The plan was to expand upon an earlier prototype that used Wi-Fi for network connectivity and TLS encrypted MQTT to send data to Wapice's IoT-Ticket cloud service.

The biggest factor for choosing NB-IoT over LoRaWAN was its inbuilt support for IP traffic. MQTT is built on top of the full IP stack while LoRaWAN has its own custom networking stack. With Digita's LoRaWAN network the data would first need to be sent to Digita's cloud and then routed from there to IoT-Ticket. In theory, it would be possible to implement a full IP stack over LoRaWAN communications, but it would be vastly outside of the scope of this thesis. With the guaranteed QoS, faster data rates and better scalability, NB-IoT would have been the preferred choice even if the support for IP traffic had not been a requirement for this prototype.

4.2 Modem Selection

There are multiple manufacturers of NB-IoT modems from which to choose. For this prototype, a BG96 modem from a Chinese manufacturer Quectel was selected. It supports NB-IoT, LTE-M and EGPRS connectivity and includes support for several higher-level protocols, such as HTTP, which can be used to save resources on the main development board. As acquiring just the modem chip would have caused unnecessary hardware work, an "LTE IoT 2 Click" expansion board by MikroElektronika was chosen and can be seen in Figure 3. In addition to the BG96 chip, the board includes a logic level converter required to interface with the modem and a debug USB connection to the BG96 chip itself, which proved invaluable when troubleshooting issues with network connectivity. The modem and board also support various global positioning technologies, hence the second antenna connector, but those were not used in this prototype. /22, 23/

Figure 3. LTE IoT 2 Click expansion board by MikroElektronika /23/

4.3 Development Board

The main development board used in the prototype was a STM32 NUCLEO-F411RE. The earlier prototype was built using the same board and when selecting components for the new one there was no reason to change it. The board features a 32-bit ARM Cortex-M4 CPU, 512 kB flash, 128 kB SRAM, integrated ST-LINK/V2-1 programmer/debugger and a long list of peripherals. The board is programmed and debugged over a USB interface and can be seen in Figure 4. /24/

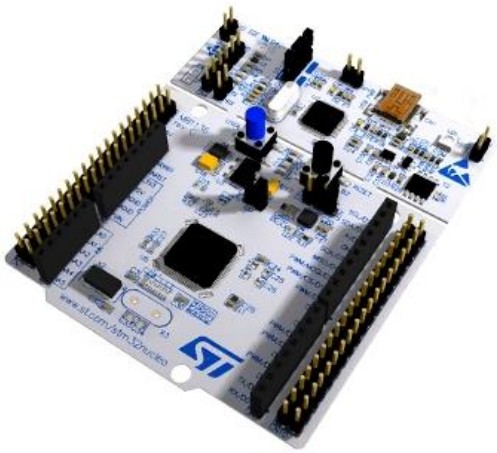

Figure 4. STM32 NUCLEO-F411RE development board /24/

4.4 Zephyr

In the time between the older and this newer prototype there had been many changes to Zephyr. It was decided to build this prototype using the current version of Zephyr as there was no longer a need for the out-of-tree Wi-Fi driver the older prototype had utilized. The current version of Zephyr was 2.2.0 at the time of writing this thesis.

For internet connectivity using the BG96 modem there were two options. The first would be to utilize Zephyr's experimental Point-to-Point Protocol (PPP) support and use the BG96 as you would use any generic cellular modem. The second option would be to offload the network connectivity from Zephyr's socket API and utilize the modems higher level protocol support. The second approach would save resources on the main development board as Zephyr would not process the network traffic on the lower layers of the network stack. /15/

4.5 Implementation

There was no written project plan for the development of the prototype. Only the end goal was set: A Zephyr IoT prototype using NB-IoT for connectivity using the older Wi-Fi prototype as a starting point. The development was done in a free-form fashion and discussions were held on how to proceed when issues arose. The operational prototype can be seen in Figure 5.

