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

TESTOVÁNÍ KOMUNIKAČNÍCH PROTOKOLŮ S VYUŽITÍM MOBILNÍCH TECHNOLOGIÍ PRO INTERNET VĚCÍ LTE-M A NB-IOT

TESTING COMMUNICATION PROTOCOLS USING MOBILE TECHNOLOGIES FOR THE INTERNET OF THINGS LTE-M AND NB-IOT

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE — Bc. Samuel Bartko

AUTHOR

VEDOUCÍ PRÁCE — Ing. Radek Možný

SUPERVISOR

BRNO 2024

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní program **Telekomunikační a informační technika**

Ústav telekomunikací

Student: Bc. Samuel Bartko ***ID:*** 220797

Ročník: 2 ***Akademický rok:*** 2023/24

NÁZEV TÉMATU:

Testování komunikačních protokolů s využitím mobilních technologií pro internet věcí LTE-M a NB-IoT

POKYNY PRO VYPRACOVÁNÍ:

Cílem diplomové práce bude testování a následné vyhodnocení vhodnosti použití a optimální konfigurace aktuálně rozšířených komunikačních protokolů v rámci internetu věcí (IoT). Pro přenos dat bude využito aktuální implementace mobilních technologií pro IoT LTE-M a NB-IoT. V teoretické části budou popsány klíčové vlastnosti technologií LTE-M a NB-IoT dle aktuální implementace 3GPP Rel. 13 a 14 s následným popisem klíčových optimalizací v nadcházejících vydáních, tj. 3GPP Rel. 15+. Teoretická část bude dále obsahovat úvahu nad aktuálně využívanými komunikačními protokoly pro přenos dat a vzdálený management IoT zařízení (MQTT, LwM2M, SSH apod.). Praktická část práce bude zahrnovat definici a realizaci testovacích scénářů pro vybrané komunikační protokoly. Výsledky testování následně budou vést k ověření vhodnosti či návrhu optimální konfigurace jednotlivých komunikačních protokolů pro využití s technologiemi NB-IoT a LTE-M.

DOPORUČENÁ LITERATURA:

Podle pokynů vedoucího práce.

Termín zadání: 5.2.2024 ***Termín odevzdání:*** 21.5.2024

Vedoucí práce: Ing. Radek Možný

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

ABSTRAKT

Táto diplomová práca sa zameriava na komplexné skúmanie a hodnotenie aktuálne rozšírených komunikačných protokolov v dynamicky sa rozvíjajúcom sektore Internetu vecí (IoT). S rozširovaním IoT vzniká potreba tvoriť nové technológie pre efektívne prepojenie fyzického a digitálneho sveta. Hlavným cieľom tejto práce je testovanie a vyhodnotenie vhodnosti použitia a optimálnej konfigurácie komunikačných protokolov v kontexte najnovších implementácií mobilných technológií pre IoT, konkrétne LTE-M (Long-Term Evolution Machine Type Communication) a NB-IoT (Narrowband Internet of Things). Táto diplomová práca skúma a hodnotí aktuálne komunikačné protokoly pre Internet vecí (IoT), zameriavajúc sa na LTE-M a NB-IoT. Obsahuje teoretický pohľad na IoT, popis mobilných technológií a analýzu protokolov ako MQTT, CoAP a LwM2M. Praktická časť sa venuje testovaniu a optimalizácii týchto protokolov. Výsledkom práce je poskytnutie komplexného prehľadu a praktických odporúčaní pre použitie a konfiguráciu komunikačných protokolov v rámci technológií NB-IoT a LTE-M.

KĽÚČOVÉ SLOVÁ

CoAP, IoT, LTE-M, LWM2M, MQTT, NB-IoT, protocol, SSH, testing

ABSTRACT

This thesis focuses on a comprehensive investigation and evaluation of the currently widespread communication protocols in the dynamically developing IoT sector (Internet of Things). With the proliferation of IoT, there is a need to create new technologies for efficient interconnection of hysical and digital worlds. The main objective of this work is to test and evaluate the suitability of use and optimal configuration of communication protocols in the context of the latest implementations of mobile technologies for IoT, namely LTE-M (Long-Term Evolution Machine Type Communication) and NB-IoT (Narrowband Internet of Things). This thesis investigates and evaluates the current communication protocols for the Internet of Things (IoT), focusing on LTE-M and NB-IoT. It includes a theoretical perspective on IoT, description of mobile technologies and analysis of protocols such as MQTT, CoAP and LwM2M. A practical part is devoted to testing and optimization of these protocols. The result of the work is providing a comprehensive overview and practical recommendations for use and configuration communication protocols in the framework of NB-IoT and LTE-M technologies.
Translated with DeepL.com (free version)

