# VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

## FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

## ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS


# SMART FOREST: VYUŽITÍ 5G KOMUNIKAČNÍCH TECHNOLOGIÍ PRO DETEKCI A PŘEDCHÁZENÍ POŽÁRU

SMART FOREST: UTILIZATION OF 5G NETWORKS FOR FIRE DETECTION AND PREDICTION

**BAKALÁŘSKÁ PRÁCE**

BACHELOR'S THESIS


**AUTOR PRÁCE** Adam Popelka

AUTHOR

**VEDOUCÍ PRÁCE** Ing. Pavel Mašek, Ph.D.

SUPERVISOR



**BRNO 2023**

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

# Bakalářská práce

bakalářský studijní program **Telekomunikační a informační systémy**

Ústav telekomunikací

***Student:*** Adam Popelka ***ID:*** 230307

***Ročník:*** 3 ***Akademický rok:*** 2022/23

**NÁZEV TÉMATU:**

## Smart Forest: využití 5G komunikačních technologií pro detekci a předcházení požáru

**POKYNY PRO VYPRACOVÁNÍ:**

Cílem bakalářské práce bude v teoretické části nastudovat aktuálně dostupné metody pro detekci a předcházení požárů z pohledu monitorování klíčových fyzikálních veličin (teplota, vlhkost, atd.) a zpracování obrazu. Praktická část bude obsahovat implementaci vybrané metody/metod pro detekci požáru a následný přenos dat s využitím 5G komunikačních technologií pro Průmysl 4.0, tj., Narrowband IoT či LTE Cat-M. V rámci bakalářské práce bude přistoupeno k vytvoření referenčního zařízení, které bude bateriově napájené. Funkcionalita zařízení bude ověřena v reálných podmínkách ve spolupráci s operátorem Vodafone Česká republika.

**DOPORUČENÁ LITERATURA:**

[1] CHAUDHARI, Bharat S. a Marco ZENNARO, 2020. LPWAN Technologies for IoT and M2M Applications. Online: Academic Press.

[2] LIBERG, Olof, Mårten SUNDBERG, Y.-P. Eric WANG, Johan BERGMAN a Joachim SACHS, [2018]. Cellular Internet of things: technologies, standards, and performance. San Diego, CA, United States: Academic Press, an imprint of Elsevier. ISBN 978-012-8124-581.

***Termín zadání:*** 6.2.2023 ***Termín odevzdání:*** 26.5.2023

***Vedoucí práce:*** Ing. Pavel Mašek, Ph.D.

**prof. Ing. Jiří Mišurec, CSc.**
předseda rady studijního programu

**UPOZORNĚNÍ:**

Autor bakalářské práce nesmí při vytváření bakalářské práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

## ABSTRAKT

Cílem bakalářské práce bylo v teoretické části nastudovat a popsat Internet věcí, zjistit rozdíli mezi H2H (Human to Human), M2M (Machine to Machine) a mMTC (Massive Machine Type Communication), popsat LPWAN (Low Power Wide Area Network) sítě v licencovaném a nelicencovaném frekvenčním pásmu a vzájemně je porovnat. Dále bylo za úkol podrobně popsat technologie v licencovaném frekvenčním pásmu NB-IoT a LTE Cat-M a vybrat si jednu z technologií pro využití v praktické části. V teoretické části se dále mělo nacházet popsání aplikačních protokolů pro LPWAN jako jsou MQTT, CoAP, LWM2M a dále popsat zabezpečení. Úkolem v praktické části bylo vybrat si komunikační technologii, komunikační modul a zařízení, pomocí kterého se bude měřit teplota, fotit okolní prostředí a získaná data se budou následně odesílat na server. Pro zprovoznění zařízení se musí vytvořit program, který bude v intervalech měřit okolní teplotu, kterou bude vyhodnocovat a v případě překročení dojde k vyfocení prostředí a odeslání dat na server.

## KLÍČOVÁ SLOVA

CoAP, Human to Human, Internet věcí, Iperf, IPsec, LoRaWAN, Low Power Wide Area Network, LTE Cat-M, LWM2M, Machine to Machine, massive Machine Type Communication, MQTT, NB-IoT, Python, Raspberry Pi, SigFox, Stunnel, TLS

## ABSTRACT

The goal of bachelor thesis was in teoretical part study and describe Internet of Things, found difference between H2H (Human to Human), M2M (Machine to Machine) and mMTC (Massive Machine Type Communication), describe LPWAN (Low Power Wide Area Network) in licensed and unlicensed frequency band and compare them. The next task was describe in detail technology in licensed frequency band NB-IoT and LTE Cat-M and choose ona of the technology for use in practical part. In teoretical part it should also be found description of application protocols for LWPAN as MQTT, CoAP, LWM2M and then describe security. The task in the practical part was to choose a communication technology, communication module and device that will be used to measure the temperature, take photos of the surrounding environment, and then send the obtained data to the server. In order to put the device into operation, a program must be created that will measure the ambient temperature at intervals, which it will evaluate and, in the event of and excess, take a picture of the environmet and send the data to the server.

## KEYWORDS

CoAP, Human to Human, Internet of Things, Iperf, IPsec, LoRaWAN, Low Power Wide Area Network, LTE Cat-M, LWM2M, Machine to Machine, massive Machine Type Communication, MQTT, NB-IoT, Python, Raspberry Pi, SigFox, Stunnel, TLS

Vysázeno pomocí balíčku `thesis` verze 4.07; `http://latex.feec.vutbr.cz`

POPELKA, Adam. *Smart Forest: využití 5G komunikačních technologií pro detekci a předcházení požáru*. Brno, VUT FEKT, T12, SC5.35: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2022, 78 s. Bakalářská práce. Vedoucí práce: Ing. Pavel Mašek, Ph.D.

# Prohlášení autora o původnosti díla

| | |
|---|---|
| **Jméno a příjmení autora:** | Adam Popelka |
| **VUT ID autora:** | 230307 |
| **Typ práce:** | Bakalářská práce |
| **Akademický rok:** | 2022/23 |
| **Téma závěrečné práce:** | Smart Forest: využití 5G komunikačních technologií pro detekci a předcházení požáru |

Prohlašuji, že svou závěrečnou práci jsem vypracoval samostatně pod vedením vedoucí/ho závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno, VUT FEKT, T12, SC5.35 ..... .....

podpis autora*

*Autor podepisuje pouze v tištěné verzi.

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu bakalářské práce panu Ing.Pavelu Maškovi, Ph.D. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

# Obsah

**Úvod** **10**

**1 5G sítě pro Internet věcí** **11**
1.1 Internet věcí . . . . . 11
1.2 Human to Human a Machine to Machine v Internetu věcí . . . . . 11
1.3 Limity sítí 2G a 4G . . . . . 13
1.4 Low Power Wide Area Networks . . . . . 13
1.5 Komunikační technologie LWPA v licencovaném a nelicencovaném frekvenčním pásmu . . . . . 14
1.5.1 SigFox . . . . . 14
1.5.2 LoRaWAN . . . . . 15
1.5.3 Narrowband IoT . . . . . 17
1.5.4 LTE Cat-M . . . . . 17
1.5.5 Porovnání LPWA komunikačních technologií . . . . . 18

**2 Popis sítí LTE Cat-M a NB-IoT** **20**
2.1 LTE Cat-M . . . . . 20
2.1.1 Rozšíření pokrytí . . . . . 20
2.1.2 Fyzická vrstva . . . . . 21
2.1.3 Spektrum a šířka pásma . . . . . 21
2.1.4 Downlink . . . . . 22
2.1.5 Uplink . . . . . 23
2.1.6 Radio Resource Control . . . . . 23
2.1.7 Nízká spotřeba energie . . . . . 24
2.2 NB-IoT . . . . . 25
2.2.1 Módy využívající NB-IoT . . . . . 25
2.2.2 Fyzická vrstva . . . . . 26
2.2.3 Downlink . . . . . 27
2.2.4 Uplink . . . . . 28
2.2.5 MAC vrstva . . . . . 29
2.2.6 Režim nízké spotřeby . . . . . 30

**3 Aplikační protokoly a zabezpečení pro IoT** **31**
3.1 Message Queue Telemetry Transport . . . . . 31
3.2 Constrained Application Protocol . . . . . 32
3.3 Leightweight M2M . . . . . 34
3.4 Zabezpečení . . . . . 34

**4 Výběr a zprovoznění modulu** **36**
4.1 Výběr modulu . . . . . 36
4.2 Zprovoznění modulu a komunikace se serverem . . . . . 37
4.3 Přehled spojení a vysvětlení příkazů . . . . . 38
4.4 Změna modulu . . . . . 41
4.5 Výběr platformy . . . . . 41
4.6 Přidání Raspberry Pi 4 . . . . . 44
4.7 Senzory . . . . . 45
4.8 Bateriové napájení . . . . . 46

**5 Testování NB-IoT sítě** **49**
5.1 Měření pomocí Iperf3 . . . . . 49
5.2 Měření pomocí PING . . . . . 51

**6 Program** **56**
6.1 Client - Raspberry Pi 4 . . . . . 56
6.2 Server - Raspberry Pi CM4 a LPWAN server . . . . . 57
6.3 Stunnel . . . . . 59

**Závěr** **61**

**Literatura** **63**

**Seznam symbolů a zkratek** **66**

**A Měřené hodnoty NB-IoT v Brně a Jeseníku** **70**

**B Programy na zařízeních a LPWAN serveru.** **74**

# Seznam obrázků


1.1 Ukázka tří kritických bodů Internetu věcí. . . . . 12
1.2 Graf znázorňující porovnání rychlostí a vzdáleností LPWAN sítí. . . . 14
1.3 Mapa pokrytí SigFox v České republice. . . . . 15
1.4 Mapa pokrytí LoRaWAN v České republice. . . . . 16
1.5 Mapa pokrytí NB-IoT společností Vodafone v České republice. . . . . 18
2.1 Ilustrace NB-IoT módů Stand alone, Guard band a In-band. . . . . 26
2.2 Zobrazení jednoho sub rámce. . . . . 27
3.1 Ilustrace komunikace MQTT. . . . . 32
3.2 Ilustrace komunikace CoAP. . . . . 33
3.3 Ilustrace komunikace LWM2M. . . . . 35
4.1 Fotografie sestaveného kitu s modulem v aktivním stavu. . . . . 36
4.2 Ukázka terminálu při poslání zprávy na server. . . . . 38
4.3 Infrastruktura sítě a LPWAN serveru. . . . . 39
4.4 Ukázka přijmu zprávy na serveru. . . . . 39
4.5 Vývojový diagram spojení modulu se serverem a odeslání dat. . . . . 42
4.6 Zařízení skládající se z Modulu BG77 a Rpi CM4. . . . . 43
4.7 Propojení Raspberry Pi 4 a Raspberry Pi Compute Module 4. . . . . 44
4.8 Raspberry Pi 4 se senzory. . . . . 45
4.9 Senzor teploty a vlhkosti BMP280. . . . . 46
4.10 Kamera Raspberry Pi Camera 3. . . . . 47
4.11 Baterie s měničem napětí a konektory pro zapojení zařízení. . . . . 48
5.1 Rychlost závislá na velikosti zprávy - Jeseník. . . . . 51
5.2 Rychlost závislá na velikosti zprávy - Brno. . . . . 52
5.3 Celkové množství přenesených dat s rostoucí velikostí zprávy - Jeseník. 53
5.4 Celkové množství přenesených dat s rostoucí velikostí zprávy - Brno. . 54
5.5 Velikost zpoždění s rostoucí velikostí zprávy - Brno. . . . . 55
6.1 Vývojový diagram programu BP.py na Raspberry Pi 4. . . . . 57
6.2 Vývojový diagram programu switch.py na Raspberry Pi Compute Module 4. . . . . 58
6.3 Vývojový diagram programu server.py na LPWAN serveru. . . . . 59
6.4 Grafické zobrazení fungování Stunnel na zařízení a serveru. . . . . 60

# Úvod

V horkých letních obdobích je zvýšené riziko ke vzniku rozsáhlých lesních požárů. Ty mohou hlavně v odlehlých lokalitách kvůli pozdnímu zjištění způsobit velmi náročné kontrolování šíření a extrémně nákladné a zdlouhavé hašení. Zařízení by tedy měřilo teplotu, vlhkost, znečištění ovzduší a případně další fyzikální veličiny. Pro rychlé zjištění požáru je zapotřebí zařízení, které by bylo schopné včas informovat o problému. Takové zařízení musí mít bateriové napájení s velmi dlouhou výdrží a být schopno spolehlivě komunikovat na velké vzdálenosti až na několik desítek kilometrů. Ideálními technologiemi, které splňují požadavky takového zařízení, jsou nové LPWA sítě.

V první části se nachází úvod do Internetu věcí, popis LPWAN (Low Power Wide Area Network) sítí jako jsou SigFox, LoRaWAN v nelicencovaném frekvenčním pásmu a NB-IoT a LTE Cat-M v licencovaném frekvenčním pásmu a jejich vzájemné porovnání. Další část práce je podrobněji zaměřena na technologie v licencovaném frekvenčním pásmu. Následně práce pokračuje s popisem aplikačních protokolů určených pro M2M (Machine to Machine) komunikaci.

V rámci praktické části byla ověřena a otestována technologie NB-IoT, která se následně využila jako komunikační technologie pro Raspberry Pi zařízení s komunikačním modulem BG 77. Pro praktický výstup se použily dvě Raspberry Pi zařízení, Raspberry Pi 4 a Raspberry Pi Compute Module 4. První zařízení je určené pro opakované měření teploty okolního prostředí a následné analyzování. V případě překročení povolené teploty dojde k pořízení fotobrafie prostředí, uložení a odeslání dat a fotografie na druhé zařízení. Druhé zařízení data s fotografií přijme a přepošle je pomocí technologie NB-IoT na LPWAN server.

# 1 5G sítě pro Internet věcí

Z důvodu nedostačujících vlastností starých sítí (legacy 2G, 4G a dnes již ukončené 3G) pro potřeby zařízení, která jsou součástí internetu věcí, došlo k vývoji nových komunikačních technologií, které splňují aktuální požadavky. Nové sítě podporují například nízkou spotřebu energie, přenos na velkou vzdálenost a schopnost připojit masivní množství zařízení. Mezi tyto sítě patří LoRaWAN, SigFox, LTE Cat-M a NB-IoT.

## 1.1 Internet věcí

Můžeme říci, že se IoT (Interet of Things) snaží propojit lidi, stroje, zařízení, sdílet užitečné infomrace a na základě jejich vyhodnocení se patřičně zachovat. Získávání důležitých informací probíhá pomocí mnoha senzorů. Senzory by měly být malé velikosti se schopností se připojit k internetu a cloudu a většinou jsou napájeny pomocí baterie. Kvůli tomu je zde požadavek pro co nejmenší spotřebu, s čímž pomáhají technologie v rámci sítí LPWAN (Low Power Wide Area Networks). IoT zahrnuje velké množství různých zařízení od malých senzorů, přes industriální roboty, po autonomní auta a je tedy i součástí revoluce Průmysl 4.0 [1].

Zařízení, která jsou součástí IoT mají 4 vrstvy [2]:

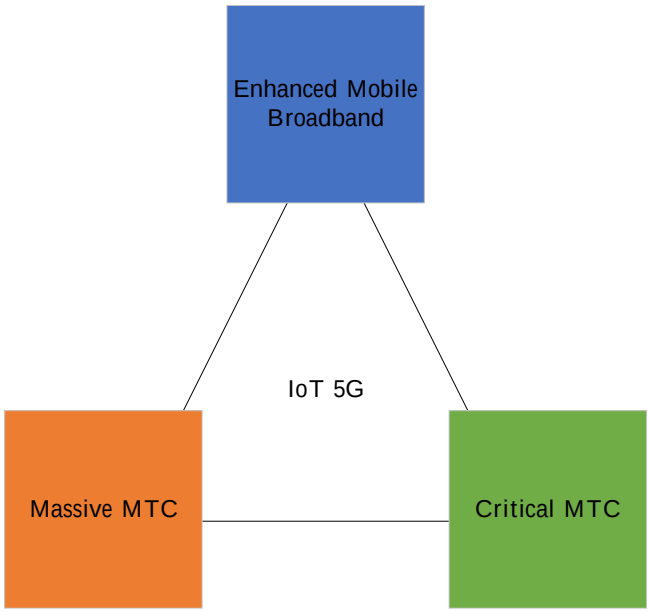
- Snímací vrstva - první vrstvou, zahrnuje všechny senzory pro sběr dat.
- Shromažďovací vrstva - druhou vrstvou, sbírá všechna získaná data od první vrstvy.
- Procesní vrstva - třetí vrstvou, připravuje shromážděná data pro přenos po síti.
- Cloud - poslední vrstvou, uložení dat, možnost připojení se zařízení.

## 1.2 Human to Human a Machine to Machine v Internetu věcí

Snahou IoT bylo propojit zařízení podobně, jako spolu komunikují lidé, kteří nemohou být spolu neustále tváří v tvář, ale stále potřebují mezi sebou komunikovat i přesto, že jsou například na různých stranách planety. Kvůli danému problému zde byl požadavek pro H2H (Human to Human) komunikaci, která se stará o propojení lidí a komunikaci mezi nimi. Zařízení by tedy podle H2H měla mezi sebou sdílet důležité informace pro případnou změnu chování v nouzové situaci, nebo jiné specifikované potřebě. Může tak docházet k velké úspoře energie, sběru dat a jejich vzájemnému sdílení a bezpečnosti [3].

Sdílení a užívání dat musí probíhat bez lidského zásahu a potřeby s nimi pracovat, nebo jakkoli interagovat. Proto se jedná o M2M (Machine to Machine) komunikaci, nebo o MTC (Machine Type Communication). IoT prochází velkým rozvojem a rozšiřováním, které způsobuje stále větší počet zařízení a senzorů, které musí posílat data a být připojeni k síti. Jedná se o mMTC (Massive Machine Type Communication). Kvůli velkému připojení různých zařízení nedostačují staré sítě 2G a 4G sítě. Řešením je nová síť 5G, která má tři různé vrcholy trojúhelníku, představující různé vlastnosti 5G jak je možno vidět na 1.1 [1, 3]:

- EMB (Enhanced Mobile Broadband) neboli rozšířené mobilní širokopásmové připojení, které poskytuje rychlý přenos velkého objemu dat, podpora streamování videa ve 4K/8K, virtuální a augmentovaná realita.
- cMTC (Critical MTC) neboli kritické MTC, které poskytuje vysokou spolehlivost a malé zpoždění tedy URLLC (Ultra-Reliable and Low Latency Communication). Kontrola dopravy a bezpečnosti.
- mMTC (Massive MTC) neboli masivní MTC, které umožňuje malou spotřebu energie, malý objem dat, velké množství připojených zařízení a velký dosah. Pro chytré domácnosti, měřící přístroje, logistiku a trasování.




Obr. 1.1: Ukázka tří kritických bodů Internetu věcí. [1]

## 1.3 Limity sítí 2G a 4G

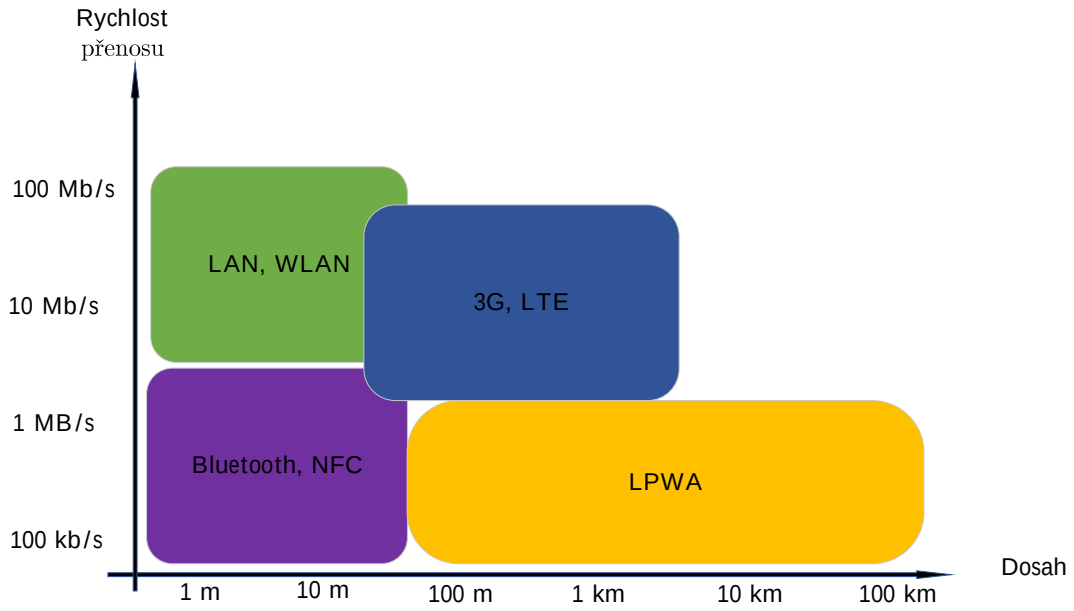
Limity 2G, 3G, 4G je schopnost spravovat velké množství připojených zařízení, které se mohou vyskytovat ve velkých těžce dosažitelných vzdálenostech, kde je hraniční úroveň signálu. Zároveň důležitým bodem mMTC je nízká spotřeba, což poskytují nové technologie 3GPP (Third Generation Partnership Project). Nové technologie se dají rozdělit do dvou skupin neboli sítí v bezlicenčním frekvenčním pásmu a v licenčním frekvenčním pásmu [1].

Mezi technologie patřící do bezlicenčního frekvenčního pásma patří SigFox a LoRa/LoRaWAN, které se vyznačují velkým dosahem, minimálně dvakrát větším jak technologie v licenčním frekvenčním pásmu, ale zároveň trpí na malou velikost přenosu dat a malé rychlosti přenosu [1].

Mezi technologie v licenčním frekvenčním pásmu patří LTE Cat-M a NB-IoT. Oproti SigFox a LoRa/LoRaWAN disponují kratším dosahem, ale mnohem většími přenosovými rychlostmi, objemem dat a výrazně lepší bezpečností. Sítě jsou primárně cílené do průmyslu a prostor, kde může docházet k rušení z okolí, a tedy vhodné pro měřicí přístroje např. elektroměry, vodoměry, plynoměry a hlášení požárů. Technologie vycházejí z již zavedeného LTE, z pohledu frekvenčního spektra využívají tedy i stejné pásmo, proto pro implementaci je potřeba pouze softwarové úpravy antén. Integrace začala probíhat v roce 2016 [1].