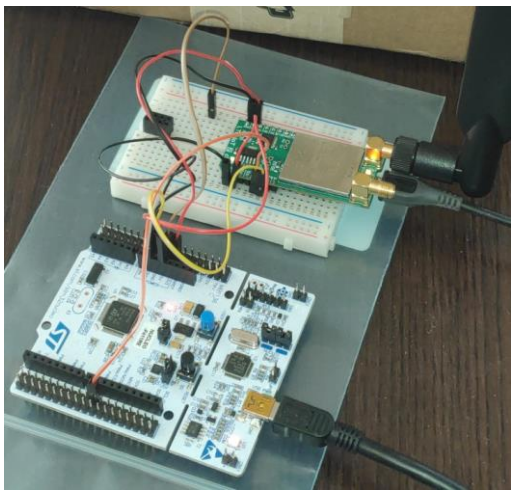

Figure 5. Zephyr IoT prototype

The Zephyr application development was done on a virtual machine running Linux. The application was built and flashed using Zephyr's "west" command-line tool, which uses GCC as its compiler and OpenOCD as its programmer. The required OS features were configured using CMake and Kconfig configuration files to be included in the build process.

To achieve internet connectivity, Zephyr's existing generic GSM modem driver was adapted for use with the BG96 modem. The driver uses the board's hardware serial port to communicate with the modem and creates a PPP connection on top of the radio interface to establish a connection to the internet. A sequence diagram describing this process can be seen in Figure 6. To achieve connectivity using the BG96 modem, a Quectel's proprietary command to activate the modems LTE networking context had to be added to the driver's modem initialization function.

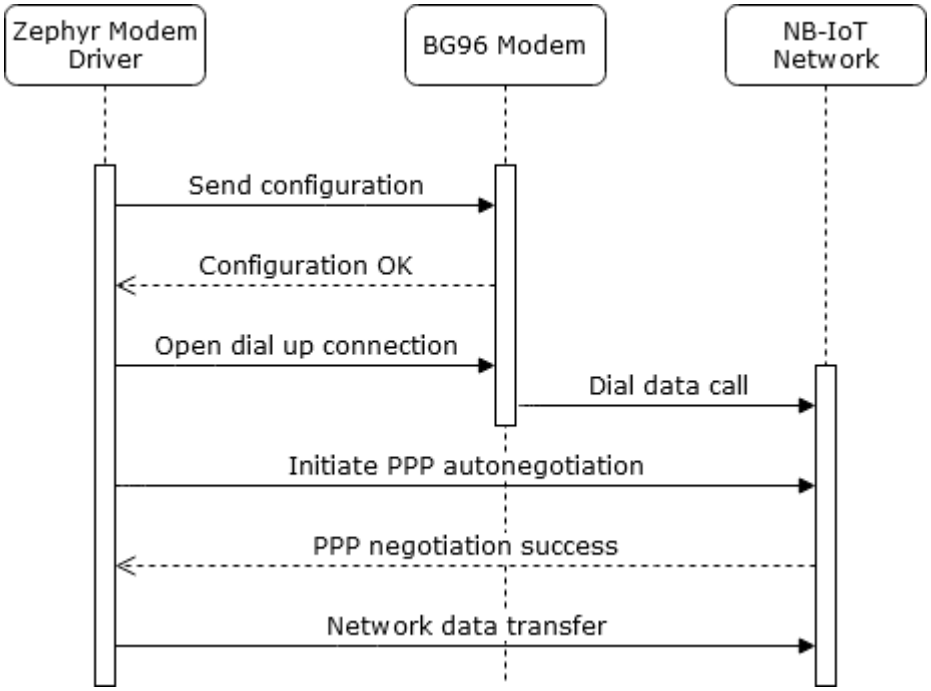

Figure 6. Zephyr modem driver connection procedure

There were also experimental attempts to use Zephyr's socket API offload functionality. An existing driver for another manufacturer's LTE modem utilizing this functionality was partly converted for use with the BG96. Due to stability

issues with Zephyr's serial modem command handler this approach was scrapped as the GSM modem approach was already functional.