KEYWORDS

CoAP, IoT, LTE-M, LWM2M, MQTT, NB-IoT, protokol, SSH, testovanie

BARTKO, Samuel. *Testování komunikačních protokolů s využitím mobilních technologií pro internet věcí LTE-M a NB-IoT*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2024, 83 s. Diplomová práca. Vedúci práce: Ing. Radek Možný

Vyhlásenie autora o pôvodnosti diela

Meno a priezvisko autora:	Bc. Samuel Bartko
VUT ID autora:	220797
Typ práce:	Diplomová práca
Akademický rok:	2023/24
Téma závěrečnej práce:	Testování komunikačních protokolů s využitím mobilních technologií pro internet věcí LTE-M a NB-IoT

Vyhlasujem, že svoju záverečnú prácu som vypracoval samostatne pod vedením vedúcej/cého záverečnej práce, s využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej záverečnej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto záverečnej práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona Českej republiky č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákonníka Českej republiky č. 40/2009 Sb.

Brno ....

podpis autora*

*Autor podpisuje iba v tlačenej verzii.

POĎAKOVANIE

Rád by som poďakoval vedúcemu diplomovej práce pánovi Ing. Radkovi Možnému, za odborné vedenie, pravidelné konzultácie, veľkú trpezlivosť a veľmi podnetné návrhy k práci.

Obsah

Zoznam obrázkov

Zoznam tabuliek

Úvod

S príchodom a rýchlym nárastom záujmu o Internet vecí vznikla potreba vytvárať a vyrábať zariadenia, ktoré svojou funkcionalitou a možnosťami zodpovedajú požiadavkám Internetu vecí. S rozširovaním možností jeho využitia vzniká potreba tvoriť nové technológie pre čo najrýchlejšie a najefektívnejšie prepojenie fyzického a digitálneho sveta. A práve z tohto dôvodu sa táto diplomová práca zameriava na komplexné skúmanie a hodnotenie aktuálne rozšírených komunikačných protokolov v dynamicky sa rozvíjajúcom sektore Internetu vecí. Je nevyhnutné pochopiť a optimalizovať využitie komunikačných protokolov, aby bola zabezpečená efektívna a bezpečná komunikácia medzi zariadeniami. Hlavným cieľom tejto práce je testovanie a vyhodnotenie vhodnosti použitia a optimálnej konfigurácie týchto komunikačných protokolov v kontexte najnovších implementácií mobilných technológií pre IoT (Internet of Things), konkrétne LTE-M (Long-Term Evolution Machine Type Communication) a NB-IoT (Narrowband Internet of Things).

Teoretická časť, konkrétne prvá kapitola, sa venuje bližšiemu pohľadu na to, čo koncept Internetu vecí je, čo zahŕňa a aká je jeho vízia do budúcnosti. Druhá kapitola je venovaná odvetviu Internetu vecí, ktorá popisuje spôsob pripojenia zariadení k internetu pomocou mobilných technológií. Kapitola sa zameriava na popis aktuálne využívaných mobilných technológií a krátko približuje organizáciu 3GPP (The 3rd Generation Partnership Project). Tretia kapitola obsahuje podrobný opis, kľúčové vlastnosti a funkcie technológií LTE-M a NB-IoT podľa špecifikácií 3GPP Release 13 až 16, zahŕňajúce aj technológiu NR-Light (RedCap). Štvrtá kapitola sa zameriava na rozbor už známych, overených komunikačných protokolov pre prenos dát a vzdialený manažment, kde naviaže rozborom novo vzniknutých a upravených protokolov pre potreby IoT zariadení, ako sú MQTT (Message Queuing Telemetry Transport), CoAP (Constrained Application Protocol) a LwM2M (Lightweight M2M). Piata kapitola je zameraná na IoT servery, cez ktoré prúdi komunikácia a teda dáta pre ďalšie spracovanie. Pre potreby správneho nastavenia využitia IoT platforiem a komunikačných protokolov sa nasledujúca šiesta kapitola, teda praktická časť práce, venuje testovaniu vybraných protokolov a hodnoteniu parametrov, ktoré môžu ovplyvniť funkčnosť a bezproblémovú prevádzku. Kapitola obsahuje popis scenárov využitých na otestovanie.