## 1.4 Low Power Wide Area Networks

Masivní MTC má různé požadavky a jejich řešením je LPWAN. LPWAN je koncept, jehož definice umožňuje nízkou spotřebu energie, posílání malého množství dat o malé velikosti po velké geografické oblasti. Tento koncept byl vytvořen pro zařízení napájených baterií a s potřebou fungovat po dlouho dobu několika let bez lidského zásahu, protože mohou být ve velké vzdálenosti od stanice za hranicemi dosahu normálního pokrytí legacy stítí 2G a 4G 1.2. Dvě nejvíce používané topologie LPWAN jsou hvězda, která funguje na principu zařízení připojených ke cloudu pomocí stanic, a buňková topologie, která využívá více stanic. V případě buňkové technologie mohou zařízení použít více stanic pro připojení se, což umožňuje konstantní připojení v případě výpadku jedné stanice. LPWA technologie jsou NB-IoT a LTE Cat – M pro licencované frekvenční pásmo a SigFox a LoRaWAN pro nelicencované frekvenční pásmo [1, 2].




Obr. 1.2: Graf znázorňující porovnání rychlostí a vzdáleností LPWAN sítí. [2]

## 1.5 Komunikační technologie LWPA v licencovaném a nelicencovaném frekvenčním pásmu

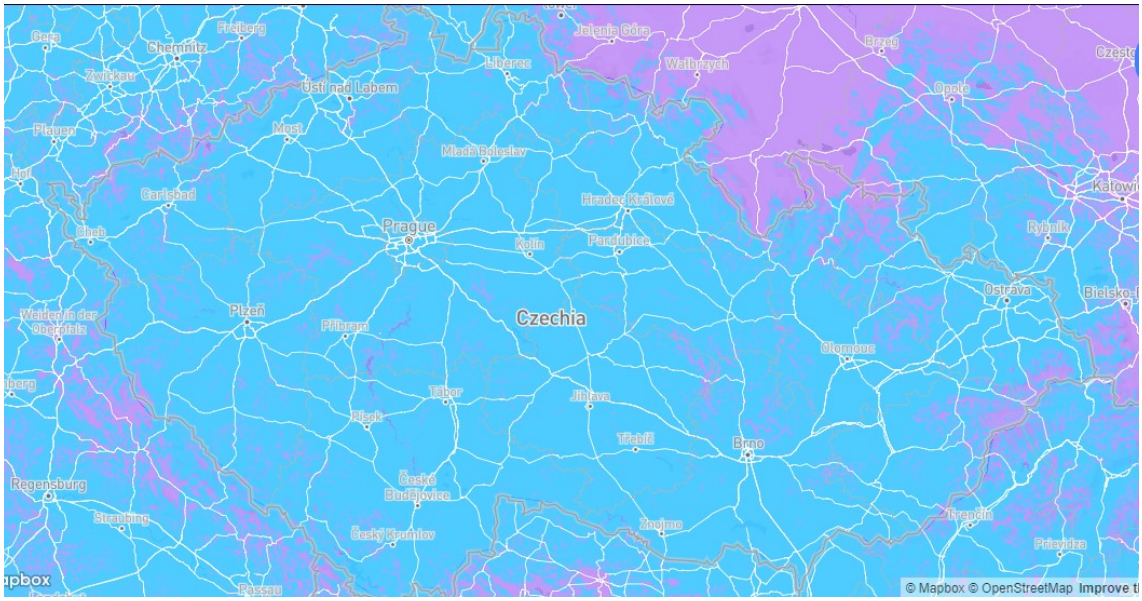
### 1.5.1 SigFox

SigFox je jedna z technologií LPWA, která využívá nelicencovaného frekvenčního pásma. Pracuje na frekvenčním pásmu 868 MHz pro Evropu, které se označuje jako ISM (Industrial Science and Medical), neboli určené pro industriální, vědecké a zdravotnické použití. Podporované šířky pásma kanálu jsou 100 a 600 Hz. Maximální rychlost je 100 bps u 100 Hz a 600 bps u 600 Hz pro oba směry. Útlum v podobě jako MCL (Maximum Coupling Loss) dosahuje až 163 dB. SigFox využívá UNB (Ultra Narrow Band) pro přenos dat. Maximální povolený výkon je 14 dBm na 2 sekundy. Maximální velikost bytu je 12 pro uplink a 8 pro downlink a maximální přenesené množství paketů je 40. Rozsah dosahu až vzdálenosti 5 km pro městkou zástavbu a 40 km v otevřeném prostranství [2, 4, 5].

V architektuře sítě zařízení komunikují s bránou a následně se servery SigFox, které mohou komunikovat se servery IP aplikace. Zařízení mohou přenášet data bez předchozí synchronizace, protože brány monitorují pásmo pro detekci signalizace

zařízení. Data by měla být zachycena alespoň třemi stanicemi, což zajišťuje větší úspěšnost přenosu dat a tedy i celkovou stabilitu a kvalitu sítě a přenosu. Může tak dojít k výběru bližší stanice se silnějším signálem a v případě výpadku k přepojení se na druhou případně třetí stanici [2, 4, 5].

SigFox funguje v 73 zemích světa včetně České Republiky, kde pokrývá 94% území a 96% populace. Společnost garantuje minimálně 5 let životnosti zařízení napájených baterií využívající SigFox služby [6].




Obr. 1.3: Mapa pokrytí SigFox v České republice. [7]

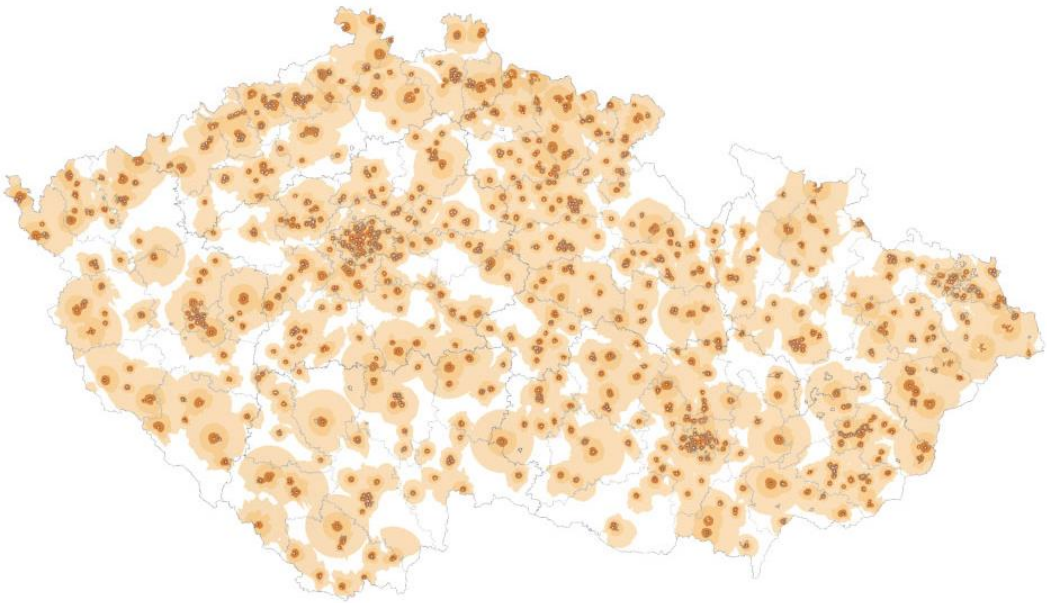
### 1.5.2 LoRaWAN

LoRaWAN pracuje také v ISM nelicencovaném frekvenčním pásmu 433 a 868 MHz a 2,4 GHz pro Evropu. Šířka pásma je 125 kHz. Síť se skládá ze dvou kategorií LoRa a LoRaWAN. LoRa byla vytvořena pro velký dosah a P2P (Peer to Peer) komunikaci a využívá CSS (Chirp Spread Spectrum) modulaci, která využívá frekvenční modulace pro rozšíření signálu. LoRaWAN je komunikační infrastruktura s protokolovým zásobníkem na vyšších vrstvách s možností připojení velkého množství zařízení. Maximální útlum vyjádřený v MCL dosahuje hodnot až 155 dB. Rychlost přenosu dat

je mezi 300 b/s až 50 kb/s pro oba směry přenosu jak uplink tak downlink. Zařízení využívající síť LoRaWAN napájená baterií mohou pracovat více jak 10 let. Maximální povolený vysílací výkon je 14 dBm, tedy stejný jako u sítě SigFox. Maximální počet zaslaných bytů je 243 pro oba směry. V městské zástavbě dosahuje rozsah 1 – 3 km a v případě otevřeného prostranství 50 – 70 km. Mapa pokrytí LoRaWAN je vidět na obrázku 1.4 [2, 5, 8, 9].

U architektury sítě nazýváme zařízení motes, která jsou připojena k branám (gateways) a brány následně k serveru, který představuje cloud. Topologie mezi moty a branami je hvězdicová a dále P2P. LoRaWAN je rozdělen do tří tříd A, B, C [8]:

- Třída A – základní třídou LoRaWAN, následující třídy vycházejí z třídy A. Poskytuje nejnižší možnou spotřebu pro moty v případě nízkého toku dat, ovlivňuje to zpoždění.
- Třída B – nadstavbou třídy A, základna vyšle Beacon rámec pro zařízení, aby vědělo, kdy má nastavit přesný čas příjmu dat.
- Třída C – neustále propojení mezi zařízeními a stanicí, nejnižší zpoždění, využívá velké množství energie.



Obr. 1.4: Mapa pokrytí LoRaWAN v České republice. [7]

### 1.5.3 Narrowband IoT

NB-IoT pracuje v licencovaném frekvenčním pásmu, které využívá LTE technologie, je tedy potřeba předplacenou SIM kartu. NB-IoT bylo uvedeno skupinou 3GPP ve 13. vydání pro IoT a specifické potřeby mMTC. Jedná se o síť umožňující přenos omezeného množství dat, s limitovanou přenosovou rychlostí a velkým zpožděním, ale pro masivní množství zařízení a senzorů [2, 5, 10].

NB-IoT využívá LTE frekvenční pásmo, pro Evropu 800 MHz, 1800 MHz a 900 MHz. Šířka pásma je 180 kHz. Technologie využívá kódování TBCC (Tail-Biting Convolution Code) pro úsporu energie. Maximální vysílací výkon je 23 dBm. Maximální množství přenesených bytů dosahuje hodnot 1600 bytů pro oba směry. V městské zástavbě je dosah 0,5 – 1,5 km a v otevřeném prostranství až 20 km [2, 5].

Implementace je velmi jednoduchá, protože vysílače potřebují pouze jednoduchou softwarovou úpravu Modulačními technologiemi jsou FDMA (Frequency Division Multiple Acces) pro uplink a OFDMA (Orthogonal Frequency Division Multiple Access) pro downlink [2, 5, 10].

NB-IoT pracuje ve třech módech Stand alone, Guard band a In-band. Stand alone používá GSM spektrum a nahrazuje GSM PRB (Physical Resource Block) za PRB NB-IoT. Proto, že nahrazuje celou buňku GSM, musí použít jeho celou šířku pásma, tedy 200 kHz místo 180 kHz. V případě Guard band je buňka umístěna v mezerách mezi pásmy LTE. In band pracuje na LTE frekvenčním pásmu [2, 10].

V České Republice poskytuje NB-IoT společnost Vodafone. Síť pokrývá 100 % v otevřeném prostranství a 94 % populace uvnitř budov 1.5 [11].

### 1.5.4 LTE Cat-M

LTE Cat-M (Long Term Evolution for Machines) také pracuje v licencovaném frekvenčním pásmu, které je stejné jako u LTE technologie, a proto je u zařízení potřeba předplacené SIM karty. Technologie byla představena skupinou 3GPP ve 13. vydání, kde bylo LTE Cat-M představeno pro IoT a mMTC potřeby. Využívá zde LTE sítě a Stand alone módu. Zařízení využívající LTE Cat-M technologii mají garantovanou výdrž baterie 10 let [2, 5, 12].

Šířka pásma je 1,4 MHz. Maximální povolený vysílací výkon je 20 a 23 dBm. Maximální počet přenesených bytů je 8188 a maximální rychlost je 1 Mbps pro oba směry přenosu. Maximální zpoždění může dosahovat až 15 ms. Modulace se využívá OFDMA pro downlink a SC-FDMA pro uplink může pracovat ve Full Duplex a Half Duplex módu. Ve městské zástavbě LTE Cat-M dosahuje vzdálenosti 1–2 km a v otevřeném prostranství 15 km [2, 5, 12].

LTE Cat-M nabízí zvýšené přenosové rychlosti a menší zpoždění oproti NB-IoT, díky využívání opakovaného rozesílání dat pro lepší pokrytí tedy CE (Coverage

Obr. 1.5: Mapa pokrytí NB-IoT společností Vodafone v České republice. [11]

Enhancement). LTE Cat-M má dva CE módy [2]:

- CE mód A - maximálně 32 opakovaní, hlavní mód.
- CE mód B - maximálně 2048 opakování.

LTE Cat-M využívá nový kanál MPDCCH (Machine Type Communication Physical Downlink Control Channel), protože je potřeba malé spotřeby energie a PDCCH bylo původně pro H2H. Technologie je snadná na implementaci díky softwarové úpravě vysílačů [2, 5].

### 1.5.5 Porovnání LPWA komunikačních technologií

| | SigFox | LoRaWAN | NB-IoT | LTE Cat-M |
|---|---|---|---|---|
| Typ spektra | ISM | ISM | licencované | licencované |
| Frekvence | 868/915 MHz | 433/868/915 MHz | 700-2100 MHz | 700-2600 MHz |
| Šířka pásma | 100/600 Hz | 125/250/500 kHz | 200 kHz | 5 MHz |
| Útlum | 162 dB | 157 dB | 164 dB | 156 dB |
| Maximální vysílací výkon | 14 dBm | 14 dBm | 23 dBm | 23 dBm |
| Maximální uplink dat | 12B | 242 B | 1600 B | 8188 B |
| Maximální downlink dat | 8 B | 242 B | 1600 B | 8188 B |
| Maximální rychlost UL | 0,1-0,6 kb/s | 0,25-11 kb/s | 0,3-159 kb/s | 7 Mbps |
| Maximální rychlost DL | 0,6 kb/s bps | 0,25-11 kb/s | 0,5-127 kb/s | 7 Mbps |
| Dosah v otevřeném prostoru | 40 km | 50-70 km | 20 km | 15 km |
| Dosah v městské zástavbě | 5 km | 1-3 km | 0,5-1,5 km | 1-2 km |
| Výdrž baterie | >10 let | >10 let | >10 let | >10 let |
| Bezpečnost | Nízká | Střední | Vysoká | Vysoká |

Tab. 1.1: Tabulka porovnání hodnot nejvyšších verzí sítí SigFox, LoRaWAN, LTE Cat-M a NB-IoT [13]

.

# 2 Popis sítí LTE Cat-M a NB-IoT

Jelikož 5G sítě LTE Cat-M a NB-IoT fungují na licencovaném frekvenčním pásmu stejně jako legacy 4G, a vycházejí ze 4G, mohou danou síť za určitých okolností využívat. Pokrytí sítí LTE Cat-M a NB-IoT poskytují velcí operátoři, jako je například Vodafone, kteří již mají k dispozici zavedenou 4G síť.

## 2.1 LTE Cat-M

LTE Cat-M je síť vytvořená skupinou 3GPP ve třináctém vydání jako NB-IoT. Vychází z rodičovské sítě LTE. Pro přehled má LTE Cat-M tyto vlastnosti [5]:

- Snadná úprava LTE vysílačů pro využití LTE Cat-M, schopnost využít LTE síť.
- Nízká spotřeba energie, zařízení mohou pracovat více jak 10 let bez zásahu člověka.
- Vyšší rychlost přenosu dat oproti ostatním technologiím jako je NB-IoT, LoRaWAN a SigFox.
- Možno připojit přes 100 000 zařízení pod jednu stanici.
- Nízká pořizovací cena zařízení využívající LTE Cat-M.
- Vhodné hlavně pro zařízení v budovách.
- Bezpečnost vycházející z LTE – autentizace uživatele a zařízení, integrita dat.

LTE Cat-M využívá v ČR frekvenční pásma číslo B20 s frekvencí 800 MHz a číslo B8 s frekvencí 900 MHz. U B20 je frekvenčí rozsah u Uplinku 832-862 MHz a u Downlinku 791-821 MHz. U B8 je frekvenční rozsah u Uplinku 880-915 MHz a u Downlinku 925-960 MHz [1, 5].

Zařízení využívající LTE Cat-M má celkem tři možnosti vysílacího výkonu, a to 23, 20, nebo 14 dBm, které byly postupně definovány v nových vydáních od 3GPP skupiny [1, 5].

### 2.1.1 Rozšíření pokrytí

Zařízení využívající LTE Cat-M síť se většinou snaží dosáhnout co největší jednoduchosti zařízení, což může ovlivnit jejich komunikační dosah. Zároveň jsou velmi často umístěná v obtížně dosažitelných místech, je proto důležité zajistit rozšíření pokrytí u LTE Cat-M. Může dojít ke zvětšení pokrytí až sedminásobnému. Zvětšení pokrytí probíhá pomocí opakovaného přenosu a zesílením spektrální hustoty výkonu [1, 5].

Opakování přenosu zajišťuje větší šanci na zachycení dat vysílačem a vyhnutí se nedoručení dat na velké vzdálenosti, v prostoru husté zástavby, hor, které mohou

rušit signál. Opakovaný přenos probíhá odesíláním stejných dat po určitou dobu [1, 5].

Pro zvýšení pokrytí tedy CE (Coverage Enhancement) se využívají dva módy [5]:

- CE mód A – až 32 opakování, základní mód, hlavně u zařízení s možným fyzickým pohybem, nebo velkým zjednodušením, který může ovlivnit jejich dosah. Většinou se tedy jedná o levnější zařízení. Maximální šířka pásma datového kanálu může být až 20 MHz.
- CE mód B – až 2048 opakování, hlavně u zařízení vázaných na jedno místo bez možnosti pohybu, větší pokrytí ale i větší zpoždění. Zařízení, které umožňuje CE mód B, má zároveň možnost CE módu A. Maximální šířka pásma datového kanálu může být až 1,4 MHz.

### 2.1.2 Fyzická vrstva

Nejdůležitější komunikační směry jsou Uplink a Downlink, které využívají stejnou modulaci jako u LTE, tedy SC-FDMA pro Uplink a OFDM pro Downlink. To umožňuje alokaci PRBs v rámci pásma LTE sítě, kdy se alokuje určítá šířka pásma pro LTE Cat-M a mohou tak fungovat obě sítě souběžně [1, 5].

Technologie využívá PSS (Primary Synchronization Signal), SSS (Secondary Sinchronization Signal) pro synchronizaci a PBCH (Physical Broadcast Channel), který přenáší MIB (Master Information Block), stejně jako LTE. Dále podporuje Full-Duplex a Half-Duplex mód, kdy využívá dvě nosné frekvence pro uplink a downlink pomocí FDD (Frequency-Division Duplex). V případě Half-Duplex módu musí zařízení přepínat příjem a odesílání dat, ale u Full-Duplex módu je zařízení schopno pracovat v obou komunikačních směrech zároveň [1, 5].

### 2.1.3 Spektrum a šířka pásma

Jedním z požadavků na IoT je flexibilní spektrum a snížení šířky pásma kvůli snížení ceny zařízení. Mezi podporované šířky pásma patří (1,4; 3; 5; 10; 15; 20) MHz včetně ochranného pásma. Frekvenční spektrum se zde skládá z PRB s šířkou pásma 180 kHz, což je řetězec bloků fyzických zdrojů. Každý PRB se skládá z 12 nosných bloků, které jsou odděleny 15 kHz. U šířky pásma 1,4 MHz je tak počet až 6 PRB a u největší šířky pásma 20 MHz může být počet až 110 PRB [1, 5].

S rostoucí šířkou pásma tak i roste počet PRB, kdy využití je 90 % až na první šířku pásma 1,4 MHz, kde je využití pouze 77 %. To je způsobeno tím, že mimo nejmenší šířku pásma nelze rozdělit šířku na menší úzkopásmové spektrum. Proto některá PRB nejsou součástí úzkopásmového spektra a jsou rovnoměrně rozděleny

do okrajů šířky pásma, ale nejde je využít na přenos ve fyzických kanálech. LTE Cat-M podporuje přeskakování frekvencí fyzických kanálů, což nabízí možnost využití PRBs, které jsou na okrajích šířky pásma [1, 5].

### 2.1.4 Downlink

K dispozici je zde velké množství kanálů pro downlink, které se dají rozdělit do tří vrstev a to logické, transportní a fyzické kanály. Pro přechod mezi vrstvami je potřeba MAC (Medium Access Control) [1, 5].

- Logické kanály:
  - PCCH (Paging Control Channel) - kanál sloužící k předání informace o příchozích žádostech o spojení.
  - CCCH(Common Control Channel) - pro přenos řídící informace mezi sítí a uživateli.
  - DCCH (Dedicated Control Channel) - přenáší informace o vyhrazeném aktivním spojení.
  - DTCH (Dedicated Traffic Channel) - provozní kanál vyhrazený pro jednoho uživatele.
  - BCCH (Broadcast Control Channel) - informuje zařízení o rádiovém prostředí.
- Transportní kanály:
  - PCH (Paging Channel) - přenáší oznamovací zprávy.
  - DL-SCH (Downlink Shared Channel) - vyhrazený pro přepravu dat.
  - BCH (Broadcast Channel) - pro přenos informací o buňce a systému.
- Fyzické kanály:
  - PSS (Primary Synchronization Signal) - primární synchronizační signál.
  - SSS (Secondary Synchronization Signal) - sekundární synchronizační signál.
  - PRS (Positioning Reference Signal)
  - PDSCH (Physical Downlink Shared Channel) - přenáší DL-SCH.
  - MPDCCH (MTC Physical Downlink Control Channel) - přenáší DCI (Downlink Control Information).
  - PBCH (Physical Broadcast Channel) - přenáší BCH.

Vysílané rámce lze rozdělit do sub-rámců, které se následně označují za platné a neplatné pro přenos. V případě označení nějakého sub-rámce za neplatný, dojde k jeho přeskočení a naváže se na následující. Sub-rámec se dá rozložit do kontrolované části a datové části. Pro synchronizaci se zde využívají stejné kanály jako u LTE, a to PSS a SSS pro získání časování rámce, nosné frekvence duplexního módu a PCID (Physical Cell Identity). Referenční signály se používají pro demodulaci fyzických

kanálů. Jedná se o předdefinované kanály vysílané stanicí [1, 5].