The network connectivity was tested using the various networking related samples distributed alongside Zephyr. The prototype was able to ping several well-known hosts including Google's primary DNS server "8.8.8.8". The same server was queried for IP addresses of various hostnames and those were acquired successfully. A HTTP sample was used to load multiple unsecure web pages and finally TLS functionality was verified by successfully loading a Google search page over HTTPS.

An MQTT connection was used for sending data to IoT-Ticket. An IoT-Ticket client utilizing Zephyr's MQTT support had been developed for the earlier prototype and was reused in the new one. The client had functionality for both publishing and subscribing to message topics while only publishing capabilities were used for this prototype.

Zephyr's TLS socket functionality was used to secure the MQTT connection. The cryptographical functionality was provided by the Mbed TLS library distributed alongside Zephyr's source code. X.509 certificates generated in IoT-Ticket were used with AES256-SHA256 cipher in establishing the secure connection. The connection procedure to IoT-Ticket using the MQTT client can be seen in Figure 7.

The application run in the prototype was very close to that of the previous prototype. Zephyr OS being hardware agnostic meant that the application built for use with the Wi-Fi networking could be used with a cellular modem simply by configuring it to include the modem driver instead of the Wi-Fi driver. The program flow of the application can be seen in Figure 8. The later stages of the application may additionally timeout after a specified number of retries and return to the initial connection stage, which is not illustrated in the flowchart to increase its readability.