Cieľom tejto práce je poskytnúť komplexný prehľad a praktické odporúčania pre použitie a konfiguráciu komunikačných protokolov v rámci technológií NB-IoT a LTE-M, čo prispeje k lepšiemu porozumeniu a efektívnemu využitiu týchto technológií v rýchlo sa rozvíjajúcom svete IoT.

1 Koncept Internet vecí

Internet vecí, viac známejší pod jednoduchou skratkou IoT, vychádzajúca z anglického názvu Internet of Things, je koncept vytvorený na základe myšlienky využitia inteligentných elektronických zariadení, ktoré by mohli autonómne vykonávať rôzne úlohy s cieľom zlepšiť, zefektívniť a automatizovať rôzne aspekty nášho každodenného života. Mohlo by sa zdať, že táto revolučná idea by bola obmedzená len na každodenné prostredie, opak je však pravdou a uplatňuje sa aj v priemysle, medicíne, poľnohospodárstve a mnohých iných oblastiach [1].

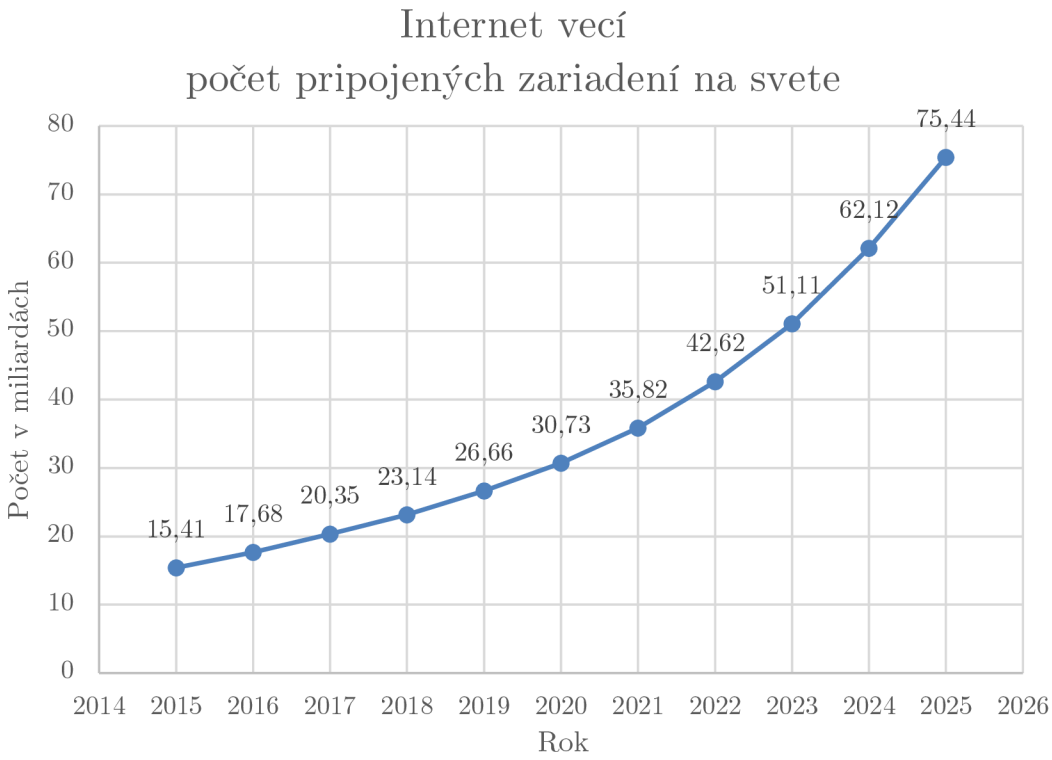
Hlavným cieľom IoT je vytvoriť budúcnosť, v ktorej budú aspekty fyzického sveta digitalizované a vzájomne prepojené pomocou spoločnej siete. Táto sieť zariadení spojí doteraz existujúce systémy, urobí z nich inteligentné systémy a umožní spojenie s novými technológiami. Teda ide o vytvorenie globálnej siete prepojených zariadení, ktoré budú schopné spolu komunikovať a spolupracovať v reálnom čase. A ako už z názvu vyplýva, celý tento proces výmeny dát, pokynov bude zabezpečený prostredníctvom internetu, čím sa vytvorí komplexný ekosystém vzájomne prepojených zariadení [1].