MPDCCH kanál přenáší DCI, které obsahuje informace o Uplink Power Control Command, Uplink Grant Information a Downlink Scheduling Information. [5]

PDSCH kanál přenáší unicast data, která jsou rozdělená do transportních bloků [5].

### 2.1.5 Uplink

K dispozici je velké množství kanálů pro uplink, které se dají rozdělit do tří vrstev, které obsahují různé kanály. Pro přechod se zde využívá opět MAC [5].

- Logické kanály – CCCH, DCCH DTCH.
- Transportní kanály – RACH, UL-SCH.
  - RACH (Random Access Channel) - přenáší informace od uživatele k síti.
  - UL-SCH (Uplink Shared Channel) - vyhrazen pro přenost dat.
- Fyzické kanály – PRACH, PUSCH, PUCCH.
  - PRACH (Physical RACH) - přenáší RACH, pro vytvoření spojení.
  - PUSCH (Physical Uplink Shared Channel) - přenos unicast data.
  - PUCCH (Physical Uplink Control Channel) - přenáší UCI (Uplink Control Information).

Sub-rámce a jejich platnost a neplatnost zde funguje stejně jako u Downlinku. Stejné to je i u synchronizace. Referenční signály zde naopak slouží k demodulaci fyzických kanálů uplinku [1, 5].

PRACH se využívá pro vytvoření spojení. PRACH má k dispozici až 64 druhů konfigurací. PUSCH kanál přenáší unicast data, která jsou rozdělená do transportních bloků. PUCCH kanál přenáší UCI, které obsahuje informace o Uplink scheduling request, Downlink HARQ feedback a Downlink CSI [1, 5].

### 2.1.6 Radio Resource Control

RRC (Radio Resource Control) je síťový protokol, který má různé stavy jako jsou IDLE, Connected a Resume. Zařízení mezi nimi přepíná podle potřeby komunikace, nebo šetření energie [1, 5].

#### IDLE

IDLE mód je klidový režim, kdy zařízení vyčkává na připojení a má několik různých procedur. Jednou z procedur je výběr buněk, kdy se nejprve musí vybrat buňka pro identifikaci, synchronizaci a určení vhodné buňky. Mezi zařízením a stanici probíhá komunikace pomocí RNTI (Radio Network Temporary Identifier). Proces výběru buňky je následující [1, 5]:

- Nejprve dojde k vyhledání PSS kanálu nalezené buňky. Pak dojde k synchronizaci frekvencí a času podle nosné frekvence.
- Následně dojde k synchronizaci pomocí SSS kanálu a dojde k identifikaci rámce a duplexního módu, PCID a CP délky.
- Proces pokračuje zjištěním MIB, šířky pásma a informacemi pro plánování.
- Nakonec dojde ke zjištění SIB1 (System Information Block 1) pro identifikaci přenosové konfigurace.

Po určení vhodné buňky dochází k získání všech informací o systému. IDLE stále monitoruje okolní buňky pro případ nalezení vhodnější buňky. Random access probíhá následovně: ze SIB2 dojde k načtení PRACH, zařízení pak pošle preambuli k přístupu do sítě. Stanice odpovídá pomocí RAR (Random Access Response), která obsahuje informace o připojení k síti. Následně stanice posílá údaje o nastavení spojení. Access control poskytuje ACB (Access Class Barring) a EAB (Extended Access Barring) [1, 5].

#### Connected

Connected mód, neboli připojený mód, kdy je zařízení připojené do sítě a komunikuje se stanicí. Největší závislost komunikace je na 16-bitovém RNTI. Součástí připojeného módu je i proces plánování přenosu dat, které se následně rozděluje do dynamického Downlink a Uplink plánování. Dále je součástí připojeného módu opětovný přenos, kontrola napájení a kontrola mobility [1, 5].

#### Resume

Resume zajišťuje opětovné propojení pozastaveného stavu a obnovení předchozího nastavení. Proces funguje díky identitě obnovení, která má schopnsot identifikace pozastaveného připojení [1].

### 2.1.7 Nízká spotřeba energie

Hlavní podmínkou IoT je, aby zařízení měla malou spotřebu energie a co nejdelší výdrž přes 10 let. K úspoře energie slouží dva módy PSM (Power Saving Mode – režim nízké spotřeby) a eDRX (Extended Discontinous Reception – rozšířený přerušovaný příjem). Ideálně by mělo zařízení využívat oba módy, což způsobí vysokou životnost baterie, je ale potřeba správné nastavení módů, aby zařízení nebylo úplně nedostupné [1, 5].

PSM zajišťuje dobu mezi ohlášením aktuálního stavu zařízení stanici, tedy pTAU (Periodic Tracking Area Updates). V aktivním PSM módu běží jeden ze dvou časovačů [5].

- T3412 Timer – v dobu časovače dochází k oznámení o připojení do sítě v pTAU rámci. Minimální délka časovače je 4 hodiny a maximální 423 dní podle třináctého vydání 3GPP, ale délka časovače se může změnit podle potřeby.
- T3324 Active Timer – v dobu časovače je zařízení v Active/IDLE módu, uživatel může nastavit délku časovače, kdy ohlašuje připojení do sítě, má dva typy Nižší a vyšší nastavení. Nižší nastavení má kratší přechod z Active/IDLE módu do hibernace a větší úsporu energie. Vyšší nastavení má delší přechod z Active/IDLE módu do hibernace, tedy delší dobu možnou pro komunikaci.

Další technologií pro úsporu energie je eDRX, která vychází z DRX v LTE. Technologie zajišťuje dobu, kdy je zařízení nedostupné. To způsobuje výraznou úsporu, ale nedostupnost je i velkou nevýhodou v případě nutnosti komunikace. PTW (Paging Transmission Window) nám umožňuje nastavení eDRX. Zařízení v režimu eDRX nepřijímá, ale je schopno v dobu potřeby okamžitě začít vysílat. Minimální délka cyklu je 5,12 sekund a maximální 43,69 minut [1, 5].

## 2.2 NB-IoT

NB-IoT je technologie vydaná skupinou 3GPP ve 13. vydání stejně jako LTE Cat-M. Maximální vysílací výkon byl ve třináctém vydání doporučen na 20 nebo 23 dBm. Následně docházelo ke snížení vysílacího výkonu na 14 dBm ve čtrnáctém vydání. V případě vysílacího výkonu 14 a 23 dBm může dojít k úpravě zařízení, kdy anténa funguje jako vysílač i přijímač [1].

Pro snížení spotřeby se místo turbo kódu jako u LTE používají konvoluční kódy. Další snížení spotřeby zajišťuje zmenšení hlavičky TBS na maximální velikost 680 bitů. NB-IoT může pouze v jeden okamžik přijímat nebo vysílat, podporuje tedy pouze Half-Duplex narozdíl od LTE Cat-M, které podporuje Half-Duplex i Full-Duplex. NB-IoT funguje v FDD módu, tedy uplink a downlink pracují na jiných frekvenčních pásmech [1, 14].

Rozšíření pokrytí neboli CE je zde stejně jako u LTE Cat-M zajištěno opakováním přenosu na úkor rychlosti přenosu dat. Další schopností pro rozšíření pokrytí je zajištění konstantního obálkového průběhu [14].

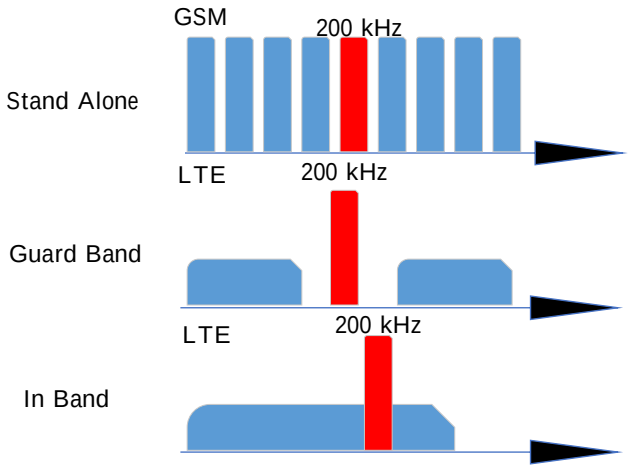
### 2.2.1 Módy využívající NB-IoT

Stand-alone je první mód, který NB-IoT využívá pro maximální flexibilitu u různých scénářů. Využívá šířku spektra alespoň 180 kHz. NB-IoT zde nahradí PTBs GSM spektra. Aby nedocházelo k vzájemnému omezení NB-IoT a GSM, je zde vložené doporučené ochranné pásmo 200 kHz viz obrázek 2.1. Pokud stejný operátor poskytuje

GSM i NB-IoT, doporučuje se ochranné pásmo 100 kHz. Kvůli ochrannému pásmu jsou tak nahrazeny dvě buňky GSM spektra pro vložení jedné NB-IoT buňky [1, 14].

Guard band mód využívá nevyužité ochranné šířky pásma u LTE viz obrázek 2.1. Díky obsazenosti šířky pásma u LTE okolo 90 %, umožňuje 5 % volné šířky ochranného pásma na obou stranách vložit NB-IoT pro přenos. Šířka LTE pásma pro využití ochranného pásma musí být 5, 10, 15 a nebo 20 MHz. V případě šířky pásma 1,4 MHz je zde obsaženo pouze 6 PRB s velmi malou šířkou ochranného pásma a proto by Gaurd band nešel použít. Stejný problém malé šířky ochranného pásma je i u 3 MHz [1, 14].

In-band mód využívá předem určené PRB pro NB-IoT v řadě PRBs u LTE viz obrázek 2.1. Stejný mód využívá i LTE Cat-M [1, 14].

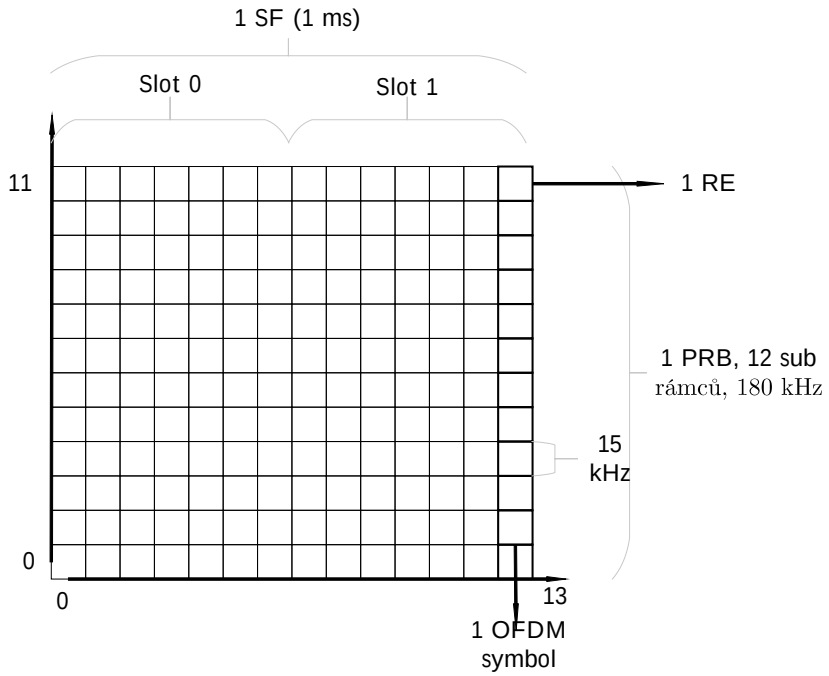



Obr. 2.1: Ilustrace NB-IoT módů Stand alone, Guard band a In-band. [1]

### 2.2.2 Fyzická vrstva

Jelikož NB-IoT vychází z LTE, využívá zde stejnou modulaci pro přenos, tedy SC-FDMA pro Uplink a OFDMA pro Downlink. Pro oba přenosy je vyhrazená šířka pásma 180 kHz, což vychází z definice šířky pásma pro PRB. Dalšími děděnými singály jsou PSS, SSS a PBCH při synchronizaci [1, 14].

Skladba zdrojů ve frekvenčním spektru zde funguje stejně jako u LTE. Jeden rámec se skládá z deseti subrámců o délce 1 ms a složený ze dvou časových slotů o 0,5 ms, délka celého jednoho rámce je tedy 10 ms. Subrámec se dále skládá z REs (Resource elements), které tvoří pole 12x14, kdy 12 REs představuje jeden PRB. Jeden REs má šířku 15 kHz, dohromady je tedy šířka 180 kHz jako jeden PRB. Jeden sloupec 12 REs představuje jeden OFDM symbol. Šířka 15 kHz jednoho REs je dána pro Downlink i pro Uplink, ale Uplink může mít ještě šířku 3,75 kHz. Menší šířka jednoho RE způsobí, že se jich do šířky pásma jednoho PRB vleze 48. Jeden rámec se tedy skládá z 5 slotů s délkou 2 ms o 7 symbolech v jednom slotu viz obrázek 2.2 [1, 14].




Obr. 2.2: Zobrazení jednoho sub rámce. [14]

### 2.2.3 Downlink

Downlink zde opět obsahuje několik kanálů a signálů, které plní potřebné role pro fungování a jsou mapovány o délce 10 ms. Pokud NB-IoT využívá módu In-band první tři OFDM symboly každého subrámce nejsou obsazeny, protože mohou náležet LTE řídícímu kanálu, pokud není LTE nastaveno na obsazení menšího počtu symbolů. V případě využití módů Stand alone a guard band může dojít k obsazení i

prvních tří OFDM symbolů, protože stand alone nahradí celou GSM buňku a guard band mód využije ochranného pásma a jsou tedy odděleny od LTE pásma. Jediným povoleným modulačním formátem je QPSK (Quadrature Phase-Shift Keying) [14]. Mezi kanály patří [14]:

- NPBCH (Narrowband Physical Broadcast Channel) – slouží k přenosu MIB (Master Information Block), který obsahuje základní informace pro příjem následujících informací. Vždy v prvním subrámci, ve kterém jsou ve všech případech módů vynechané první tři symboly.
- NPDCCH (Narrowband Physical Downlink Control Channel) – zajišťuje řízení a plánování následného přenosu dat. Informace jsou zde přenášeny pomocí logického bloku DCI, který se dá rozdělit do tří druhů N0, N1 a N2. N0 obsahuje plánování zdrojů Uplinku, N1 plánování zdrojů pro Downlink a potvrzení a N2 stránkování a přímé indikace. Může se nacházet ve všech sub rámcích, kromě prvního, šestého a posledního desátého. V případě In-band módu musí být vždy první tři OFDM symboly vynechány pro LTE. Ve zbývajících módech může být využit kompletně celý sub rámec.
- NPDSCH (Narrowband Physical Downlink Shared Channel) – kanál určený pro přenos dat. Může se nacházet ve všech sub rámcích stejně jako NPDCCH, kromě prvního, šestého a posledního desátého. V případě In-band módu musí být vždy první tři OFDM symboly vynechány pro LTE. Ve zbývajících módech může být využit kompletně celý sub rámec.

Mezi signály [14]:

- NPSS (Narrowband Primary Synchronization Signal) – časová a frekvenční synchronizace, tedy odstranění frekvenčního posunu. Vyskytuje se v šestém-subrámci. I v případě Guard band a Stand alone módu jsou první tři OFDM symboly pátého subrámce vynechány.
- NSSS (Narrowband Secondary Synchronization Signal) – zajišťuje přenos ID pro identifikaci. ID může nabývat hodnot 0 – 533. NB-IoT může mít stejné ID buňky jako LTE. Nachází se vždy v posledním tedy desátém subrámci.
- NRS (Narrowband Reference Signal) – zajišťuje výběr kanálu ve frekvenční oblasti. Nachází se ve všech subrámcích kromě šestého a posledního desátého.
- NPRS - pozicování.

### 2.2.4 Uplink

Uplink zde stejně jako downlink obsahuje několik kanálů a signálů, které plní potřebné role pro fungování a jsou mapovány o délce 10 ms. Využívá se zde SC-FDMA modulace. Je zde velká podobnost s LTE uplinkem, až na nově vytvořenou preambuli a seskupení dat a řídicích informací do jednoho kanálu [14].

Mezi kanály patří [14]:

- NPUSCH (Narrowband Physical Uplink Shared Channel) – jedná se o kanál určený pro přenos kontrolních informací a dat. Kvůli seskupení kontrolních informací a dat došlo k rozdělení na dva formáty 1 a 2. První formát je určený pro data a druhý pro kontrolní informace jako je kladné nebo záporné potvrzení, tedy ACK a NACK. Využívá se zde SC-FDMA modulace díky její nízké spotřebě energie. Zároveň se pro nižší spotřebu využívá místo turbo kódů jejich opakování, což je šestnáctkrát opakované poslání potvrzení. Šířka REs zde může být 15 kHz i 3,75 kHz, kdy záleží na požadavcích přijímače. V budovách je vhodnější použít šířku 3,75 kHz a 48 RE a ve volném prostranství může být šířka 15 kHz s 12 RE. Opakování přenosu může být až 128 krát.
- NPRACH (Narrowband Physical Random Access Channel) – kanál zajišťuje přenos preambule a tedy vyžádání přístupu do sítě, proto se jedná o první poslaný signál. Preambule se skládá ze čtyř různých skupin pěti symbolů. REs má zde šířku 3,75 kHz, aby se jich vlezlo 48 do jednoho PRM s šířkou 180 kHz. Pro znemožnění kolize mezi více zařízeními se pro přenos preambule využívají čtyři různé, podle určitého vzorce náhodně vybrané frekvence, mezi kterými se následně přeskakuje. Frekvenční přeskakování se nachází ve předem daných dvanácti sub rámcích.

Mezi signály patří [14]:

- DMRS (Demodulation Reference Signal) – jedná se o signál zajišťující odhad kanálu ve frekvenční doméně. Nazývá se také Uplink Pilot.

### 2.2.5 MAC vrstva

Aby komunikace mezi zařízením a serverem fungovala, je potřeba zajistit spolehlivé a bezpečné fungování downlinku a uplinku, které obsahují několik kanálů a signálů potřebných pro správné fungování. Pro přechody a plánovaní jednotlivých kanálů a signálů slouží vrstva MAC (Media Access Control). Dalšími schopnostmi MAC vrstvy je zajištění a hlídání správné frekvence a času, multiplexování a demultiplexování vyšších a nižší vrstev, mapovaní mezi transportními a logickými kanály a správa prioritních zpráv. Aby došlo ke kvalitnímu navázání spojení a následnému přenosu dat, je potřeba, aby došlo k výměně několika předem definovaných informací důležitých pro přenos. Mezi základní a nejdůležitější patří [14]:

- MIB-NB – nejdůležitější informační blok. Přenáší informace důležité pro zařízení fungující v NB-IoT. Dále informace o přenosu SIB1-NB a v případě TDD sděluje, zda bude SIB1-NB přenášen pomocí kotvy. MIB-NB je přenášen v prvním sub rámci v NPBCH.
- SIB1-NB – druhý nejdůležitější informační blok. Obsahuje informace o NB-IoT

buňce a o plánování přenosu dalších SIB-NB, podobné jako u LTE. Mapován do pátého sub rámce v NPDSCH. Mapování je závislé na operačním módu, kdy v případě In-band jsou první tři symboly vynechány.

- SIBs-NB – NB-IoT využívá velké množství různých SIB-NB, které přenášejí různé infomrace. Počet přenesených SIB-NB udává první SIB1-NB. NB-IoT buňka může přenést bloky SIB-NB s čísly 2, 3, 4, 5, 14 a 16. SIB2-NB je povinné přenést.

### 2.2.6 Režim nízké spotřeby

Zařízení běží ve dvou režimech, CONNECTED a IDLE režimu. Jelikož v připojeném módu dochází k výměně dat v síti, dochází k velké spotřebě energie a proto v něm nemůže být mMTC zařízení příliš dlouho. Proto v IDLE módu zařízení jen vyčkává a nekomunikuje a šetří tak energii. Zároveň v obou režimech může zařízení použít DRX (Discontinuous reception) mód, který na určité intervaly vypíná přijímač a šetří tak energii. Zařízení je dosažitelné díky sdílení stavu se stanicí. Dnes se už využívá novější verze eDRX, která může běžet až 3 hodiny [1, 14].

Dalším módem pro úsporu energie je PSM, jehož hlavním účelem bylo zvýšit životnost zařízení napájeného pomocí baterie. Jedná se o stav, kdy zařízení kompletně spí a nekontroluje průběžně stav sítě na rozdíl od DRX. Délka spánku zařízení může být až jeden rok. Jediná spotřeba energie je v udržení reálného času a udržení naplánovaných událostí pro IDLE mód. Zařízení může přepínat PSM mód na eDRX na velmi krátké chvíle kvůli pro zjištění stavu sítě a možnosti být dosažitelné. PSM používá dva časovače TAU (Tracking Area Update), který je definovaný pomocí T3412, může trvat až jeden rok, a druhým časovačem je aktivní časovač definovaný pomocí T3324, který může trvat až 3 hodiny [1, 14].

# 3 Aplikační protokoly a zabezpečení pro IoT

Zařízení součástí IoT mají 3 základní vrstvy, které je definují [5]:

- Sběr dat– první vrstvou, jejíž součástí jsou fyzické senzory, sběr dat.
- Síťová vrstva – druhou vrstvou zajišťující přenos dat po síti.
- Aplikační vrstva – třetí vrstvou, zajišťuje uložení a formátování dat do cloudu a jejich následné zpracování a prezentování. Základním protokolem je HTTP (Hyper Text Transfer Protocol). Dalšími protokoly jsou MQTT (Message Queue Telemetry Transport), CoAP (Constrained Application Protocol) a LWM2M (Leightweight M2M).

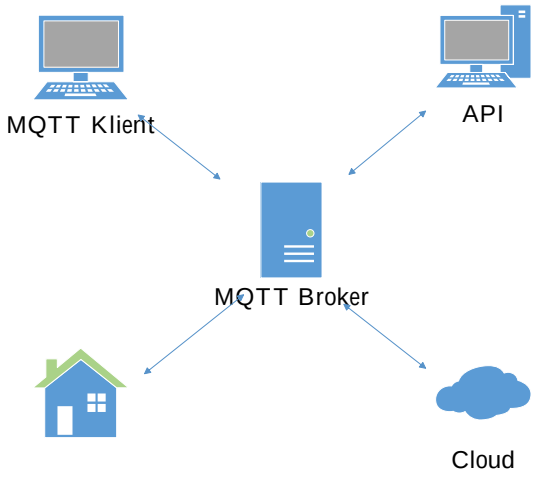
## 3.1 Message Queue Telemetry Transport

Jedná se v IoT o nejpopulárnější lehký aplikační textově založený protokol fungující na bázi zařízení – zařízení, nebo klient-server. Byl představen společností IBM už v roce 1999. Navržený na posílání dat při nízké šířce pásma a velkém zpoždění. MQTT má čtrnáct řídících paketů, rozdělených do tří částí, jako je fixní hlavička, variabilní hlavička a payload. Využívaný transportní protokol je TCP. Architektura se dá rozdělit do dvou bodů Klient a Broker 3.1 [1, 15].