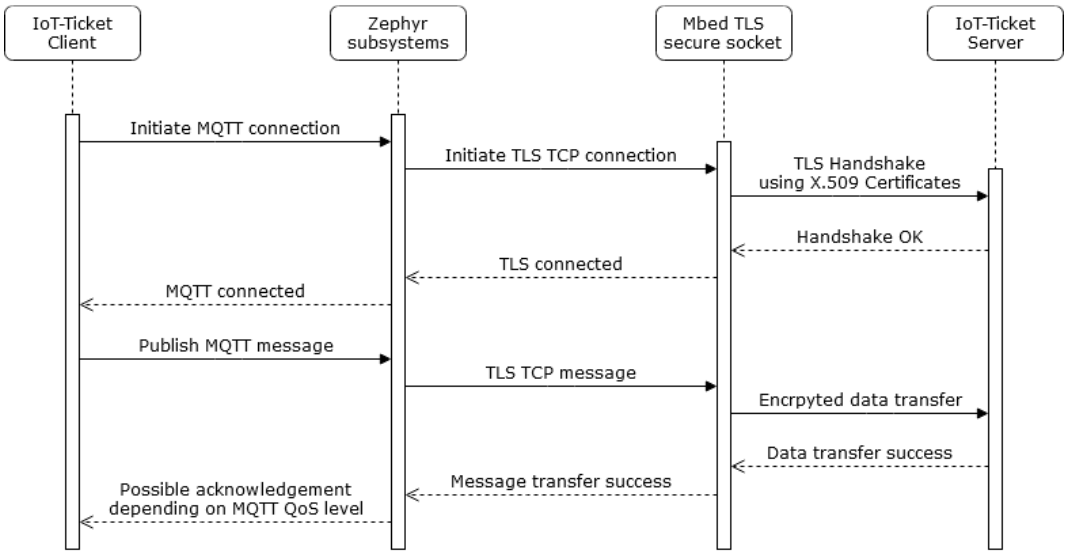

Figure 7. Zephyr IoT-Ticket client MQTT publish procedure

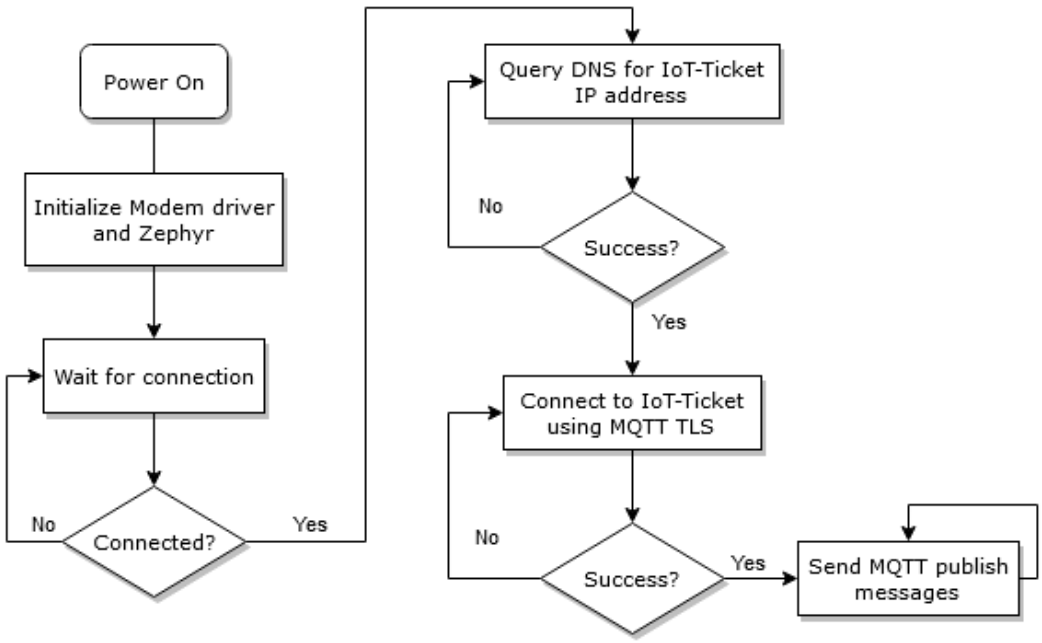

Figure 8. IoT-Ticket prototype program flow

4.6 Setbacks

The biggest hurdle in the development of the prototype was the Zephyr OS itself. It is still young, and as such contains quite a lot of unstable and experimental features that were utilized in both prototypes. Particularly the networking stack

was still under heavy development and was quite volatile at times which makes it unfit for any serious commercial or industrial applications yet.

Initially there were issues with the modem being unable to attach to the NB-IoT network. The modem was verified to be working by swapping the NB-IoT SIM card to a regular GSM one after which the network attach completed successfully. After exhausting possible ideas as to why this was the case, the ISP's technical support was contacted. It was found that the modem had gotten an incorrect Access Point Name (APN) from the SIM card. After changing the APN to the one provided by support, the network attach was completed successfully. Incorrect APN was suspected early as a possible cause, but the ISP's documentation never mentioned the use of a different APN for the NB-IoT network.

Another challenge encountered was the limited memory of the main development board, which made debug logging difficult at times. Particularly during the TLS handshake procedure, the logger thread would not get allocated enough time to process the queued messages which lead to the log buffer filling and messages being lost. In a final product this would not be an issue as most if not all logging would be disabled due to security concerns. There were often situations where various network and log buffers would need to be adjusted to get the SRAM usage below the 128 kB present on the board.

Finally, there was an unsolved issue with the TLS handshake, which lead to the secure MQTT connection to fail. The certificates were verified successfully but the server seemed to abruptly close the connection, which led the prototype to try again just to fail in an identical fashion. Nothing was found from investigating the logs on the server's end and it was concluded that this issue was not caused by the firewalls or other security equipment set up server side. This issue remained unsolved at the time of writing this thesis.

5 CONCLUSIONS & FUTURE WORK

The aim of this thesis project was to evaluate two promising LPWAN technologies and implement a prototype using the chosen technology. Despite the prototype not being completely functional, this outcome was deemed adequate for Wapice at the time of writing this thesis. The evaluation part provided valuable insight into the two LPWAN technologies in question, which can be utilized in the future when selecting appropriate technologies for real-world applications.

The development of the prototype will be continued after this thesis to achieve secure data transfer. Other future improvements would be to write a completely new networking driver utilising the socket offload functionality to save resources on the microcontroller and to read the sent data from a real-world source over a commonly used fieldbus such as Modbus. If such improvements are successfully implemented and the Zephyr OS stabilizes, this prototype could lead to a new commercially available product.