Tento koncept má za cieľ vytvoriť zariadenia, schopné bez prítomnosti človeka automaticky vykonávať úlohy a reagovať na podnety kedykoľvek a kdekoľvek. Na základe vývoja technológii a spoločnosti, v období od prvej myšlienky konceptu IoT až do dnes, je možné konštatovať, že vízia prepojeného sveta je budúcnosťou. V súčasnosti vidíme množstvo inovácií v dôležitých odvetviach, či už ide o jednoduché bezdrôtové senzory, alebo pokročilé nanotechnológie [1].

Internet vecí nám otvára dvere k novým možnostiam a vytvára potenciál pre efektívnejšie, inteligentnejšie a pohodlnejšie životy. Vzhľadom na neustály pokrok v oblasti IoT môžeme očakávať, že bude mať stále väčší vplyv na našu spoločnosť a náš životný štýl v budúcnosti [1].

Podľa predpovedí sa každoročne očakáva exponenciálny rast počtu zariadení. Tieto predpovede sú založené na mnohých aspektoch, ako je rozširovanie povedomia o výhodách IoT zariadení, keď stále viac spoločností skúša nové možnosti a investuje do tejto technologickej oblasti. Toto vedie k uplatneniu nových prístupov v odvetviach ako poľnohospodárstvo a zdravotníctvo. Ohromný podiel na tomto raste majú nielen veľkí hráči, ale aj jednotlivci. Vďaka využívaniu IoT v rámci tzv. Smart Homes (inteligentných domácností) ľudia vedia ovládať a automatizovať prvky domácnosti, ako sú kúrenie a klimatizácia, osvetlenie a monitorovať prostredie z hľadiska zdravia a bezpečnosti. Možnosti zefektívnenia úkonov, správy a kontroly nemajú využitie

len v našich obydliach, ale pretavujú sa aj do konceptu Smart Cities (inteligentných miest), kde sa všetky aspekty mesta stanú súčasťou IoT siete [1].



Obr. 1.1: Predpokladaný počet IoT zariadení v roku 2025 [2].

Po prečítaní úvodu do konceptu Internetu vecí je jasné, že IoT má širokú oblasť použitia, od domácností po inteligentné mestá. Tento rozsah naznačuje, že pre jednoduchšie pochopenie by bolo vhodné aplikácie IoT kategorizovať. Rozdelením môžeme lepšie chápať špecifické potreby a bezpečnostné požiadavky každého sektora. Takáto kategorizácia uľahčuje navrhovanie cielených riešení a efektívnejšie využívanie zdrojov, či už ide o energetické požiadavky, komunikačné protokoly alebo zabezpečenie dát.

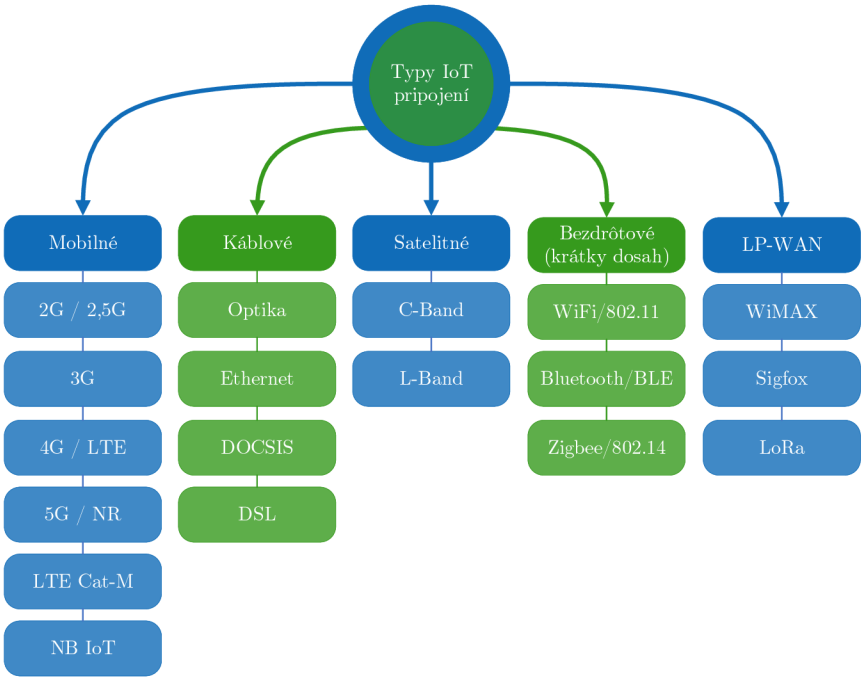
V konečnom dôsledku, kategorizácia IoT aplikácií vedie k lepšiemu porozumeniu ich potenciálu a limitácií. Medzi často používané rozdelenie patrí delenie na základe oblasti použitia, ktoré možno klasifikovať nasledovne:

- **Spotrebiteľské IoT**,
- **Komerčné IoT**,
- **Priemyselné IoT**,
- **Vojenské IoT**,
- **Infraštruktúrne IoT**.