- Klient může vydávat nebo přijímat data a navazuje spojení s Brokerem. Klient dále určuje, jaká data chce přijímat a případně může zrušit jejich odběr.
- Broker přijímá data od klientů, zpracuje je a rozešle klientům, kteří odebírají dané zprávy. Broker dále zpracovává přidání a odeprání klientů z odběrů daných zpráv.

MQTT má šest základních bodů, které jej definují [15]:

- Publikace/odběr – Klient publikuje data, která Broker (Server) rozdělí a následně rozesílá odběratelům vybraného topiku.
- Témata a odběr – Klient, který chce odebírat zprávy určitého tématu se musí přihlásit o odběr, který musí Broker schválit. Klient následně může odběr u určitého topiku zrušit.
- QoS (Quality of Service – Kvalita služeb) – zajišťuje kvalitu rozeslání správných dat. MQTT obsahuje tři úrovně QoS.
  - QoS0 – nejnižší úroveň, zpráva je odeslána pouze jednou, bez jistoty doručení.
  - QoS1 – umožňuje poslat zprávu v případě potřeby znovu.
  - QoS2 – jistota doručení zprávy je zajištěná pomocí 4 – way handshake.
- Uchování zprávy – Broker ukládá zprávy a data, která pošle novému odběrateli v případě nového připojení




Obr. 3.1: Ilustrace komunikace MQTT. [16]

- Čistá relace a spolehlivé spojení – propojení Klienta a Brokera je bráno jako permanentní, v případě obnovení relace je použito nejvyšší QoS tedy QoS2.
- Závěť – Klient informuje Brokera o zprávě, která bude rozeslána v případě odpojení klienta.

MQTT má problém s životností zpráv, kdy jsou nevyzvednuté zprávy stále ukládány a Broker může být přetížen. Bezpečnost je založená na TLS, které zatěžuje procesor, a je zde potřeba přihlašovacího jména a hesla pro autentifikaci. MQTT nepodporuje upřednostnění důležitých dat, tedy např. v případě požáru se data posílají postupně [15].

## 3.2 Constrained Application Protocol

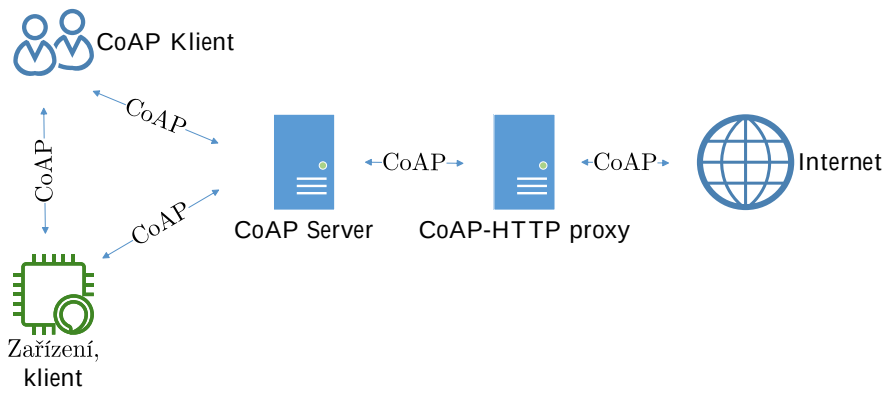
Jedná se o aplikační webový odlehčený protokol využívaný ve většině aplikací a nahrazuje HTTP díky nízké režii a podpoře multicastu, jelikož je jeho zjednodušenou verzí. Je ideální pro menší objemy dat. Výhodou CoAP je nízká spotřeba energie, podpora M2M, asynchronní rozesílání zpráv, nízká režie a podpora URI (Universal Resource Identifier). Typický dotaz obsahuje velikostně 10-20 bytů. Využívaný transportní protokol je UDP s modifikací potvrzování zpráv. Jelikož protokol

vychází z HTTP, mají stejnou strukturu a metody REST, jako jsou GET, PUT, POST, DELETE. Díky tomu můžeme použít oba protokoly na dvou stranách komunikace [17, 18].

Další součásti CoAP je funkce stop-and-wait přenosu, podpora mutlicastu a detekce duplikátů. CoAP se dá rozdělit do dvou vrstev [17]:

- Vrstva zpráv – kontrola doručení zpráv pomocí UDP.
- Vrstva dotaz/odpověď – zajišťuje plynulý tok dat bez kolizí a duplikátů na principu dotaz odpověď.

CoAP funguje na principu klient server viz obrázek 3.2. Klient generuje požadavky a server zajišťuje přístup k datům. Komunikace je zde možná i v podobě P2P, tedy mezi klienty, kdy jeden z klientů představuje server, funkci využívá M2M komunikace [16].




Obr. 3.2: Ilustrace komunikace CoAP. [16]

Jako bezpečnostní složka se zde používá DTLS (Datagram Transport Layer Security) a občas IPSec. DTLS je založeno na TLS a je o 8 bytů delší. Jelikož je bezpečnost jedním z hlavních témat vývoje, součástí CoAPu jsou čtyři vrstvy [17]:

- NoSec – není zde žádné zabezpečení.
- PreshardKey – zařízení mají předem naprogramovaný klíč pro šifrování a dešifrování.

- RewPublicKey – zařízení mají předem naprogramovaný seznam klíčů pro DTLS přenos, povinný mód pro zařízení využívající veřejný klíč pro ověření.
- Certifikát – zařízení využívající veřejný klíč a certifikaci pro ověření.

## 3.3 Leightweight M2M

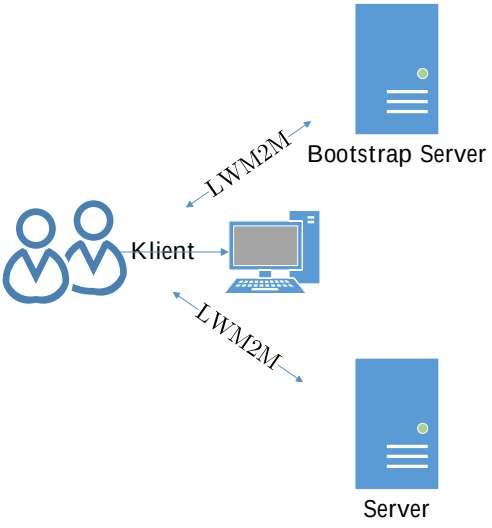
LWM2M poskytuje odlehčené komunikační rozhraní, zajišťující efektivní a bezpečný datový přenos pro M2M. Jeho využití snižuje spotřebu energie, což jej dělá ideálním pro M2M. Jedná se o OMA (Open Mobile Alliance) standard. LWM2M lze použít v jednoduchých zařízeních s malým výkonem pro M2M a zároveň i pro výkonnější zařízení. Funguje na principu klient – server s CoAP protokolem a UDP transportním protokolem s modifikací potvrzení zpráv viz obrázek 3.3. LWM2M označuje všechna validní data za Zdroje, které jsou následně rozděleny do Objektů. Objekt může mít vícero Zdrojů. Definuje aplikační vrstvu pro přenos mezi klientem a serverem. Klient je zde softwarová knihovna, nebo funkce zařízení a server je zajištěn poskytovatelem aplikačních nebo síťových služeb. Klient a server mezi sebou mají 4 rozhraní [1, 19]:

- Bootstrap – zajišťuje přístup a registraci k serveru.
- Objevení zařízení a registrace – zařízení oznámí schopnost registrace k serveru.
- Správa a povolení – server může zajišťovat správu zařízení, získá zprávy od klienta a uděluje povolení zařízením.
- Report informací – odesílání získaných zpráv zařízení může probíhat prostřednictvím řady, nebo prioritně odeslaných zpráv.

Architektura je členěná do 7 částí, kdy první je LWM2M jádro zajišťující aplikační rozhraní, následuje vrstva rozhraní, která zajišťuje API (Application Programming interface) pro přístup do dalších vrstev rozhraní, dále CoAP, DTLS pro zabezpečení přenosu, UDP/SMS, IPv6/6LoWPAN, IEEE 802.15.4 MAC/PHY. Mezi výhody patří dobře zpracované API, pomocí kterého se dá dělat potřebná modifikace, zároveň flexibilní architektura, vložená možnost správy zařízení už od výrobce a není tedy potřeba uživatelská modifikace, jednoduché propojení [1, 19].

## 3.4 Zabezpečení

TLS (Transport Layer Security) je bezpečnostní E2E (End to End) protokol využívaný v IoT. Využívá TCP transportní protokol na rozdíl od DTLS, které využívá UDP, protože TLS bylo vytvořeno s představou, že nedojde ke ztrátám paketů, nebo změně jejich pořadí. Základní vlastnosti jsou integrita, autentizace a důvěryhodnost. TLS obsahuje Autentizační hlavičku a Kvůli bezpečnosti není uveřejněný kód. Pro ověření se zde využívají certifikáty, které jsou předem vydány a v případě odhalení




Obr. 3.3: Ilustrace komunikace LWM2M. [16]

mohou být změněny. TLS handshake je bezpečné propojení mezi dvěma komunikujícími stranami a data, která jsou poslána po vytvoření bezpečného propojení, již nejsou šifrována [1, 20].

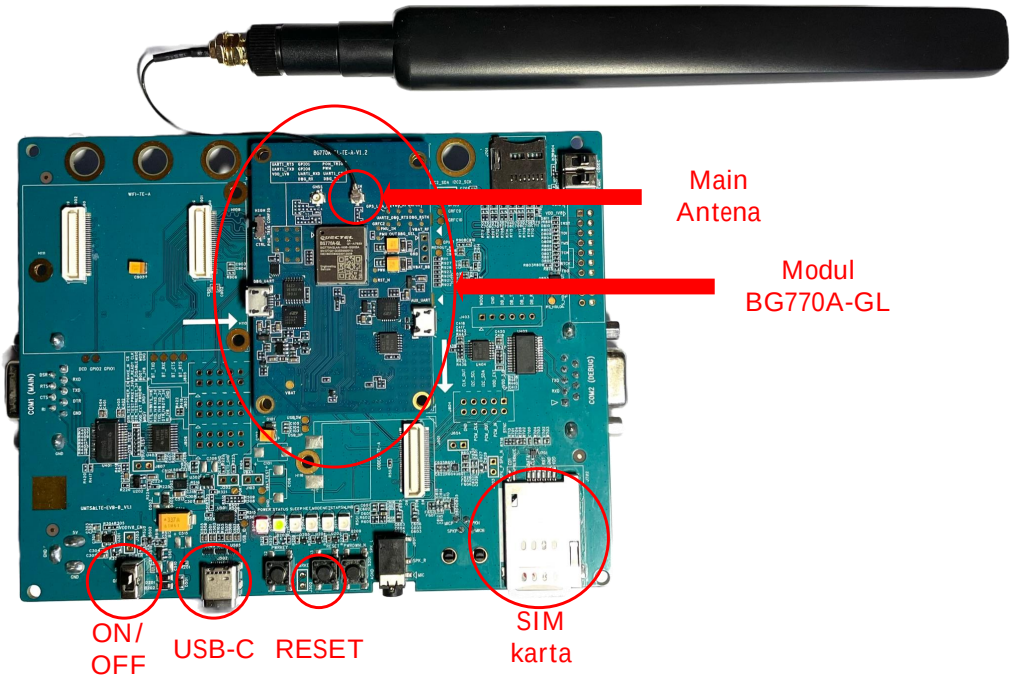
IPSec je bezpečnostní protokol pro E2E komunikaci, kdy je bezpečnost zajištěna pomocí bezpečnostního klíče, který nesmí být prozrazen. Funguje na autentizaci a šifrování. Jedná se o zabezpečení již na IP, tedy síťové vrstvě. Součástí je Autentizační hlavička [1, 20].

# 4 Výběr a zprovoznění modulu

Pro technickou realizaci bakalářské práce je potřeba vybrat si vhodný modul, který poskytně veškeré potřebné vlastnosti. Následně musí dojít k jeho seskládání a zprovoznění komunikace.

## 4.1 Výběr modulu

Pro praktické řešení byl vybrán modul Quectel BG770A-GL, který je vybaven bez limmitní SIM kartou od společnosti Vodafone. Modul je připojený k desce z UMTS LTE-EVB kitu. Kit je vybaven sadou základních antén, GNSS anténou, RS232-to-USB kabelem, USB na USB-C kabelem, RF kabelem a USB driverem 4.1 [21].




Obr. 4.1: Fotografie sestaveného kitu s modulem v aktivním stavu.

BG770A-GL je kompaktní LPWA modul splňující požadavky 3GPP 13. a 14. vydání. Mezi vlastnosti modulu patří podpora LTE Cat M1, LTE Cat NB1 a LTE Cat NB2 sítí. Nízká spotřeba energie je zajištěná díky procesoru MIPS 5150 s integrovanou RAM a flash. Modul má rozměry 14,9 x 12,9, x 1,9 mm. Podporované frakvenční pásma využívaná v České republice, a to B8 a B20 pro LTE Cat M1 i LTE Cat NB1/NB2. Maximální rychlosti přenosu dat, které modul umožňuje, jsou pro Cat M1 ve 13. vydání 300 kb/s DL a 375 kb/s UL a ve 14. vydání 588 kb/s DL

a 1119 kb/s UL. U NB1 jsou rychlosti 27,2 kb/s DL a 62,5 UL a u NB2 127 kb/s DL a 158 kb/s UL. Maximální vysílací výkon modulu je 23 dBm [21].

Mezi klíčové vlastnosti modulu patří extrémně nízká spotřeba energie, integrovaná RAM a flash. Modul dále obsahuje velké množství internetových protokolů, možnost externího rozšíření a modifikace modulu podle potřeby, dále má USB 2.0 interface a kompaktní velikost [21].

## 4.2 Zprovoznění modulu a komunikace se serverem

Kit je zapotřebí sestavit, tedy vsadit modul do desky, zasunout předplacenou SIM kartu od společnosti Vodafone a přišroubovat anténu. Následně je potřeba instalace USB ovladačů do PC a propojení s počítačem pomocí USB kabelu.

Pro ovládání modulu je zapotřebí využít programu, do kterého je možno zadávat příkazy jako například program YAT. Jedná se o terminál určený pro sériovou komunikaci, optimalizovaný pro jednoduché a rychlé zadávání příkazů určených pro práci se zařízením. YAT umožňuje vytvoření tabulky předdefinovaných příkazů, které urychlují ovládání modulu.

Při první registraci do sítě se musí nejprve zkontrolovat stav SIM karty. Dalším krokem je nastavení pásma, v aktuálním případě se jedná o LTE pásmo B20 pro LTE Cat-M a NB-IoT. Následně je potřeba nastavit APN (Acces Point Name) k bráně sítě Vodafone. Posléze dojde k určení sítě, a to NB-IoT, LTE Cat-M a nebo obou sítí zároveň. Posledním krokem je registrace k síti Vodafone.

Při zprovoznění komunikace se serverem je zapotřebí dodržet kroky, které zajistí funkční přenos zpráv. Nejprve je zapotřebí ověřit stav rádiového připojení a případně pomocí příkazu modul přepnout do připojeného režimu. Dalším krokem je otevření a nastavení TCP komunikace na adresu 147.229.146.40 s portem 65402. Po úspěšném nastavení je možné poslat zprávu na server a následně musí dojít k uzavření spojení se serverem.

WislabServer 5 je Ubuntu Server a LPWAN server s IP adresou 10.10.0.50/24. Data posílána na server z veřejné sítě Internetu musí projít přes Mikrotik Switch, Wislab Router a L3 Switch Cisco 3560 4.3.

Aby mohl WislabServer 5 přijímat zprávy z modulu, je zapotřebí zapnout naslouchání na portu 65402, jelikož modul neposílá přímo na IP adresu 10.10.0.50, ale na 147.229.146.40. K připojení a nastavení naslouchání na portu je potřeba OpenVPN. Server následně ukazuje z jaké IP adresy došlo k připojení, port, na kterém naslouchá a transportní protokol a i příchozí zprávu viz obrázek 4.4. Pro poslání další zprávy je zapotřebí opětovné zapnutí naslouchání na portu 65402.

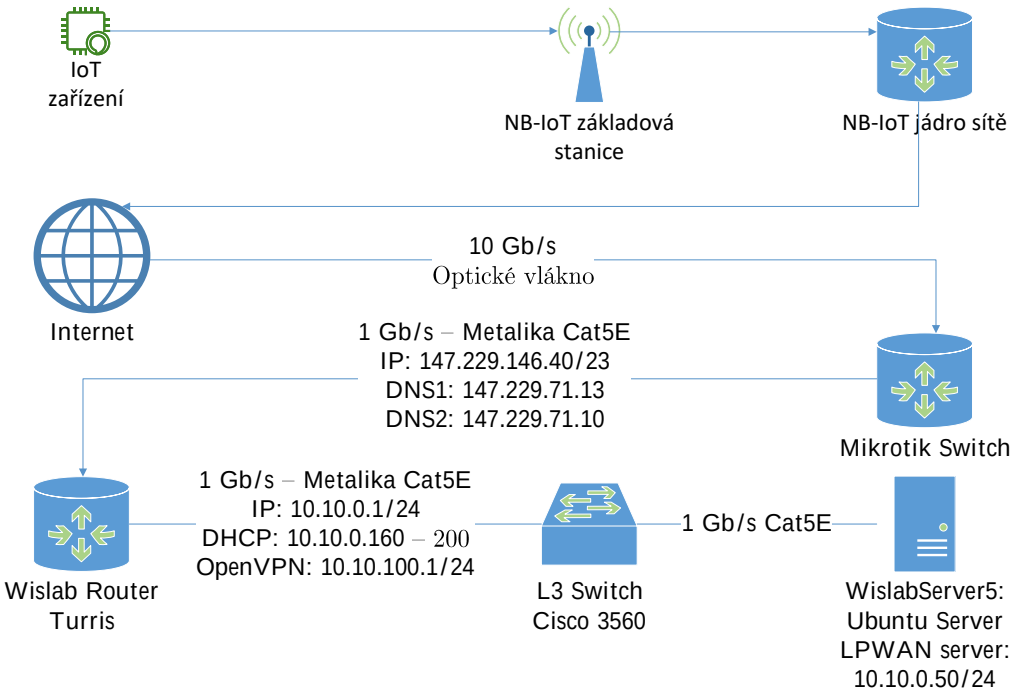
```
(15:01:52.515) AT+QCSCON?<CR><LF>
(15:01:52.592) AT+QCSCON?<CR><CR><LF>
(15:01:52.592) +QCSCON: 1,0<CR><LF>
(15:01:52.592) <CR><LF>
(15:01:52.592) OK<CR><LF>
(15:01:59.892) AT+QCSCON=1<CR><LF>
(15:01:59.970) AT+QCSCON=1<CR><CR><LF>
(15:01:59.970) OK<CR><LF>
(15:02:02.621) AT+QIOPEN=1,0,"TCP","147.229.146.40",65402,0,1<CR><LF>
(15:02:02.696) AT+QIOPEN=1,0,"TCP","147.229.146.40",65402,0,1<CR><CR><LF>
(15:02:02.696) OK<CR><LF>
(15:02:05.744) <CR><LF>
(15:02:05.744) +QCSCON: 1,1<CR><LF>
(15:02:08.731) <CR><LF>
(15:02:08.731) +QCSCON: 1,0<CR><LF>
(15:02:18.610) <CR><LF>
(15:02:18.610) +QCSCON: 1,1<CR><LF>
(15:02:23.134) <CR><LF>
(15:02:23.134) +QCSCON: 1,0<CR><LF>
(15:02:29.415) <CR><LF>
(15:02:29.415) +QCSCON: 1,1<CR><LF>
(15:02:31.991) <CR><LF>
(15:02:31.991) +QIOPEN: 0,0<CR><LF>
(15:02:40.946) AT+QISEND=0,10<CR><LF>
(15:02:41.001) AT+QISEND=0,10<CR><CR><LF>
(15:02:41.001) >
(15:03:04.333) Ahojtest22<CR><LF>
(15:03:04.408) Ahojtest22<CR><LF>
(15:03:04.408) SEND OK<CR><LF>
(15:03:04.978) <CR><LF>
(15:03:04.978) +QCSCON: 1,0<CR><LF>
(15:03:09.743) <CR><LF>
(15:03:09.743) +QCSCON: 1,1<CR><LF>
(15:03:12.748) at+qiclose=0<CR><LF>
(15:03:12.820) at+qiclose=0<CR><CR><LF>
(15:03:12.820) OK<CR><LF>
```

Obr. 4.2: Ukázka terminálu při poslání zprávy na server.

## 4.3 Přehled spojení a vysvětlení příkazů

K utvoření spojení je potřeba nastavit modul a následně jej připojit do sítě a až po úspěšném spojení může dojít ke komunikaci, která je znázorněna na obrázku ve vývojovém diagramu 4.5. Příkazy se zadávají v počítači v terminálu YAT, kde kterému se pomocí USB kabelu připojí komunikační modul. Seznam příkazů potřebných k provozu komunikačního modulu:

- AT+QCFG="usb",1 - aktivace/deaktivace usb na modulu.
- AT+QCFG="iotmode"- konfigurace síťové kategorie pod LTE RAT.
- AT+QCFG="iotmode",1 - nastavení omezení RAT na NB-IoT. v případě 0 = pouze LTE-M, 1 = pouze NB-IoT a 2 = NB-IoT a LTE-M zároveň.




Obr. 4.3: Infrastruktura sítě a LPWAN serveru.

```
lpwan@WislabServer5:~/230307$ nc -l -v -p 65402
Listening on [0.0.0.0] (family 0, port 65402)
Connection from [46.190.188.99] port 65402 [tcp/*] accepted (family 2, sport 28154)
Ahojtest22lpwan@WislabServer5:~/230307$
```

Obr. 4.4: Ukázka přijmu zprávy na serveru.