REFERENCES

/1/ Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020, Accessed 12.2.2020. https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io

/2/ Mekki K., Bajic E., Chaxel F., Meyer F. 2019. A comparative study of LPWAN technologies for large-scale IoT deployment. ICT Express 5 (1), 1–7 Accessed 12.2.2020. https://doi.org/10.1016/j.icte.2017.12.005

/3/ Wapice home page. 2020. Accesses 4.5.2020. https://www.wapice.com/

/4/ AN1200.22. LoRa™ Modulation Basics. 2015. Rev 2. Semtech Corporation. Accessed 17.2.2020. http://wiki.lahoud.fr/lib/exe/fetch.php?media=an1200.22.pdf

/5/ LoRa Alliance web pages. Accessed 19.2.2020. https://lora-alliance.org/

/6/ RP002-1.0.0 LoRaWAN Regional Parameters. 2019. Accessed 17.2.2020. https://lora-alliance.org/resource-hub/rp002-100-lorawanr-regional-parameters

/7/ LoRaWAN 1.1 Specification. 2017. Accessed 17.2.2020. https://lora-alliance.org/resource-hub/lorawanr-specification-v11

/8/ Digita LoRaWAN promotional page. Accessed 19.2.2020. https://www.digita.fi/etusivu/palvelut-yrityksille/iot/lorawan-teknologia/

/9/ Liberg, O., Sunberg, M., Wang, E., Bergman, J. & Sachs, J. 2018. Cellular Internet of Things, technologies, standards, and performance. Elsevier Ltd. https://doi.org/10.1016/C2016-0-01868-5

/10/ Standards for the IoT. 2016. 3GPP. Accessed 17.2.2020. https://www.3gpp.org/news-events/1805-iot_r14

/11/ Mobile IoT in the 5G future. 2018. GSMA. Accessed 17.2.2020. https://www.gsma.com/iot/resources/mobile-iot-5g-future/

/12/ LTE Handbook, LTE-M & NB-IoT pages, Accessed 24.2.2020. https://www.sharetechnote.com/html/Handbook_LTE.html

/13/ MQTT web page and documentation. Accessed 5.3.2020. http://mqtt.org/

/14/ Zephyr RTOS home pages. Accessed 2.3.2020. https://www.zephyrproject.org/

/15/ Zephyr RTOS documentation pages. Accessed 2.3.2020. https://docs.zephyrproject.org/latest/

/16/ What is the Mirai Botnet? Cloudflare. Accessed 7.5.2020. https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/

/17/ SP 800-187. Guide to LTE Security. 2017. NIST. Accessed 19.2.2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-187.pdf

/18/ Cryptographic Key Length Recommendation. 2020. BlueKrypt. Accessed 19.2.2020. https://www.keylength.com/en/compare

/19/ Petäjäjärvi, J., Mikhaylov, K., Pettisalo, M., Janhunen, J., Iinatti, J. 2017. Performance of a low-power wide-area network based on LoRa technology: Doppler robustness, scalability, and coverage. Accessed 19.2.2020. https://doi.org/10.1177/1550147717699412

/20/ Bouguera, T., Diouris, J-F., Chaillout, J-J., Jaouadi, R., Andrieux, G. 2018. Energy Consumption Model for Sensor Nodes Based on LoRa and LoRaWAN. Accessed 19.2.2020 https://doi.org/10.3390/s18072104

/21/ NB-IoT Deployment Guide to Basic Feature set Requirements. 2018. GSMA. Accessed 17.2.2020. https://www.gsma.com/newsroom/resources/nb-iot-deployment-guide-clp-28/

/22/ BG96 product page. 2020. Quectel. Accessed 9.3.2020. https://www.quectel.com/product/bg96.htm

/23/ LTE IoT 2 Click product page. 2020. MikroElektronika. Accessed 9.3.2020. https://www.mikroe.com/lte-iot-2-click

/24/ NUCLEO-F411RE product page. 2020. STMicroelectronics. Accessed 9.3.2020. https://www.st.com/en/evaluation-tools/nucleo-f411re.html

APPENDIX 1.

Zephyr network stack architecture /15/