1.1 Delenie IoT na základe použitého pripojenia

Kategorizovanie a delenie IoT je rôznorodé. Avšak každé odvetvie sa musí zaoberať otázkou akým spôsobom budú zariadenia v rámci IoT riešení napájané, akým spôsobom budú komunikovať vymieňať si dáta, v akých podmienkach okolitého prostredia budú fungovať a mnoho iných ďalších aspektov. Vrámci tejto práce pripadá v úvahu rozdeliť si IoT na kategórie líšiac sa typom prepojení zariadení k sieti internetu.
S uvážením tohto predpokladu sa IoT na základe použitého pripojenia delí na [3]:

- **Mobilné IoT** – využívajú či už existujúce mobilné technológie v licencovanom pásme primárne určené na prenos hlasu 2G, 3G, 4G, alebo nové určené priamo pre IoT.
- **Káblové IoT** – využívajú pevné pripojenie, či metalickými ako napríklad ethernet alebo optickými vláknami.
- **Satelitné IoT** – využíva bezdrôtovú komunikáciu GAN (Global Area Network) sietí s neobmedzeným dosahom.
- **Bezdrôtové IoT** – využívajú bezdrôtovú komunikáciu v bez-licenčnom pásme s použitím existujúcich technológii (Wifi, Bluetooth) alebo nové navrhnuté priamo pre IoT (ZigBee, LoRa).



Obr. 1.2: Rozdelenie IoT na základe pripojenia [3].

2 Mobilné IoT

Mobilné IoT alebo Cellular IoT, v preklade bunkové IoT, je kategória využívajúca pre potreby komunikácie licencované frekvenčné pásma. Spadajú sem pásma UHF rozsahu, konkrétne od 300 MHz do 3 GHz, typicky používané pre mobilné siete. S príchodom piatej generácie mobilných sietí sa rozsah rozrástol do vyšších frekvencii typicky až do 5 GHz [4].

V začiatkoch tejto kategórie IoT, bolo jedinou možnosťou využívať, dnes už zastaralé tzv. legacy mobilné technológie 2G, 3G, ktoré operátory postupne vypínajú a tzv. "nízke"kategórie LTE ako LTE Cat-1. Pre potreby IoT poskytovali dostatočné, nie však ideálne vlastnosti. Tieto technológie boli pôvodne navrhnuté pre spoľahlivý a neprerušovaný prenos hlasu a SMS správ. S vývojom technológii ale hlavne zmenou orientácie na iné služby využívane primárne pre komunikáciu, sa poskytovatelia mobilných služieb zamerali na prenos paketových dát. Táto zmena priamo nahráva potrebám IoT. Medzi najväčších podporovateľov tejto kategórie IoT založenej na pripojení cez mobilné služby sú spoločnosti ako: Ericsson, Huawei, Qualcomm a Vodafone a ďalšie. Všetky spomenuté sú súčasťou štandardizačnej entity 3GPP (The 3rd Generation Partnership) [4].

2.1 Sieťová architektúra

Architektúra CIoT sa odlišuje od existujúcich sieťových architektúr typicky implementovaných firmami. Umožňuje pripojenie zariadení k Internetu pomocou IoT infraštruktúry poskytovanou samotnými mobilnými operátormi. Táto infraštruktúra prestavuje tzv. middleware, teda prostredník medzi samotným zariadením a serverom/platformou kde dochádza ďalšiemu spracovávaniu. Jej podstatou je umožniť veľkú škálovateľnosť, flexibilitu a umožniť podporu veľkého množstva zariadení a aplikácii. Oproti klasickej sieťovej architektúre, kde sa zariadenia priamo komunikujú s prístupovým bodom, dovoľuje vytvoriť flexibilnú sieť. Toto dovoľuje zariadenia prepojenie navzájom, vďaka čomu dokážu tvoriť menšie sub-siete pripomínajúce siete typu mesh známe napr. z Wi-Fi prístupových bodov. Vďaka tejto medzi vrstve dovoľuje integrovať zariadenia do existujúcich sietí bez potreby výrazne meniť existujúce infraštruktúry zákazníka [5].