- AT+QCFG="celevel"- úroveň rozšíření pokrytí NB-IoT dotazů, výpis ECL. Odpověď ve tvaru +QCFG:"celevel",<level> nám řekne čísly 0,1 nebo 2 o jaký level rozšíření pokrytí se jedná.
- AT+QCFG="band"- konfigurace frekvenčního pásma.
- AT+QCFG="band",0,0x80000,0x80000 - nastavení LTE pásma 20 pro LTE-M a NB-IoT. První se určuje GSM frekvenční pásmo, které necháme nastavné na nule. Dále eMTC frekvenční pásmo a NB-IoT frekvenční pásmo se nastaví na hodnotu 0x80000, která náleží LTE B20.
- AT+CPIN? - kontrola stavu SIM karty. V případě výpisu odpovědi "READY"je SIM karta funkční a v provozu.
- AT+CPIN=? - slouží pro zobrazení pin kódu u karty SIM. Odpověď je číselná zpráva pinu a zpráva o stavu. V případě READY je SIM karta připravena a nevyžaduje žádné heslo. V případě SIM PIN čeká na zadání pin.

- AT+CGDCONT=1,"IP","lpwa.vodafone.iot"- číslo jedna značí minimální hodnotu u rozsahu povolených hodnot. Dále se udá PDP (Packet Data Protocol), zde IP, což značí IPv4. Následně nastavení APN, název přístupového bodu.
- AT+CGDCONT=? - dotaz pro výpis informací o APN (Access point name) a PDP (Packet data protocol).
- AT+COPS=1,2,"23003"- manuální registrace k mobilní síti Vodafone. Číslo 1 udává, že je operátor přístupný. Číslo 2 následně nastavuje formát na numerický. Číslo 23003 se dá rozdělit na 230 a označuje kód pro Vodafone v zemi Česká republika a 03 kód pro mobilní sít Vodafone Česká republika.
- AT+CEREG? - kontrola stavu registrace do sítě. V případě 0 = nic se neděje, 2 = registrace v průběhu, 1 nebo 5 = registrace úspěšná a platná.
- AT+QCSQ - výpis informací o signálu. Na začátku je typ sítě a vypíše se NOSERVICE, LTEM nebo NBIoT. Dále se vypíší čtyři číselné hodnoty. Na prvním místě RSSI (Received Singal Strength Indicator), na druhém RSRP (Reference Signal Received Power), na třetím SINR (Signal-To-Interference-Plus-Noise-Ration), kde jsou hodnoty 0-250, které se převádí na -20 dB až 30 dB. Jedna hodnota je jedna pětina decibelu. Poslední hodnota značí RSRQ (Reference Singal Received Quality) a je v dB.
- AT+QCSQ=? - dotaz na typ sítě.
- AT+GSN - dotaz na mezinárodní mobilní identitu. Odpověď v podobě String zprávy.
- AT&V - zobrazuje nastavení některých AT příkazů.
- AT+QCSCON - signalizace stavu připojení v aktuálním stavu.
- AT+QCSCON? - dotaz na aktuální stav připojení. Odpověď pomocí +QCSCON.
- +QCSCON: - indikuje stav signalizačního připojení. Odpověď na dotaz AT+QCSCON? a po zapsání příkazu AT+QIOPEN. Odpověď ve dvou číslech. První číslo udává 0 = Disable a 1 = Enable. Druhá vypasná hodnota značí 0 = IDLE, 1 = Connected, případně Error.
- AT+QCSCON=1 - přepnutí z modu disable do modu enable. Je zapotřebí pro následné úspěšné proběhnutí komunikace.
- AT+QIOPEN=1,0,"TCP","147.229.146.40",65402,0,1 - otevření služby socketu. Na prvním místě se píše contextID s rozsahem 1-5. Na druhém je connectID s rozsahem 0-11. Na třetím se udává typ služby TCP, UDP, TCP LISTENER a UDP SERVICE. Na čtvrtém místě se zadává IP adresa. Na pátém místě se zadává port v rozsahu 0-65535. Na šestém je přístupový režim s hodnotami 0 - buffer, 1 - přímý režim, 2 - transparentní přenosový režim. Na šestém se nachází result, který nabýva hodnot 0 - úspěch a 550-575 - typ chyby. Odpověď je pomocí +QIOPEN:, kde je na prvním místě conncectID a na druhém result.
- AT+QISEND - posílání dat. Udává se délka zprávy. Přijde potvrzení o úspěš-

ném odeslání zprávou SEND OK, nebo SEND FAIL a error v případě neúspěchu.

- AT+QICLOSE - zavření služby socketu. Může se skládat ze dvou částí. První je connectID s rozsahem 0-11. Druhá je timeout s rozsahem 0-65535, ale s defaultní hodnotou 10 sekund.

## 4.4 Změna modulu

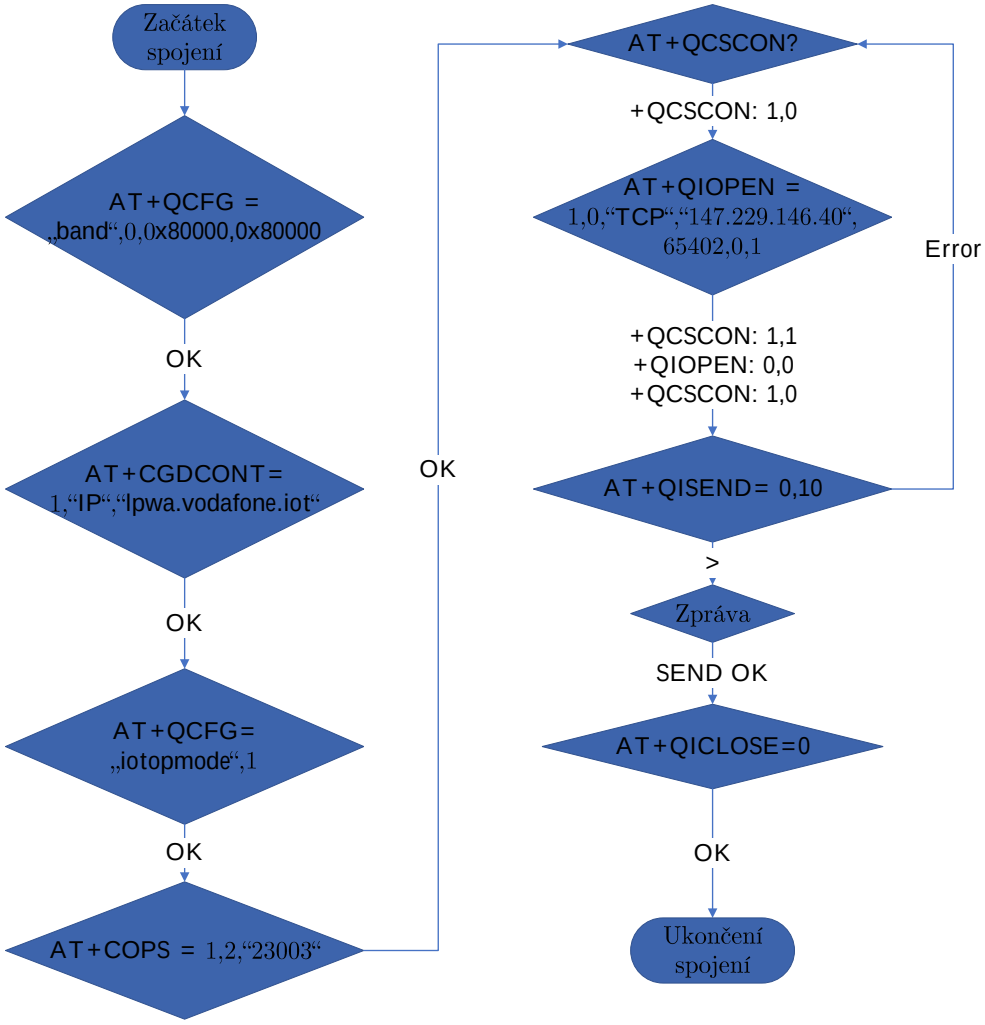
Kvůli náročnému způsobu testování sítě a následné práci s modulem došlo k výměně modulu BG770A-GL za BG77. Starší školní projekt pracoval s Raspberry Pi Compute Module 4 a komunikačním modulem BG77, pro který používají software DietPi, který prošel potřebnou úpravou, a umožňuje jednoduchou práci s modulem a platformou Raspberry Pi CM4. Software sám automaticky píše AT příkazy, takže je možné spustit běžné potřebné linuxové programy. Modul Quectel BG77 je vybaven bez limmitní SIM kartou od společnosti Vodafone. Modul je připojený k desce Raspberry Pi Compute Module 4 10 Board pomocí USB 2.0 a UART 4.6 [22]. Ke komunikačnímu modulu je připojená anténa.

BG77 je kompaktní LPWA modul splňující požadavky 3GPP 14. vydání. Mezi vlastnosti modulu patří podpora LTE Cat M1, LTE Cat NB1/NB2 sítí. Nízká spotřeba energie je zajištěná díky procesoru ARM Cortex A7 s integrovanou RAM a flash. Modul má rozměry 14,9 x 12,9, x 1,9 mm. Podporované frekvenční pásma využívaná v České republice, a to B8 a B20 pro LTE Cat M1 i LTE Cat NB1/NB2. Maximální rychlosti přenosu dat, které modul umožňuje, jsou pro Cat M1 ve 14. vydání 588 kb/s DL a 1119 kb/s UL. U NB1 jsou rychlosti 32 kb/s DL a 70 kb/s UL a u NB2 127 kb/s DL a 158,5 kb/s UL. Maximální vysílací výkon modulu je 21 dBm [22].

Mezi klíčové vlastnosti modulu patří extrémně nízká spotřeba energie, integrovaná RAM a flash. Modul dále obsahuje velké množství internetových protokolů, možnost externího rozšíření a modifikace modulu podle potřeby, dále má USB 2.0 interface a kompaktní velikost. Modul je velmi podobný předchozímu používanému modulu BG770A-GL a díky tomu jsou AT příkazy pro ovládání stejné [22].

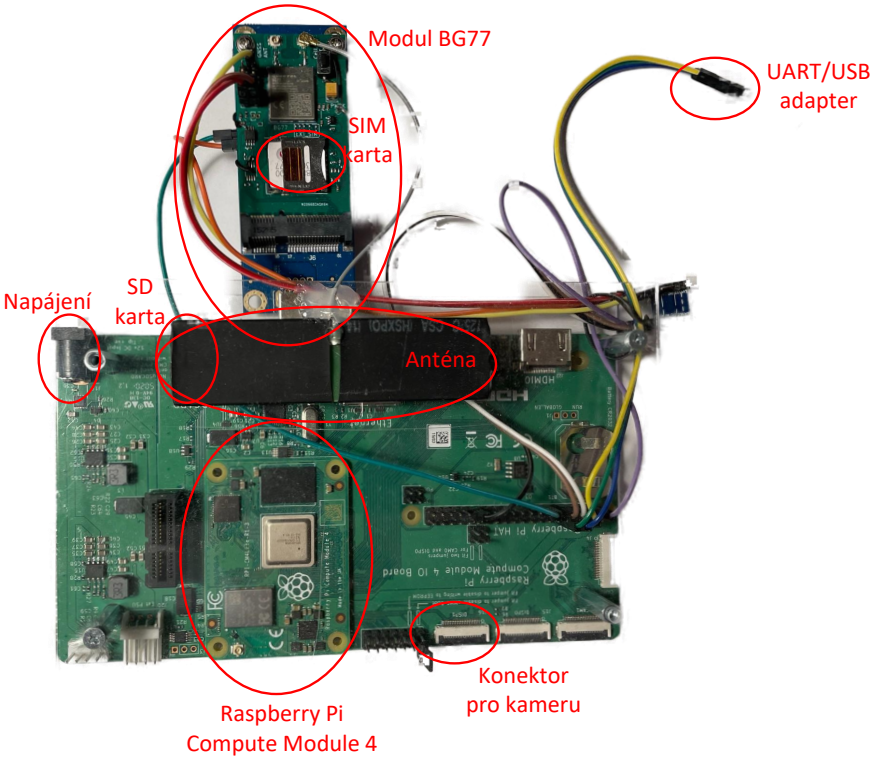
## 4.5 Výběr platformy

Pro praktickou část práce byla vybrána platforma Raspberry Pi Compute Module 4. Platforma disponuje 64 bitový čtyřjádrovým procesorem Broadcom BCM2711 quad-core Cortex-A72 (ARM v8) 64-bit SoC @ 1,5 GHz a 4 GB RAM. Dále obsahuje konektor pro externí anténu, integrovaný Gigabit Ehternet s podporou IEEE 1588,




Obr. 4.5: Vývojový diagram spojení modulu se serverem a odeslání dat.

USB 2.0 rozhraní, PCIe Gen 2 rozhraní, 28 GPIO a rozhraní pro SD karu. Rozměrny jsou 55 x 40 mm, příkon je 5V DC a provozní teplota 0 - 80 °C [23].




Obr. 4.6: Zařízení skládající se z Modulu BG77 a Rpi CM4.

Platformu Raspberry Pi CM4 je potřeba zapojit do rozšiřující desky, kterou jsem si vybral Raspberry Pi CM4 IO Board. Deska obsahuje dva FPC MIPI DSI konektory, dva FPC MIPI CSI-2 konektory na kameru, HAT konektor, Ralt-time clock, dva konektory pro HDMI, jeden Gigabit Ehternet konetkor, dva USB 2.0 konektory, DC powerjack, PCle, čtyřiceti pinový GPIO header a slot pro MicroSD kartu. Deska se musí samostatně napájet vstupním napětím 5-12 V [23].

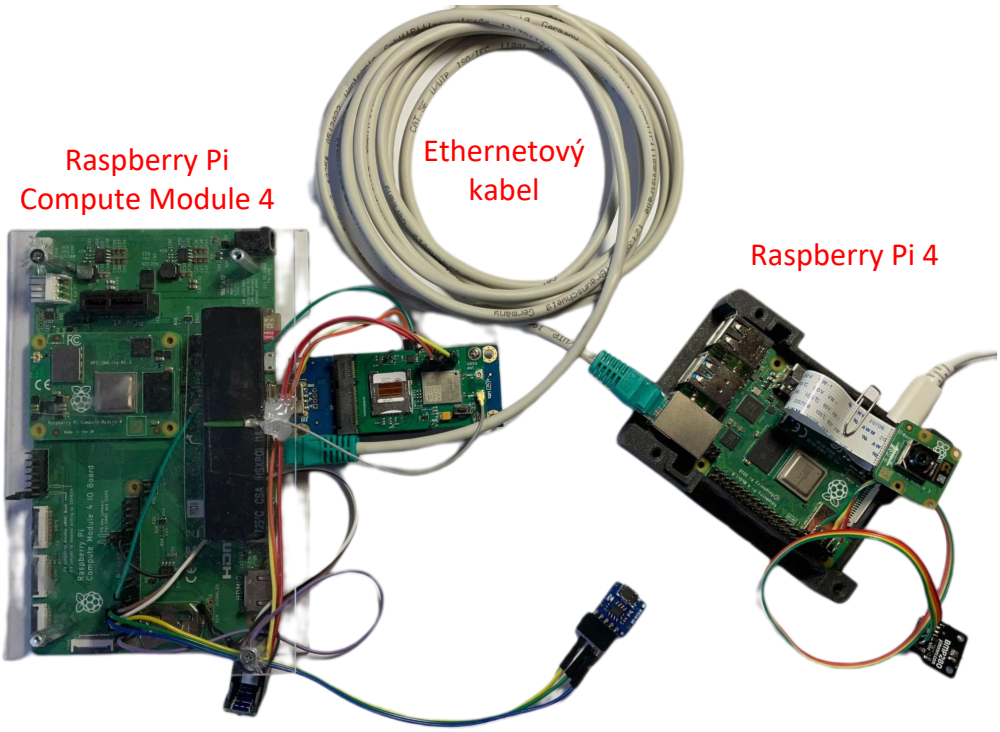
K rozšiřující desce Raspberry Pi CM4 IO Board je připojené Raspberry Pi CM4, MicroSD karta se softwarem a komunikační modul BG77 pomocí USB konektoru a UART rozhraní, protože bez UART rozhraní by nešlo vypisovat informace o síti, jako jsou např. typ sítě, frekvenční pásmo, SINR, RSRP a další. Z UART rozhraní na desce vede také připojení k PC s redukcí na USB. Celá platoforma se spustí piřpojením desky do elektrické sítě.

Na zařízení ja nahraný software DietPi, který je upravený pro LPWA komunikaci a projení jednotlivích částí zařízení potřebných pro funkci. Systém byl již používán u jiného podobného projektu, a protot byl převzat i pro tuto bakalářskou práci. Důvod převzetí systému byla nemožnost otestování vlastností NB-IoT sítě pomocí programu Iperf3 v terminálu YAT a jednoduchých AT příkazů. Zařízení se ovládá pomocí linuxového příkazového řádku a díky úpravě pro LPWA komunikaci s mo-

dulem BG77 není potřeba pro komunikaci zadávat jednotlivé AT příkazy, protože je zadává systém automaticky místo uživatele. Díky tomu je možné naisntalovat Iperf3 knihovnu a provést otestování sítě.

## 4.6 Přidání Raspberry Pi 4

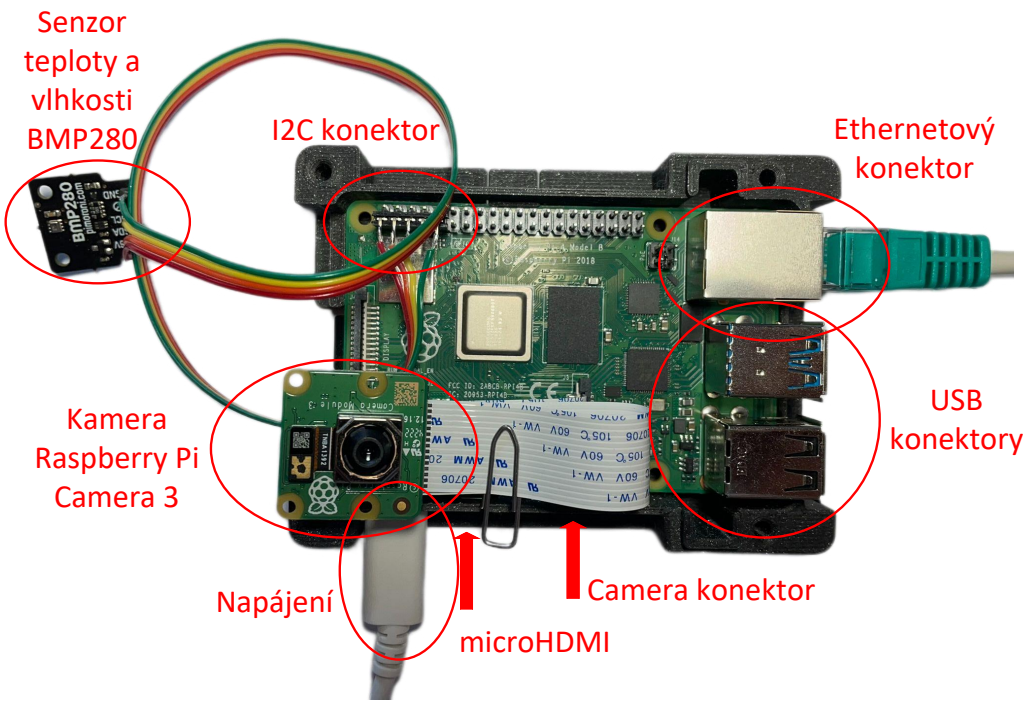
Zařízení Raspberry Pi CM 4 s komunikačním modulem BG 77 má speciálně upravený systém DietPi s několika programy, které fungují pod systémovým démonem. Patří mezi ně upravený Modemmanager a Networkmanager, které jsou upravené přímo na míru pro systém DietPi a práci s modulem BG 77. Z toho důvodu bylo při pokusech o instalaci balíčků a knihoven pro ovládání kamery velmi složité a rizikové, došlo tedy ke změně zařízení, které bude měřit potřebné hodnoty, a to na Raspberry Pi 4 model B 4G RAM. Propojení mezi Raspberry Pi 4 a CM4 je pomocí kříženého ethernetového kabelu 4.7. Na obou zařízeních se musela nastavit statická IP adresa, aby se zařízení navzájem viděla a mohla spolu komunikovat. Komunikace probíhá pomocí knihovny socket v programu vytvořeném v Pyhton3.




Obr. 4.7: Propojení Raspberry Pi 4 a Raspberry Pi Compute Module 4.

Zařízení Raspberry Pi 4 model B 4 GB RAM 4.8má v této konfiguraci 4 GB RAM paměti typu LPDDR4, 28 nm a 1,5 GHz čtyřjádrový procesor ARM Cortex-

A72 s podporou videa až 4Kp60. Zařízení dále obsahuje napájecí konektor USB-C, dva microHDMI konektory, Ethernetový port a dvě USB 2.0 a dvě USB 3.0. Součástí jsou i i2c konektory a konektor pro Raspberry Pi cameru. Raspberry také umožňuje WiFi a Bluetooth 5.0 připojení. Dále se zde nachází slot na SD kartu, na které je i operační systém Raspbian Raspberry Pi OS 32-BIT [24].




Obr. 4.8: Raspberry Pi 4 se senzory.

## 4.7 Senzory

Zařízení musí měřit teplotu a v případě jejího překročení poslat fotografii prostředí i s teplotou na server. Pro měření teploty se zde používá senzor Pimoroni BMP280 4.9, který má i2c připojení a dovede měřit také tlak a nadmořskou výšku. Rozmezí měřitelných teplot senzoru je od -40 °C do +85 °C s přesností +-1 °C, tlak s rozmezím 300 - 1100 hPa s přesností +-1 hPa a nadmořská výška s přesností +- 1 metr. Ovládání senzoru probíhá pomocí python knihoven a programů bmp280 a bmp280-python, které jsou volně k dispozici od výrobce. Pro práci se senzorem tedy stačí využít předem připravený programový kód v jazyce python [25].

Pro zaznamenání fotografie se zde používá kamera Raspberry Pi Camera 3 4.10. Jedná se o kameru se senzorem Sony IMX708 a rozlišením 12 Mpx, automatic-

Obr. 4.9: Senzor teploty a vlhkosti BMP280.

kým ostřením, podporou HDR a rozlišením snímače 4608 x 2592 px. Mezi další parametry kamery patří digitální zorné pole 75° a vertikální zorné pole 41°, minimální zaostřovací vzdálenost 10 cm, maximální doba expozice 112 s a minimální zaostřovací vzdálenost 10 cm. Pro práci s kamerou se používá knihovna Picamera2, která je založená na libcamera. Picamera2 i libcamera jsou předem nainstalované na Raspberry Pi 4 se systémem Raspbian Raspberry Pi OS 32-BIT. Pro používání v python programu se musí importovat knihovna Picamera2 a libcamera [26].

## 4.8 Bateriové napájení

Zařízení musí být napájeno baterií pro svou práci v lese. Napájení je zde zajištěno pomocí 10 baterií 18650 3,7V 2600mAh ICR18650P - 5C Doublepow. Jedna baterie má více jak 500 nabíjecích cyklů a kapacitu 2600 mAh. Jelikož je jmenovité napájení na jedné baterii 3,7 V, musí dojít k sériovému zapojení dvou baterií, aby bylo napětí 7,4 V. Baterie jsou tedy sériově zapojené po dvojcích kvůli navýšení napětí a následně zapojeny paralelně, pro navýšení celkové kapacity, která naroste až na 13000 mAh. Na obou zařízeních je vstupní napětí +5 V, musí zde být tedy také step-down měnič napětí. Používá se zde Step down nastavitelný měnič s LM2596 DC-DC, který mění

Obr. 4.10: Kamera Raspberry Pi Camera 3.

vstupní napětí z rozsahu 4,5 V - 40 V na výstupní napětí v rozsahu 3 V - 35 V a výstupní proud je zde 3 A. Napětí z baterií 7,4 V se sníží na požadovaných 5 V na napájení obou zařízení [27, 28].

Obr. 4.11: Baterie s měničem napětí a konektory pro zapojení zařízení.

# 5 Testování NB-IoT sítě

Pro ověření správného fungování modulu a platformy a následný výběr vhodného aplikačního protokolu můsí dojít k testu sítě. Pro test jsou vhodné programy Iperf3 a PING, kdy se pomocí Iperf3 změří přenosové rychlosti a celkové množství přenesených dat, a pomocí PING se změří zpoždění. V průběhu všech měření se také zaznamenávali rádiové podmínky z výpisu modulu. Celková měření jsou zaznamenána v příloze.

## 5.1 Měření pomocí Iperf3

Iperf3 musí být nainstalováno na obou zařízeních, mezi kterými probíhá test. Testování proběhlo mezi modulem a LPWAN Wislab serverem, na které se vytvoří Iperf3 server s nasloucháním na portu 65402. Na zařízení se následně spustí klient a v příkazu musí figurovat IP adresa serveru, port na kterém server naslouchá a případně další volitelné podmínky. Příkazy použité pro testování s Iperf3 [29]:

- Zprovoznění iperf3 serveru - iperf3 -s -p 65402 (-s značí server a -p port, na kterém sever naslouchá).
- Příkaz zajišťující komunikaci - iperf3 -c 147.229.146.40 -w 8000 -t 90 -i 5s -p 65402.
  - -c - značí klienta a následuje IP adresa, na kterou se klient připojuje.
  - -w - značí velikost zprávy v bytech.
  - -t - určuje délku testování v sekundách.
  - -i - určuje interval mezi jednotlivými dotazy.
  - -p - značí port, na kterém naslouchá server.

Testování proběhlo v Brně a Jeseníku. Proběhlo celkem 21 testů, kdy každý test měl větší velikost zprávy. Začátek byl 8000 B a poslední velikost zprávy pro test byla 350000 B. Při každém testu se zaznamenaly rádiové podmínky jako RSRP, SINR a ECL. Z výsledků testování po 90 sekundách jsou v tabulce zaznamenány hodnoty Uplink a Downlink na straně klienta a serveru. Další zaznamené hodnoty jsou celková velikost odeslaných dat za dobu 90 sekund na straně Sendera a Recievera a opakovanému zaslání TCP paketů.

Z výsledků měření, které jsou v tabulce 5.1, můžeme říci, že lepší rádiové podmínky byly v Jeseníku, díky kterým byly i větší průměrné přenosové rychlosti. Výsledné průměrné rychlosti v Jeseníku jsou na straně klienta UL = 46,98 kb/s, DL = 39,83 kb/s a na straně serveru UL = 40,84 kb/s, DL = 34,67 kb/s. Nejvyšší dosažená rychlost byla na straně klienta, kdy se UL = 63,40 kb/s a nejmenší na straně serveru DL = 30,7 kb/s. V Brně s horšími rádiovými podmínkami, jak může být viděno v tabulce výsledných hodnot pro Brno 5.2, rychlosti dosahovali průměrných

hodnot na straně klienta UL = 43,81 kb/s, DL = 34,13 kb/s a na straně serveru UL = 39,87 kb/s, DL = 30,93 kb/s. Nejvyšší dosažená rychlost byla opět na straně klienta s UL = 57,4 kb/s a nejnižší na straně serveru s DL = 17,2 kb/s. Kompletní měřená data pro různé velikosti jsou v tabulce v příloze.

Při porovnání měřených dat s těmi teoretickými 1.1 můžeme vidět, že i v případě dobrých rádiových podmínek v Jeseníku, kdy SINR byl průměrně 18 dB a RSRP průměrně -69 dBm, přenosové rychlosti zdaleka nedosahovali maximálních teoretických rychlostí. Maximální teoretická hodnota UL = 159 kB/s a naše největší změřená hodnota byla v Jeseníku UL = 63,3 kb/s. U porovnání downlinku je rozdíl v poměru větší, kdy maximální teoretická hodnota DL = 127 kb/s a maximální změřená DL = 41,8 kb/s. Pro přiblížení se teoretickým rychlostem by musely být rádiové podmínky velmi dobré. Jedná se o porovnání nejlepších možných přenosových rychlostí u verze LTE Cat NB2, v případě porovnání s verzí LTE Cat NB1 by byly hodnoty více než výborné, protože u NB1 dosahuje maximální UL = 62,5 kb/s a maximální DL = 27,2 kb/s. Rádiové podmínky a přenosové rychlosti tedy dostačují pro jednoduchý přenos malého množství dat, jako údaje o teplotě a vlhkosti a fotografickém snímku měřeného prostředí.

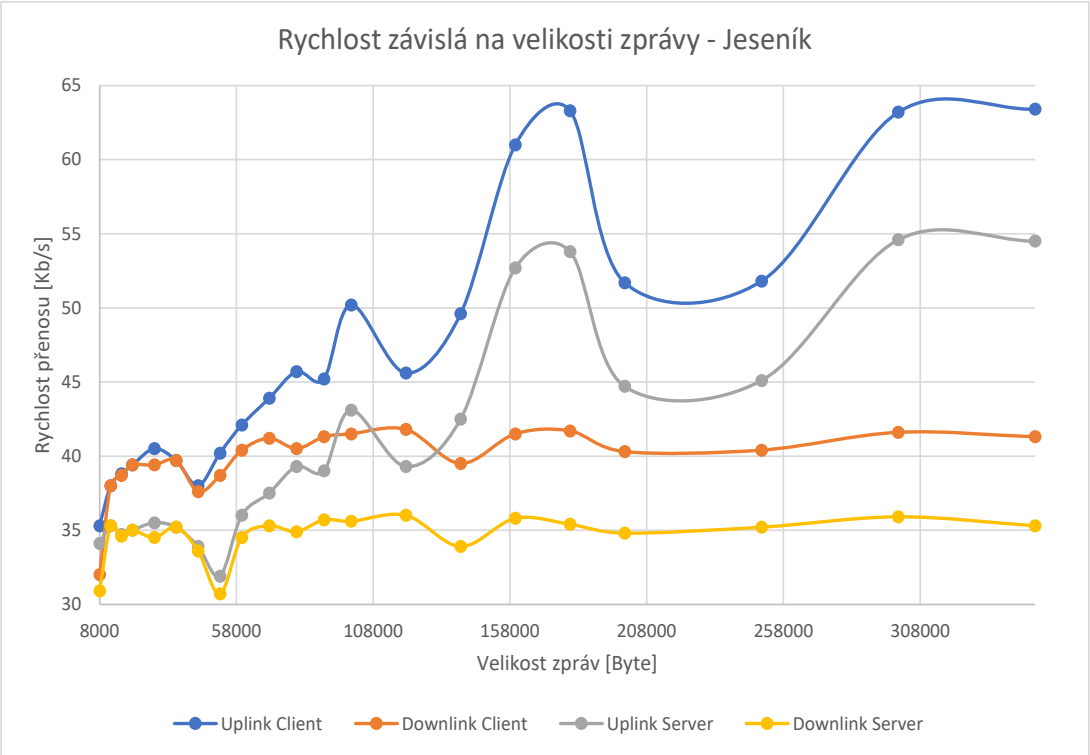
| Jeseník | Průměr | Maximum | Minimum |
|---|---|---|---|
| RSRP [dBm] | -69.33 | -73 | -68 |
| SINR [dB] | 18.04 | 22 | 13 |
| UL C [kbit/s] | 46.98 | 63.4 | 35.3 |
| DL C [kbit/s] | 39.83 | 41.8 | 32 |
| UL S [kbit/s] | 40.84 | 54.6 | 31.9 |
| DL S [kbit/s] | 34.67 | 36 | 30.7 |
| Přenesená data Sender [kB] | 516.04 | 696 | 387 |
| Přenesená data Reciever [kB] | 437.52 | 459 | 352 |
| Retr | 2.09 | 11 | 0 |

Tab. 5.1: Tabulka výsledných měřených hodnot z Jeseníku.

Na výsledných hodnotách lze vidět, jak rychlosti rostly s navyšujícímmi se velikostmi posílaných zpráv a zároveň, jak docházelo i k většímu počtu celkových přenesených dat. Vypracované grafy jsou pro rychlosti v Jeseníku 5.1 a v Brně 5.2, dále jsou zde 2 grafy pro celkový počet odeslaných zpráv, na kterých lze vidět také nárůst, pro Jeseník 5.3 i Brno 5.4.

| Brno | Průměr | Maximum | Minimum |
|---|---|---|---|
| RSRP [dBm] | -75.71 | -77 | -74 |
| SINR [dB] | 2.48 | 4 | -5 |
| UL C [kbit/s] | 43.81 | 57.4 | 23 |
| DL C [kbit/s] | 34.13 | 40.8 | 19.5 |
| UL S [kbit/s] | 39.87 | 52.5 | 20.3 |
| DL S [kbit/s] | 30.93 | 35.5 | 17.2 |
| Přenesená data Sender [KB] | 481.52 | 631 | 253 |
| Přenesená data Reciever [KB] | 375.143 | 448 | 215 |
| Retr | 8.6 | 17 | 2 |

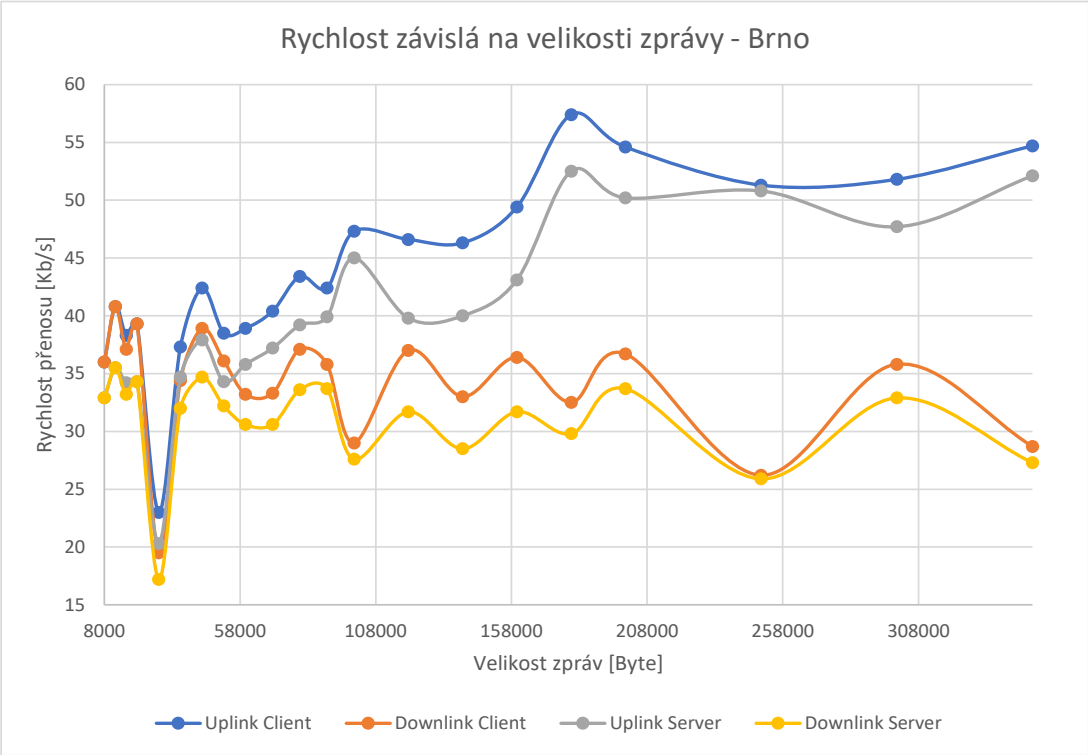
Tab. 5.2: Tabulka výsledných měřených hodnot z Brna.




Obr. 5.1: Rychlost závislá na velikosti zprávy - Jeseník.

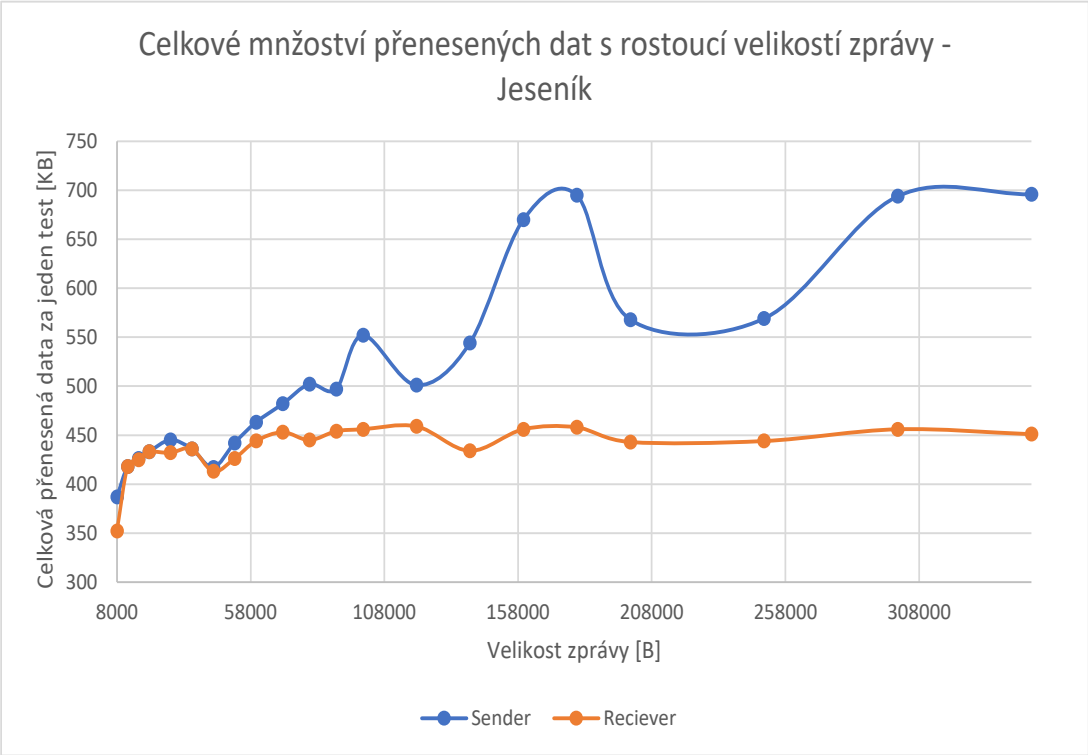
## 5.2 Měření pomocí PING

Jelikož program Iperf3 neumožňuje měření zpoždění, musí se měření zpoždění provést pomocí PING. Příkaz, pomocí kterého probíhalo měření: ping 147.229.146.40 -s 8000 -c 20, kde -s znační velikost odeslané zprávy, -c znační počet zaslání zpráv ping. U velikosti 16000 B a výše přestal ping procházet a ztrátovost byla 100 %. Důvodem

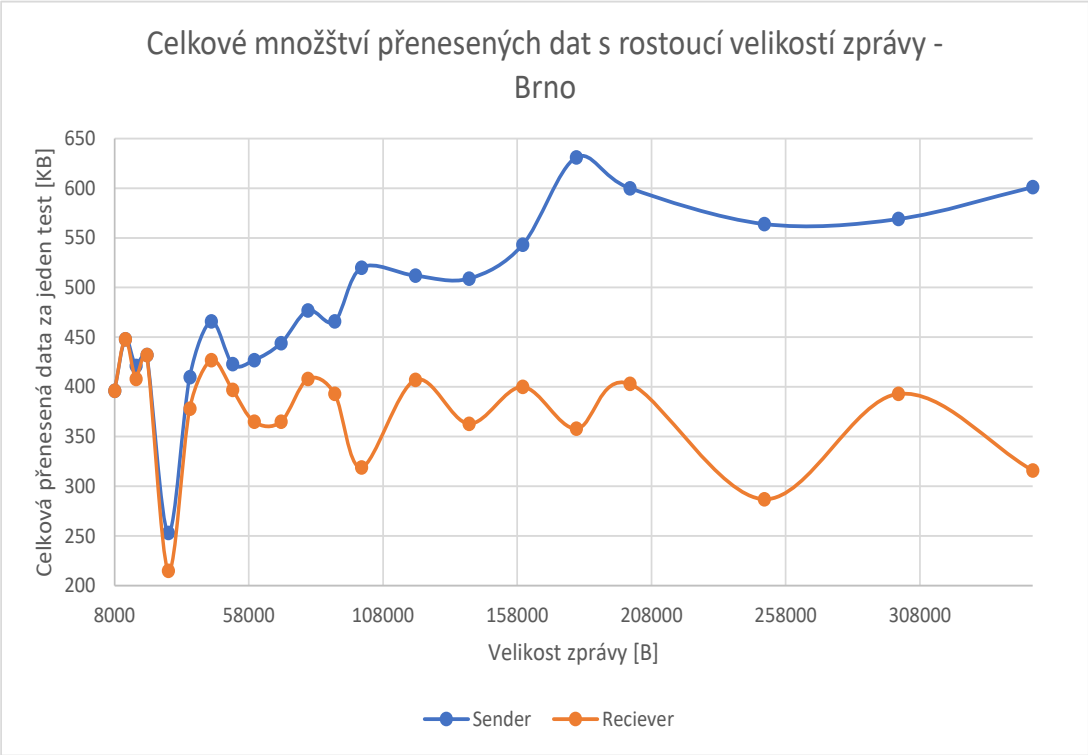



Obr. 5.2: Rychlost závislá na velikosti zprávy - Brno.

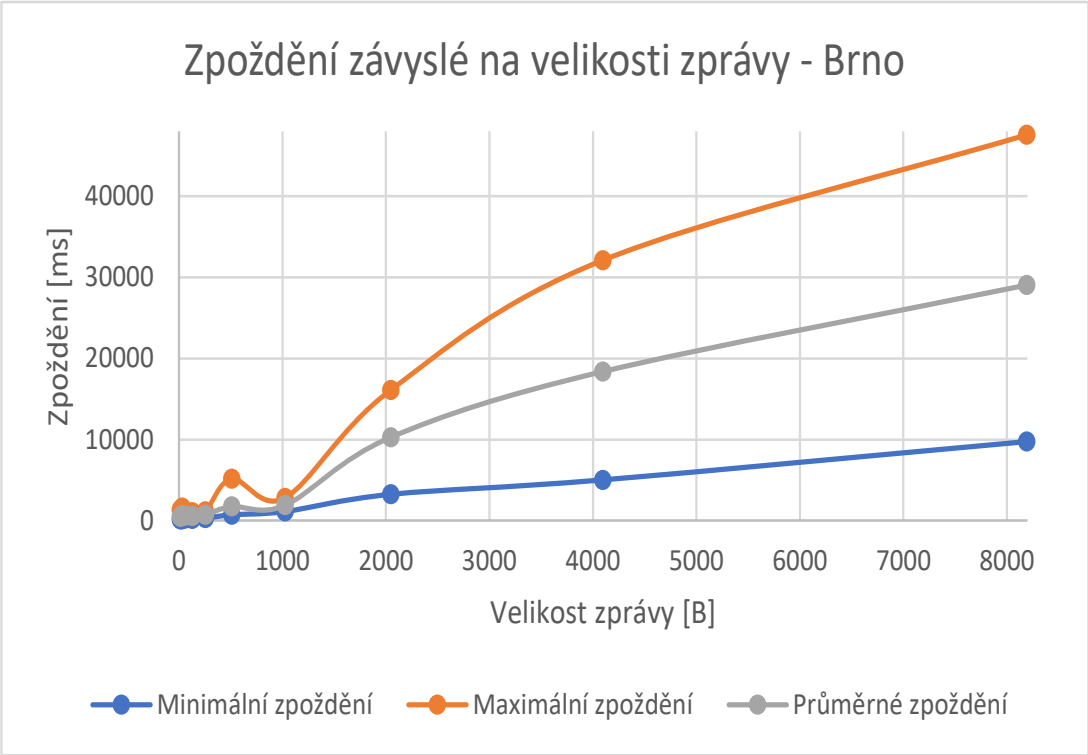
bylo, že na rozdíl od programu Iperf3, PING nedokáže provádět fragmentaci dat a tak větší velikosti zpráv neprojdou a dojde ke 100 % ztrátovosti a zahození. Proto muselo dojít k měření velikostně menších zpráv s počátkem u 12 B až do 16384 B. V měření se zaznamenávalo minimální, maximální a průměrné zpoždění. U velikosti zprávy bylo průměrné zpoždění 538 ms, které pomalu rostlo, až do velikosti zrpávy 512 B, kde došlo k velkému skoku zpoždění na 1758 ms a velmi rostlo. U velikosti zprávy 16384 už nedocházelo k průchodu a byla 100 % ztrátovost. Průběh zvyšování zpoždění jde vidět v grafu 5.5. Rádiové podmínky byly špatné v době měření a mohlo to tedy také ovlivnit výsledné zpoždění a tedy způsobit větší hodnoty, které mohou odpovídat reálných podmínkám v lese, protože ideální podmínky mít zařízení nebude.




Obr. 5.3: Celkové množství přenesených dat s rostoucí velikostí zprávy - Jeseník.




Obr. 5.4: Celkové množství přenesených dat s rostoucí velikostí zprávy - Brno.




Obr. 5.5: Velikost zpoždění s rostoucí velikostí zprávy - Brno.

# 6 Program

Pro finální používání se musí vytvořit program, který bude v předem určených časových oknech měřit teplotu a v případě překročení určité hodnoty program udělá fotografii prostředí a změřená data s fotografií uloží a pošle na druhé zařízení pomocí knihovny socket na Raspberry Pi CM4 zařízení, které pomocí aplikace Stunnel pošle data i s fotografií na server. Pro spojení mezi zařízeními se používá ethernetový kabel a knihovna socket, kdy je první zařízení, které měří teplotu za klienta a druhé zařízení, které posílá data na LPWAN server jako server, který přijímá data. Na obou zařízeních musí být python program, pomocí kterého přeposílání funguje. Všechny programy se nacházejí přidané v příloze.

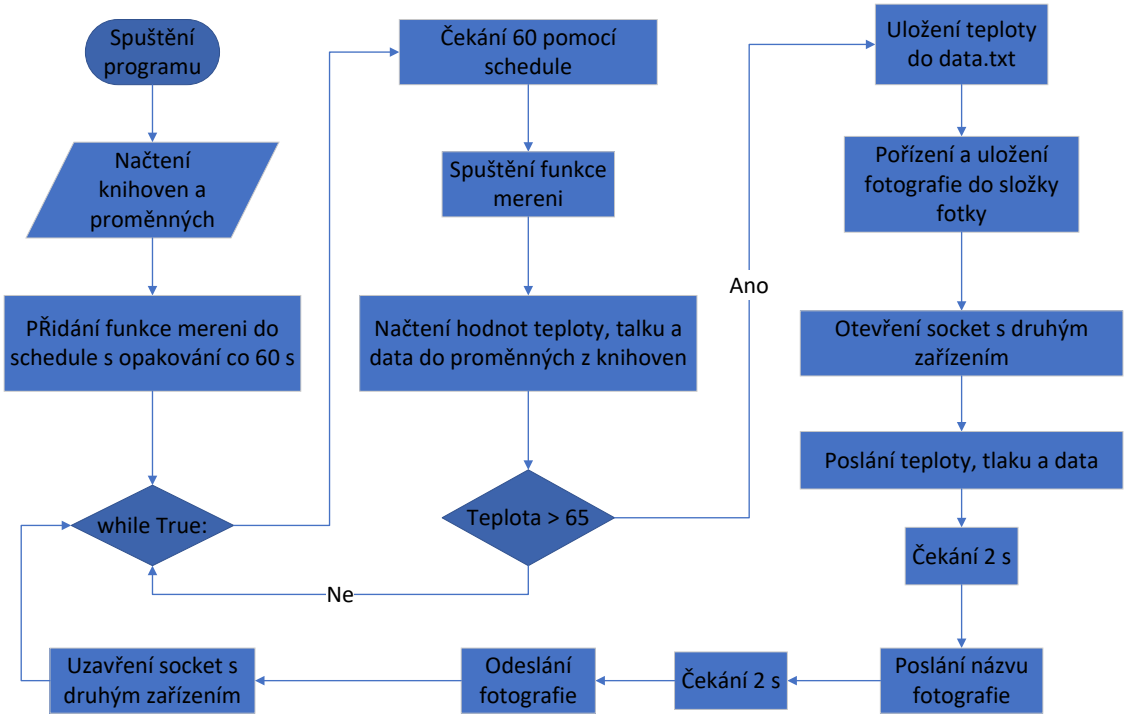
## 6.1 Client - Raspberry Pi 4

V programu na straně klienta se pro měření teploty používá knihovna bmp280, pomocí které dochází k měření teploty a tlaku. Měření probíhá každou 1 minutu a v případě překorčení teploty 65 °C se pořídí fotografie pomocí knihovny libcamera. Pořízená fotografie je ve sníženém rozlišení 1280x720 px, protože fotografie v plné velikosti by se přenášela pomocí NB-IoT velmi dlouho, jak lze usoudit z výsledků měření rychlostí. Zvolené rozlišení je ještě dost velké na rozpoznání obrazu, ale dostatečně malé, aby se snáze přeneslo na LPWAN server.

Změřené hodnoty se i s fotografií uloží na SSD disk zařízení a pošlou pomocí knihovny socket na druhé Raspberry Pi, které je zde jako server. Teplota s tlakem se uloží do souboru data.txt a přidá se navíc i aktuální datum a čas změření. Fotografie se ve formátu jpg uloží do složky fotky s názvem aktuálního data a času pořízení fotografie. Pro zjištění aktuálního data a času se používá knihovna datetime, kdy se do proměnné datum uloží datum a čas před každým měřením. Čas je tedy stejný u teploty s tlakem a fotografie, i když je zde rozdíl změření a pořízení několik sekund. Opakování měření probíhá pomocí knihovny schedule, která každých 10 minut vyvolá funkci mereni, která provádí měření, vyfocení prostředí, ukládní a odesílání na druhé zařízení.

Odesílání na druhé Raspberry Pi zařízení, které funguje jako server probíhá pomocí knihovny socket. Pro propojení a vzájemnou komunikaci je na obou zařízeních nastavená statická IP adresa pro ethernetový port. Statiká IP adresa na Raspberry Pi 4 je 192.168.1.5/24 a na Raspberry Pi CM4 192.168.1.6/24. Při odesílání se zařízení (client) připojí na druhé zařízení (server), následně pošle jako první zprávu tepolotu, tlak, datum a čas v textové podobě a přijme odpověď ze strany serveru o úspěšném přijetí. Druhá odeslaná zpráva je název fotografie, která se bude odesílat a opět přijme klient potvrzení o doručení názvu. Nakonec dojde k odeslání fotografie,

která se neposílá celá najednou, ale rozdělí se na balíčky o velikosti 2048 B, které se postupně posílají na server. Po odeslání fotografie dojde k odpojení od serveru a ukončení komunikace. Znázornění celého programu u Raspberry Pi 4 je zobrazeno ve vývojovém diagramu 6.1.

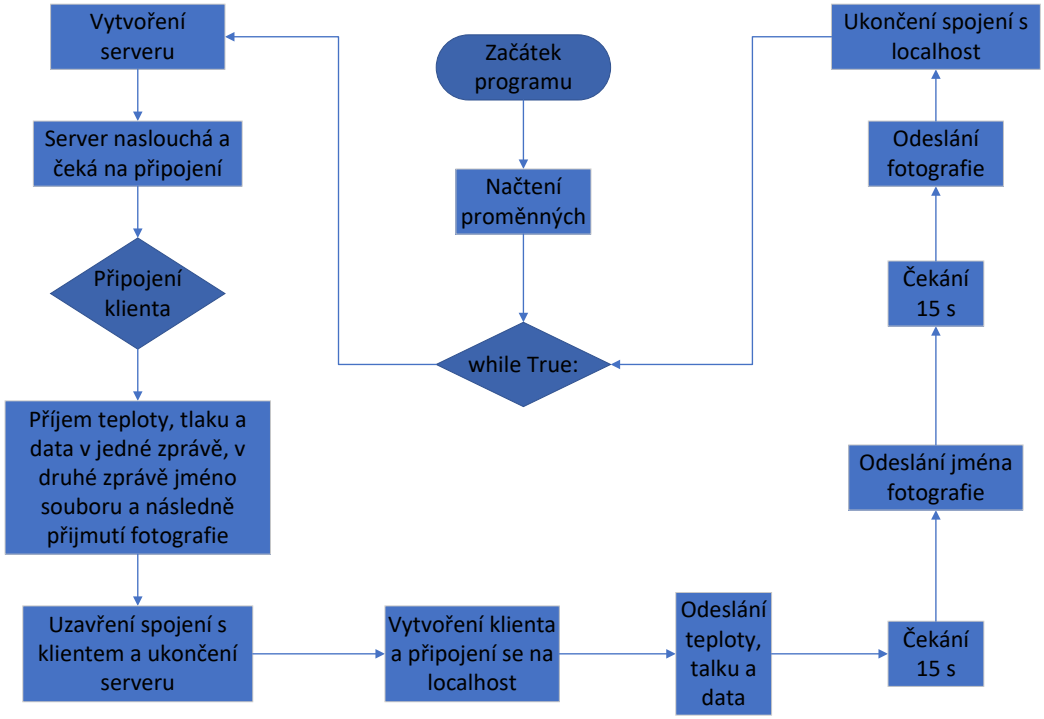



Obr. 6.1: Vývojový diagram programu BP.py na Raspberry Pi 4.

## 6.2 Server - Raspberry Pi CM4 a LPWAN server

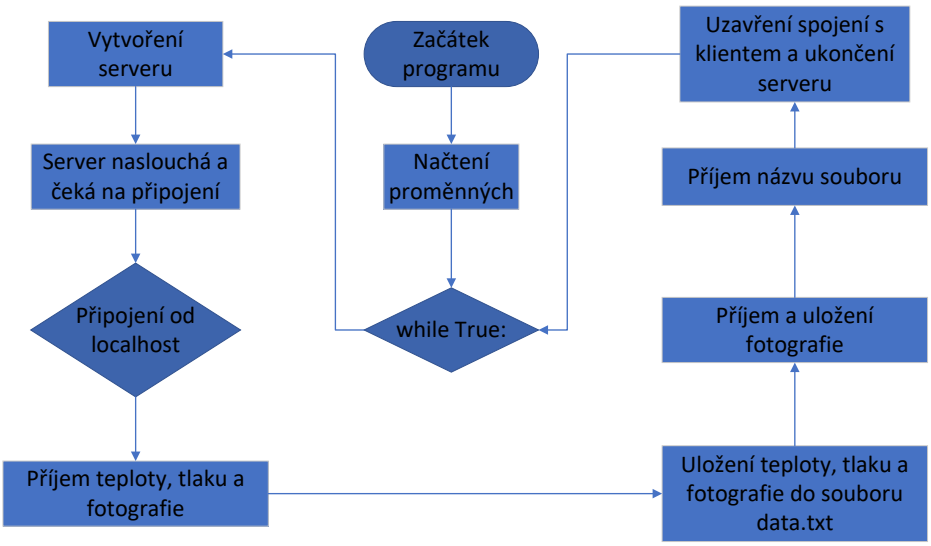
Druhé zařízení Raspberry Pi CM4 je bráno jako server pro komunikaci s prvním zařízením. V druhém programu jsou tři funkce startServer, startConnection a dataPrijem. Funkce startServer vytvoří server, který naslouchá na portu 6401, funkce startConnection naslouchá a čeká na připojení a funkce dataPrijem přijímá zprávy a fotografii. Po ukončení naslouchání a úspěšném připojení server čeká na první zprávu, na kterou po přijetí odpoví ověřovací zprávou o příjmu zprávy. První zpráva jsou změřená data. Následně čeká na druhou zprávu, na kterou také odpovídá a uloží si ji do proměnné name pro vytvoření fotografie. Nakonec funkce dataPrijem vytvoří fotografii do složky fotky ve formátu jpg s názvem, který byl doručen v druhé zprávě a postupně přijímá balíčky o velikosti 2048, dokud nepřijde celá fotografie.

Kompletní data fotografie se uloží a server ukončí spojení a dojde k jeho kompletnímu vypnutí. Znázornění celého programu u Raspberry Pi Compute Module 4 je zobrazeno ve vývojovém diagramu 6.2.




Obr. 6.2: Vývojový diagram programu switch.py na Raspberry Pi Compute Module 4.

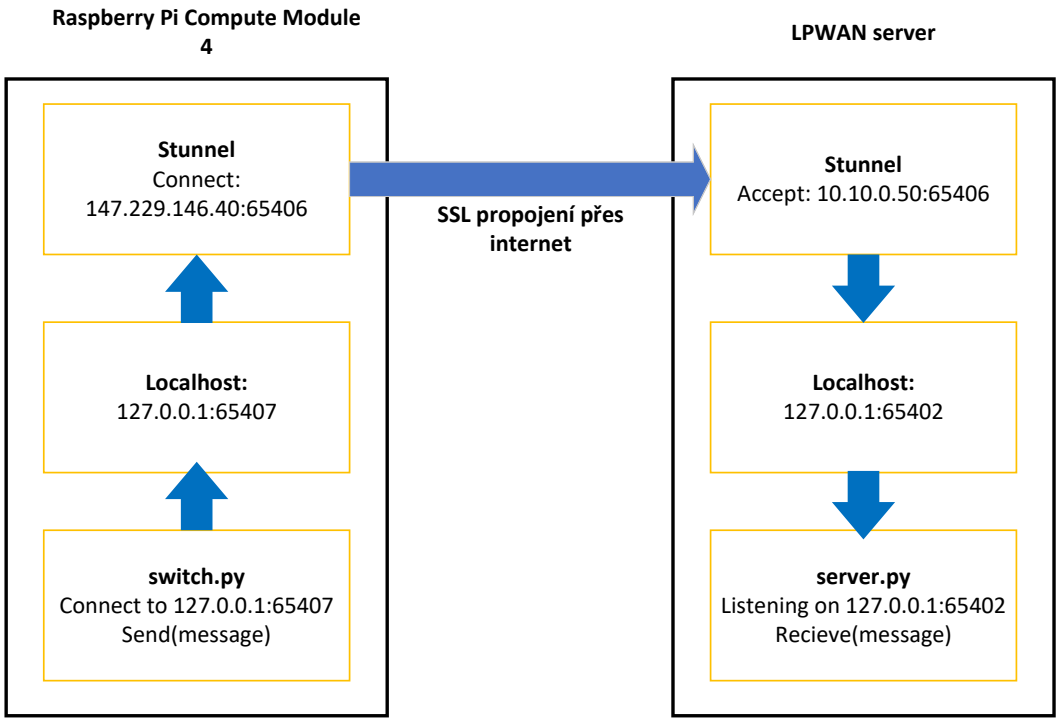
Následně dojde k zapnutí klienta na zařízení Raspberry Pi CM4, který pošle data na localhost 127.0.0.1 s portem 65407, na kterém naslouchá stunnel. Stunnel data postupně příjmá a posílá na LWAN server, kde dojde k poslání dat na localhost 127.0.0.1 s portem 65407, na kterém naslouchá python program, který se chová v architektuře socket jako server a přijmá data i fotku. Data uloží do souboru data.txt a fotku do složky fotky. Aktuální klient na zařízení Raspberry Pi CM4 uzavře spojení na klientovi, přepne se opět na server a čeká na příjem dat z prvního zařízení. Program serveru na LPWAN serveru ukončí spojení a opět naslouchá na adrese 127.0.0.1 a portu 65407. Znázornění celého programu na LPWAN serveru je zobrazeno ve vývojovém diagramu 6.3.




Obr. 6.3: Vývojový diagram programu server.py na LPWAN serveru.

## 6.3 Stunnel

Pro zabezpečené propojení mezi zařízením a LPWAN serverem je potřeba využít aplikaci, která zajišťuje zabezpečený přenos dat. Vhodným řešením je Stunnel, který zajišťuje zabezpečené spojení TLS (Transport Layer Security). Stunnel se musí nainstalovat na obou stranách a provést vhodnou konfiguraci, kde se nastaví u klienta adresa s portem, na které stunnel naslouchá, tedy 127.0.0.1 a 65407 a následně, na kterou se připojuje 147.229.146.40 s portem 65406. Na serveru je nastavení opačné, tedy nejprve stunnel naslouchá na adrese serveru se zadaným portem 10.10.0.50 a 65406 a přijatá data následně posílá na adresu 127.0.0.1 s portem 65402. Pro lepší vizualizaci je zde grafické znázornění fugnování Stunnel na zařízení a LPWAN serveru 6.4. Pro zabezpečení se zde používá bezpečnostní klíč a certifikát, který byl ze serveru nasdílen na zařízení a jsou tak stejné.




Obr. 6.4: Grafické zobrazení fungování Stunnel na zařízení a serveru.

# Závěr

Bakalářská práce je zaměřená na teoretické zpracování LPWAN (Low Power Wide Area Network) technologií, následný výběr jedné technologie a její použití v praxi. Následně je úkolem sestavit zařízení, které bude snímat teplotu a fotografie prostředí a v případě překročení povolených hodnot výsledky pošle na LPWAN server.

V první kapitole se v semestrální práci nachází úvod do Internetu věcí, rozdíl mezi H2H(Human to Human) a M2M (Machine to Machine) komunikací a porovnání jednotlivých LPWAN sítí a jejich základní popis.

V druhé kapitole je práce zaměřená na podrobný popis technologií v licencovaném frekvenčním pásmu NB-IoT a LTE Cat-M.

Třetí kapitola je zaměřená na aplikační protokoly LPWAN, které jsou MQTT (Message Queue Telemetry transport), CoAP (Constrained Application Protocol) a LWM2M (Leightweight M2M). Ve třetí kapitole se dále nachází i popis zajiště zabezpečení dat.

Ve čtvrté kapitole se náchází začátek popisu praktické části bakalářské práce. Pro zajištění komunikace je vybrán modul BG770A-GL. Pro zprovoznění modulu bylo potřeba zkompletování modulu s vývojovým kitem a provést registraci do Vodafone sítě. Zprovozněná komunikace proběhla mezi modulem a LPWAN WislabServer 5 serverem pomocí transportního protokolu TCP (Transmission Control Protocol). Přenesená zpráva byla Ahojtest22.

Pro pokračování v praktické části bylo potřeba otestovat síť pro pozdější potřeby využití technologie NB-IoT. Došlo tedy ke změně komunikačního modulu na BG 77, který byl spojený s Raspberry Pi Compute Module 4. Na Raspberry Pi Compute Module 4 je nahraný upravený systém DietPi, na kterém je upravený Modemmanager a Networkmanager pro práci s modulem BG 77. Díky úpravě se automaticky zařízení připojí k Vodafone NB-IoT síti a není zde potřeba zadávání AT příkazů, celý proces komunikace je tak automatizovaný a jednodušší pro práci. Následně proběhlo testování na dvou místěch, a to v Brně a v Jeseníku popsané v kapitole 5. Testování probíhalo pomocí aplikace Iperf a PING. Z výsledných hodnot vyplývá, že v Jeseníku byly mnohem lepší rádiové podmínky než v Brně a byla zde i lepší průměrná rychlost v Uplinku 46,98 Kbit/s, průměrná hodnota SINR 18.04 dB. V Brně byla průměrná rychlost v Uplinku 43,81 Kbit/s a průměrná hodnota SINR 2,48 dB.

Následně bylo potřeba vybrat si senzor na měření teploty a kameru pro pořízení fotografie okolního prostředí. Pro měření teploty se zde používá senzor Pimoroni BMP280 a pro pořízení fotografie Raspberry Pi Camera 3. Pro fungování kamery je potřeba, aby systém zvládal práci s kamerou a obsahoval knihovny Picamera2 a libcamera. Původně se měl senzor s kamerou připojit k Raspberry Pi Compute

Module 4, ale kvůli riziku poškození systému, který by musel být upraven pro práci s kamerou a potřeby správného fungování upravených programů pro práci s komunikačním modulem BG 77, muselo dojít ke změně zařízení, které bude provádět měření. Došlo tedy k rozdělení a používání dvou Raspberry Pi 4 a Compute Module 4. K Raspberry Pi 4 je připojený senzor teploty a kamera, pro jejíž fungování musela být zvýšena grafická paměť na zařízení.

Finální podoba zařízení je propojení dvou Raspberry Pi pomocí ethernetového kabelu. Jedno zařízení měří teplotu, fotí prostředí a výsledné hodnoty v případě překročení teploty pošle na druhé zařízení, které data následně pošle pomocí komunikačního modulu BG 77 a technologie NB-IoT na LPWAN server. Pro spojení obou zařízení bylo potřeba nastavit statické IP adresy na ethernetový port. Spojení mezi Raspberry Pi CM4 a LPWAN serverem je pomocí Stunnel. Měření teploty probíhá každou 1 minutu, teplota se analyzuje a v případě překročení teploty 65 °C dojde k vyfocení okolního prostředí, uložení dat na SDXC disk zařízení, odeslání teploty a fotografie na druhé zařízení, které je propojené s LPWAN serverem pomocí aplikace Stunnel. Na LPWAN serveru se nachází program v jazyce python, který naslouchá na výstupu Stunnelu a přijatá data ukládá, teplotu do souboru data.txt a fotografie do složky fotky.

Obě zařízení jsou napájená jednou velkou baterií, která je složená z 10 menších baterií s kapacitou 2600 mAh. Jednotlivé baterie jsou spojené sériově do dvojic kvůli navýšení napětí a jednotlivé dvojce jsou paralelně spojené pro navýšení kapacity. Celková kapacita je tedy 13000 mAh. Jelikož mají obě zařízení velkou spotřebu energie i při malém zatížení, tak zařízení nevydrží příliš dlouho zavislé pouze na baterii. Zvětšení výdrže obou zařízení by se dalo uskutečnit baterií s výšší kapacitou, ale jednalo by se o mnohem dražší řešení.

Celková finální podoba zařízení je pouze prototypem, který je kompromisem mezi požadavky zadání a aktuální možností reálné kostrukce. Pro lepší výdrž baterie by bylo vhodné využít jednodušší Raspberry Pi zařízení s lightweight operačním systémem. Toto řešení by zamezilo použití kamery, která kontroluje pomocí fotografií prostředí správné měření senzorů a snižuje tak riziko falešných poplachů. Způsob kontroly požárů také není vhodný, jelikož pouze kontrola teploty okolního prostředí může být nedostatečná. Aktuálně je problém sehnat vhodný senzor pro detekci kouře nebo požáru, protože většina senzorů není dostupná, nebo určená k detekci požáru mimo budovy. Ideálním řešením, by bylo vytvoření návrhu desky plošného spoje s využitím mikrokontroléru např. STM32LO, který umožňuje výdrž baterie na několik let.

# Literatura


[1] O. Liberg, M. Sundberg, E. Wang, J. Bergman, J. Sachs, and G. Wikström, *Cellular internet of things: from massive deployments to critical 5G applications.* Academic Press, 2019.

[2] P. B. R. Drápela and P. Mašek, "IMPLEMENTACE A VYHODNOCENÍ KOMUNIKAČNÍ TECHNOLOGIE LTE CAT-M1 V SIMULAČNÍM PROSTŘEDÍ NETWORK SIMULATOR 3," 2019.

[3] V. L. Kalyani and D. Sharma, "IoT: machine to machine (M2M), device to device (D2D) internet of everything (IoE) and human to human (H2H): future of communication," *J. Manag. Eng. Inf. Technol*, vol. 2, no. 6, pp. 17–23, 2015.

[4] A. Lavric, A. I. Petrariu, and V. Popa, "SigFox communication protocol: The new era of IoT?," in *2019 international conference on sensing and instrumentation in IoT Era (ISSI)*, pp. 1–4, IEEE, 2019.

[5] P. B. R. Maslak and P. Mašek, "IMPLEMENTACE A VYHODNOCENÍ KOMUNIKAČNÍ TECHNOLOGIE LTE CAT-M1 V SIMULAČNÍM PROSTŘEDÍ NS-3," 2021.

[6] SigFox, "SigFox O síti." `https://sigfox.cz/cs`. Citováno dne: 2022-11-14.

[7] IoT Portal, "Mapy pokrytí IoT." `https://www.iot-portal.cz/mapa-pokryti/`. Citováno dne: 2022-12-03.

[8] D. Bankov, E. Khorov, and A. Lyakhov, "On the limits of LoRaWAN channel access," in *2016 International conference on engineering and telecommunication (EnT)*, pp. 10–14, IEEE, 2016.

[9] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, and T. Watteyne, "Understanding the limits of LoRaWAN," *IEEE Communications magazine*, vol. 55, no. 9, pp. 34–40, 2017.

[10] R. Ratasuk, B. Vejlgaard, N. Mangalvedhe, and A. Ghosh, "NB-IoT system for M2M communication," in *2016 IEEE wireless communications and networking conference*, pp. 1–5, IEEE, 2016.

[11] Vodafone Czech Republic a.s., "Mapa pokrytí NB-IoT." `https://www.vodafone.cz/mapa-pokryti/`. Citováno dne: 2022-12-03.

[12] P. Masek, M. Stusek, K. Zeman, R. Drapela, A. Ometov, and J. Hosek, "Implementation of 3GPP LTE Cat-M1 technology in NS-3: System simulation and

performance," in *2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, pp. 1–7, IEEE, 2019.

[13] M. Stusek, "Research on Reliable Low-Power Wide-Area Communications Utilizing Multi-RAT LPWAN Technologies for IoT Applications," 2021.

[14] M. Kanj, V. Savaux, and M. Le Guen, "A tutorial on NB-IoT physical layer design," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2408–2446, 2020.

[15] D. Soni and A. Makwana, "A survey on mqtt: a protocol of internet of things (iot)," in *International conference on telecommunication, power analysis and computing techniques (ICTPACT-2017)*, vol. 20, pp. 173–177, 2017.

[16] P. B. R. Dvořák and P. Mašek, "VYTVOŘENÍ LABORATORNÍ ÚLOHY PRO TECHNOLOGIE LPWA VYUŘÍVAJÍCÍ PROTOKOL LIGHTWEIGHT M2M (LWM2M)," 2022.

[17] R. A. Rahman and B. Shah, "Security analysis of IoT protocols: A focus in CoAP," in *2016 3rd MEC international conference on big data and smart city (ICBDSC)*, pp. 1–7, IEEE, 2016.

[18] C. Bormann, A. P. Castellani, and Z. Shelby, "Coap: An application protocol for billions of tiny internet nodes," *IEEE Internet Computing*, vol. 16, no. 2, pp. 62–67, 2012.

[19] S. Rao, D. Chendanda, C. Deshpande, and V. Lakkundi, "Implementing LWM2M in constrained IoT devices," in *2015 IEEE Conference on Wireless Sensors (ICWiSe)*, pp. 52–57, IEEE, 2015.

[20] D. Diaz-Sanchez, A. Marin-Lopez, F. A. Mendoza, P. A. Cabarcos, and R. S. Sherratt, "TLS/PKI challenges and certificate pinning techniques for IoT and M2M secure communications," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3502–3531, 2019.

[21] Quectel, "Quectel BG77xA-GL CatM1/NB1/NB2 Series." `https://www.quectel.com/product/lpwa-bg770x-gl`. Citováno dne: 2022-11-14.

[22] Quectel, "LPWA BG77 Cat M1/NB2." `https://www.quectel.com/product/lte-bg77-cat-m1-nb2`. Citováno dne: 2022-5-1.

[23] RPishop, "Raspberry Pi Compute Module 4." `https://rpishop.cz/compute-module-4/3086-raspberry-pi-compute-module-4.html`. Citováno dne: 2022-5-1.

[24] RPishop, “Raspberry Pi 4 Model B - 4GB RAM.” https://rpishop.cz/raspberry-pi-4/1598-raspberry-pi-4-model-b-4gb-ram-765756931182.html. Citováno dne: 2022-5-1.

[25] RPishop, “Pimoroni BMP280 - senzor teploty, tlaku a nadmořské výšky, I2C, breakout modul.” https://rpishop.cz/breakout-garden-/2308-pimoroni-bmp280-senzor-teploty-tlaku-a-nadmorske-vysky-i2c-breakout-modul.html. Citováno dne: 2022-5-1.

[26] RPishop, “Raspberry Pi Camera 3.” https://rpishop.cz/mipi-kamerove-moduly/5599-raspberry-pi-camera-3-5056561803241.html. Citováno dne: 2022-5-1.

[27] Drátek, “Baterie 18650 3,7V 2600mAh ICR18650P - 5C Doublepow.” https://dratek.cz/arduino/5127-baterie-18650-3-7v-2600-mah-inr18650.html. Citováno dne: 2022-5-18.

[28] Drátek, “Step down nastavitelný měnič s LM2596 DC-DC.” https://dratek.cz/arduino/1303-stepdown-nastavitelny-menic-s-lm2596-dc-dc.html. Citováno dne: 2022-5-18.

[29] Dell, “Jak otestovat dostupnou šířku pásma sítě pomocí nástroje „iperf“.” https://www.dell.com/support/kbdoc/cs-cz/000139427/jak-otestovat-dostupnou-šířku-pásma-sítě-pomocí-nástroje-iperf. Citováno dne: 2022-5-1.

# Seznam symbolů a zkratek

**ACB** Access Class Barring

**API** Application Programming interface

**BCCH** Broadcast Control Channel

**BCH** Broadcast Channel

**CCCH** Common Control Channel

**CE** Coverage Enhancement

**cMTC** Ctritical Machine Type Communication

**CoAP** Constrained Application Protocol

**CSS** Chirp Spread Spectrum

**DCCH** Dedicated Control Channel

**DCI** Downlink Control Information

**DL** Downlink

**DL-SCH** Downlink Shared Channel

**DMRS** Demodulation Reference Signal

**DRX** Discontinous reception

**DTCH** Dedicated Traffic Channel

**DTLS** Datagram Transport Layer Security

**EAB** Extended Access Barring

**eDRX** Extended Discontinous Reception

**EMB** Enhanced Mobile Broadband

**E2E** End to End

**FDD** Frequency Division Duplex

**FDMA** Frequency Division Multiple Acces

**HDMI** High Definition Multimedia Interface

| | |
|---|---|
| **HTTP** | Hyper Text Transfer Protocol |
| **H2H** | Human to Human |
| **IoT** | Internet of Things |
| **ISM** | Industrial Science and Medical |
| **LPWAN** | Low Power Wide Area Networks |
| **LWM2M** | Leightweight Machine to Machine |
| **MAC** | Media Access Control |
| **MCL** | Maximum Coupling Loss |
| **MIB** | Master Information Block |
| **mMTC** | Massive Machine Type Communication |
| **MPDCCH** | Machine Type Communication Physical Downlink Control Channel |
| **MQTT** | Message Queue Telemetry Transport |
| **MTC** | Machine Type Communication |
| **M2M** | Machine to Machine |
| **NPBCH** | Narrowband Physical Broadcast Channel |
| **NPDCCH** | Narrowband Physical Downlink Control Channel |
| **NPDSCH** | Narrowband Physical Downlink Shared Channel |
| **NPRACH** | Narrowband Physical Random Acces Channel |
| **NPSS** | Narrowband Primary Synchronization Signal |
| **NPUSCH** | Narrowband Physical Uplink Shared Channel |
| **NSSS** | Narrowband Secondary Synchronization Signal |
| **OFDMA** | Orthogonal Frequency Division Multiple Access |
| **OMA** | Open Mobile Alliance |
| **PBCH** | Physical Broadcast Channel |
| **PCCH** | Paging Control Channel |

| | |
|---|---|
| **PCH** | Paging Channel |
| **PDSCH** | Physical Downlink Shared Channel |
| **PRACH** | Physical Random Acces Channel |
| **PRB** | Physical Resource Block |
| **PRS** | Positioning Reference Signal |
| **PSM** | Power Saving Mode |
| **PSS** | Primary Synchronization Singal |
| **pTAU** | Periodic Tracking Area Updates |
| **PTW** | Paging Transmission Window |
| **PUCCH** | Physical Uplink Control Channel |
| **PUSCH** | Physical Uplink Shared Channel |
| **P2P** | Peer to Peer |
| **QoS** | Quality of Service |
| **QPSK** | Quadrature Phase-Shift Keying |
| **RACH** | Random Access Channel |
| **RAM** | Random Access Memory |
| **RAR** | Random Access Response |
| **REs** | Resource elements |
| **RNTI** | Radio Network Temporary Identifier |
| **RRC** | Radio Resource Control |
| **RSRP** | Reference Signal Receive Power |
| **SIB1** | System Information Block 1 |
| **SINR** | Signal to Interference plus Noise Ratio |
| **SSS** | Secondary Synchronization Signal |
| **TBCC** | Tail-Biting Convolution Code |

| | |
|---|---|
| **TCP** | Transmission Control Protocol |
| **TLS** | Transport Layer Security |
| **UCI** | Uplink Control Information |
| **UL** | Uplink |
| **UL-SCH** | Uplink Shared Channel |
| **UART** | Universal Asynchronous Receiver Transmitter |
| **UNB** | Ultra Narrow Band |
| **URI** | Universal Resource Identifier |
| **USB** | Universal Serial Bus |
| **3GPP** | Third Generation Partnership Project |

# A Měřené hodnoty NB-IoT v Brně a Jeseníku

Měření pomocí Iperf probíhalo s ECL = 0, protokolem TCP, intervalem zasílání 5 s, časem testu 5s. Poslední tři řádky tabulky jsou určené pro průměrné, maximální a minimální hodnoty měření. Označení C je pro Client, Se pro Server, S pro Sender, R pro Reciever.

U testování pomocí PING byl ECL = 0, počet odeslání zprávy PING roven 20.

| Zpráva [B] | RSRP [dBm] | SINR [dB] | UL C [Kb/s] | DL C [Kb/s] | UL Se [Kb/s] | DL Se [Kb/s] | Data S [KB] | Data R [KB] | Retr |
|---|---|---|---|---|---|---|---|---|---|
| 8000 | -75 | 2 | 36 | 36 | 32.9 | 32.9 | 396 | 396 | 12 |
| 12000 | -75 | 2 | 40.8 | 40.8 | 35.5 | 35.5 | 448 | 448 | 2 |
| 16000 | -76 | 3 | 38.3 | 37.1 | 34.2 | 33.2 | 421 | 408 | 4 |
| 20000 | -76 | 2 | 39.3 | 39.3 | 34.3 | 34.3 | 432 | 432 | 4 |
| 28000 | -76 | 3 | 23 | 19.5 | 20.3 | 17.2 | 253 | 215 | 7 |
| 36000 | -74 | 2 | 37.3 | 34.4 | 34.7 | 32 | 410 | 378 | 13 |
| 44000 | -75 | 4 | 42.4 | 38.9 | 37.9 | 34.7 | 466 | 427 | 7 |
| 52000 | -76 | 2 | 38.5 | 36.1 | 34.3 | 32.2 | 423 | 397 | 5 |
| 60000 | -75 | 3 | 38.9 | 33.2 | 35.8 | 30.6 | 427 | 365 | 5 |
| 70000 | -75 | 3 | 40.4 | 33.3 | 37.2 | 30.6 | 444 | 365 | 17 |
| 80000 | -76 | 3 | 43.4 | 37.1 | 39.2 | 33.6 | 477 | 408 | 12 |
| 90000 | -76 | 3 | 42.4 | 35.8 | 39.9 | 33.7 | 466 | 393 | 8 |
| 100000 | -76 | 3 | 47.3 | 29 | 45 | 27.6 | 520 | 319 | 6 |
| 120000 | -75 | 4 | 46.6 | 37 | 39.8 | 31.7 | 512 | 407 | 2 |
| 140000 | -75 | 4 | 46.3 | 33 | 40 | 28.5 | 509 | 363 | 8 |
| 160000 | -76 | 4 | 49.4 | 36.4 | 43.1 | 31.7 | 543 | 400 | 12 |
| 180000 | -76 | 3 | 57.4 | 32.5 | 52.5 | 29.8 | 631 | 358 | 15 |
| 200000 | -77 | 4 | 54.6 | 36.7 | 50.2 | 33.7 | 600 | 403 | 9 |
| 250000 | -76 | 0 | 51.3 | 26.2 | 50.8 | 25.9 | 564 | 287 | 7 |
| 300000 | -77 | -5 | 51.8 | 35.8 | 47.7 | 32.9 | 569 | 393 | 12 |
| 350000 | -77 | 3 | 54.7 | 28.7 | 52.1 | 27.3 | 601 | 316 | 14 |
| Průměr | -75.71 | 2.48 | 43.81 | 34.13 | 39.88 | 30.93 | 481.52 | 375.14 | 8.62 |
| Max | -77 | 4 | 57.4 | 40.8 | 52.5 | 35.5 | 631 | 448 | 17 |
| Min | -74 | -5 | 23 | 19.5 | 20.3 | 17.2 | 253 | 215 | 2 |

Tab. A.1: Tabulka měřených hodnot pomocí Iperf z Brna

| Zpráva [B] | RSRP [dBm] | SINR [dB] | UL C [Kb/s] | DL C [Kb/s] | UL Se [Kb/s] | DL Se [Kb/s] | Data S [KB] | Data R [KB] | Retr |
|---|---|---|---|---|---|---|---|---|---|
| 8000 | -69 | 19 | 35.3 | 32 | 34.1 | 30.9 | 387 | 352 | 3 |
| 12000 | -69 | 21 | 38 | 38 | 35.3 | 35.3 | 418 | 418 | 2 |
| 16000 | -69 | 20 | 38.8 | 38.7 | 34.7 | 34.6 | 426 | 425 | 2 |
| 20000 | -68 | 16 | 39.4 | 39.4 | 35 | 35 | 433 | 433 | 0 |
| 28000 | -68 | 22 | 40.5 | 39.4 | 35.5 | 34.5 | 445 | 432 | 7 |
| 36000 | -69 | 21 | 39.7 | 39.7 | 35.2 | 35.2 | 436 | 436 | 1 |
| 44000 | -68 | 21 | 38 | 37.6 | 33.9 | 33.6 | 417 | 413 | 11 |
| 52000 | -68 | 22 | 40.2 | 38.7 | 31.9 | 30.7 | 442 | 426 | 0 |
| 60000 | -69 | 22 | 42.1 | 40.4 | 36 | 34.5 | 463 | 444 | 1 |
| 70000 | -70 | 15 | 43.9 | 41.2 | 37.5 | 35.3 | 482 | 453 | 0 |
| 80000 | -70 | 17 | 45.7 | 40.5 | 39.3 | 34.9 | 502 | 445 | 2 |
| 90000 | -70 | 22 | 45.2 | 41.3 | 39 | 35.7 | 497 | 454 | 0 |
| 100000 | -70 | 16 | 50.2 | 41.5 | 43.1 | 35.6 | 552 | 456 | 1 |
| 120000 | -73 | 17 | 45.6 | 41.8 | 39.3 | 36 | 501 | 459 | 4 |
| 140000 | -70 | 22 | 49.6 | 39.5 | 42.5 | 33.9 | 544 | 434 | 0 |
| 160000 | -69 | 14 | 61 | 41.5 | 52.7 | 35.8 | 670 | 456 | 4 |
| 180000 | -70 | 17 | 63.3 | 41.7 | 53.8 | 35.4 | 695 | 458 | 0 |
| 200000 | -69 | 14 | 51.7 | 40.3 | 44.7 | 34.8 | 568 | 443 | 3 |
| 250000 | -68 | 14 | 51.8 | 40.4 | 45.1 | 35.2 | 569 | 444 | 2 |
| 300000 | -70 | 13 | 63.2 | 41.6 | 54.6 | 35.9 | 694 | 456 | 0 |
| 350000 | -70 | 14 | 63.4 | 41.3 | 54.5 | 35.3 | 696 | 451 | 1 |
| Průměr | -69.33 | 18.05 | 46.98 | 39.83 | 40.84 | 34.67 | 516.05 | 437.52 | 2.10 |
| Max | -73 | 22 | 63.4 | 41.8 | 54.6 | 36 | 696 | 459 | 11 |
| Min | -68 | 13 | 35.3 | 32 | 31.9 | 30.7 | 387 | 352 | 0 |

Tab. A.2: Tabulka měřených hodnot pomocí Iperf z Jeseníku

| Velikost zprávy [B] | 12 | 16 | 32 | 64 | 128 | 256 | 512 | 1024 | 2048 | 4096 | 8192 | 16384 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| RSRP [dBm] | -79 | -77 | -80 | -78 | -79 | -79 | -80 | -79 | -79 | -79 | -78 | -79 |
| SINR [dB] | 2 | 2 | 1 | 0 | 1 | 0 | -15 | 4 | 1 | 1 | 1 | 3 |
| Minimální zpoždění [ms] | 173 | 177 | 177 | 259 | 216 | 336 | 729 | 1140 | 3261 | 5044 | 9762 | 0 |
| Maximální zpoždění [ms] | 1380 | 1099 | 1647 | 989 | 1032 | 1168 | 5166 | 2808 | 16125 | 32124 | 47591 | 0 |
| Průměrné zpoždění [ms] | 548 | 505 | 702 | 633 | 580 | 766 | 1758 | 1911 | 10312 | 18406 | 29069 | 0 |
| Packet loss [%] | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 30 | 60 | 100 |

Tab. A.3: Tabulka měřených hodnot pomocí PING z Jeseníku

# B Programy na zařízeních a LPWAN serveru.

Výpis B.1: Ukázka programu BP.py na Raspberry Pi 4B. Cast 1/3

```
from picamera2 import Picamera2
from libcamera import controls
from bmp280 import BMP280
from time import sleep
import datetime
import schedule
import socket

ipAddress= '192.168.1.6'
port = 65401

try:
    from smbus2 import SMBus
except ImportError:
    from smbus import SMBus

bus = SMBus(1)
bmp280= BMP280(i2c_dev=bus)

camera = Picamera2()

cas_mereni = 60
hranicni_teplota = 65
width = 1280
height = 720
```

Výpis B.2: Ukázka programu BP.py na Raspberry Pi 4B. Cast 2/3

```
def mereni():
    teplota=bmp280.get_temperature()
    tlak = bmp280.get_pressure()
    datum = datetime.datetime.now().strftime('%Y-%m-%d--%H:%M
:%S')
    name = datum + ".jpg"
    msg = ("Teplota: {:.2f}*C".format(teplota) + ", Tlak: {:.
2f}hPa".format(tlak) + f", Datum: {datum} ")
    print(msg)
    print("----------------------------------------")

    if (teplota > hranicni_teplota):
        with open("data.txt", "a") as file:
            file.write(msg + " \n")
        file.close()
        config = camera.create_preview_configuration(main={
"size": (width, height)})
        camera.configure(config)
        camera.start()
        sleep(3)
        camera.capture_file("/home/student/fotky/" + name)
        camera.stop()

        sock = socket.socket(socket.AF_INET, socket.
SOCK_STREAM)
        sock.connect((ipAddress, port))
        sock.send(str.encode(msg))
        print("Zprava odeslana")
        sleep(2)
        sock.send(str.encode(name))
        print("Zprava odeslana")
        sleep(2)

        file = open("/home/student/fotky/" + name, 'rb')
        imagePiece = file.read(2048)

        while imagePiece:
            sock.send(imagePiece)
            imagePiece = file.read(2048)
        file.close()
        sock.close()
```

Výpis B.3: Ukázka programu BP.py na Raspberry Pi 4B. Část 3/3

```
schedule.every(cas_mereni).seconds.do(mereni)

while True:
    datum = datetime.datetime.now().strftime('%Y-%m-%d--%H:%M
:%S')
    schedule.run_pending()
    sleep(1)

sock.close()
```

Výpis B.4: Ukázka programu switch.py na Raspberry Pi CM4

```
import socket
import time
ipAddressC =''
portC = 65401
ipAddressS = '127.0.0.1'
portS = 65407

while True:
    server = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    print("Socket␣vytvoren")
    server.bind((ipAddressC, portC))
    server.listen()
    print("Listening...")
    client, address = server.accept()
    msg = client.recv(1024).decode('utf-8')
    print("Prijata␣zprava:␣" + msg)
    name = client.recv(1024).decode('utf-8')
    print("Jmeno␣souboru:␣" + name)
    file = open('/root/fotky/' + name, "wb")
    imagePiece = client.recv(2048)
    while imagePiece:
        file.write(imagePiece)
        imagePiece = client.recv(2048)
    print("Fotka␣dorucena")
    file.close()
    client.close()
    server.close()
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    sock.connect((ipAddress, port))
    sock.send(str.encode(msg))
    print("Zprava␣odeslana")
    time.sleep(15)
    sock.send(str.encode(name))
    print("Zprava␣odeslana")
    sleep(15)
    file = open("/root/fotky/" + name, 'rb')
    imagePiece = file.read(2048)
    while imagePiece:
        sock.send(imagePiece)
        imagePiece = file.read(2048)
    file.close()
    sock.close())
```

Výpis B.5: Ukázka programu server.py na LPWAN serveru.

```
import socket
ipAddress = '127.0.0.1'
port = 65407

def startServer():
    server = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    print("Socket␣uspesne␣vytvoren")
    server.bind((ipAddress, port))
    return server

def startConnection():
    server.listen()
    print("Listening...")
    client, address = server.accept()
    return client

def dataPrijem(client):
    msg = client.recv(1024).decode('utf-8')
    print("Prijata␣zprava:␣" + msg)
    with open("/home/lpwan/230307/data.txt", "a") as file:
     file.write(msg + "␣\n")
    file.close()
    name = client.recv(1024).decode('utf-8')
    print("Jmeno␣souboru:␣" + name)
    file = open('/home/lpwan/230307/fotky/' + name, "wb")
    imagePiece = client.recv(2048)
    while imagePiece:
        file.write(imagePiece)
        imagePiece = client.recv(2048)
    print("Fotka␣dorucena")

while True:
    try:
        server = startServer()
        client = startConnection()
        dataPrijem(client)
        client.close()
        server.close()
    except:
        break
```