Podstatou architektúry je poskytovať neustále pripojenie a robustnosť samotnej siete. Vďaka využívaniu existujúce infraštruktúry operátorov, dovoľuje ľahšiu interoperabilitu medzi zariadeniami a využívať komunikačné a výpočtové zdroje naprieč celou ich sieťou [5].

2.2 Delenie mobilného IoT

Vďaka pomerne rýchlemu vývoju a rozširovaniu oblastí ich využitia, sa požiadavky na mobilné siete v IoT aplikáciach viac a viac líšia. Príkladom rozdielnych potrieb môžu byť zariadenia, prioritne požadujúcich dlhú výdrž batérie s nízky objemom prenesených dát, pre iné zariadenia výdrž nebude najdôležitejším aspektom ale hlavnú úlohu bude zohrávať nízka latencia. Z týchto dôvodov je vhodné a nutné si Cellular IoT rozdeliť do podkategórii, odrážajúce potreby jednotlivých odvetví. Každý z propagátorov CIoT si však tieto kategórie delí inak. Delenia s ktorými sa stretneme najčastejšie sú od spoločností 3GPP a Ericsson [6, 5].

Delenie podľa 3GPP je nasledovné:

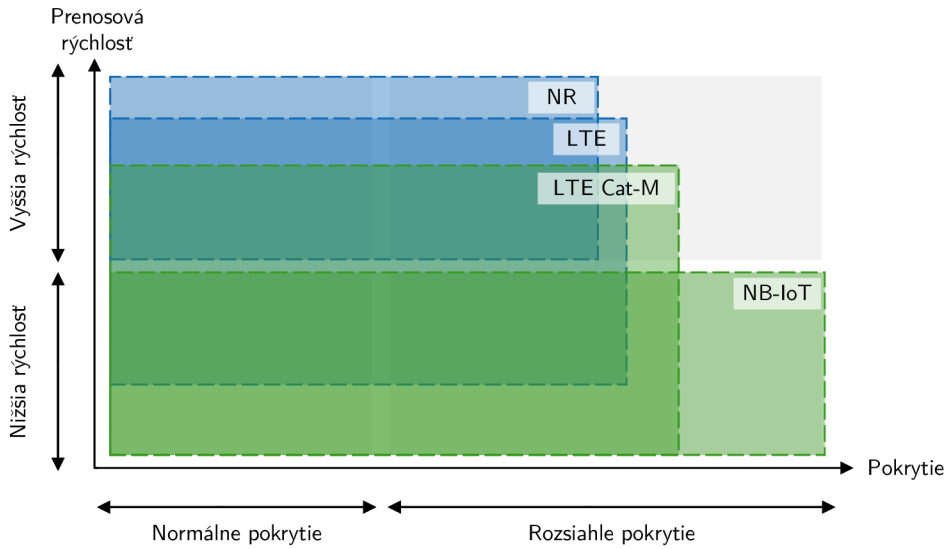
- **mMTC (massive Machine Type Communications)** - špecifikuje ohromné množstvo jednoduchších a nenáročných zariadení.
- **URLLC (Ultra-Reliable and Low Latency Communications)** - určené pre potreby vysokej spoľahlivosti a nízkej odozvy.
- **eMBB (enhanced Mobile Broadband)** - navrhnutá pre potreby prenosu veľkých objemov dát a nízkej latencie s hlavným využitím streamovacích aplikácii.

Ericsson však kategorizuje nasledovne:

- **Massive IoT** - poskytuje mobilné pripojenie jednoduchších a nenáročných zariadení.
- **Broadband IoT** - využitie tu nájdu technológie, vyžadujúce vysoké objemy prenesených dát s nižšou odozvou.
- **Critical IoT** - kategória určená pre najnáročnejšie využitie, pre potreby extrémne nízkej odozvy s čo najlepšou spoľahlivosťou.
- **Industrial IoT** - určená pre pokročilé potreby priemyselnej automatizácie

Pre potreby práce bola bližšia pozornosť venovaná deleniu firmy Ericsson. Na základe tohto rozdelenia by sa k spomenutým kategóriám dali prideliť jednotlivé technológie vhodné na ich použitie. Pre kategóriu Critical IoT sa javí ako vhodná, novo nastupujúca technológia 5G NR(New Radio), využívajúca vyššie frekvencie s veľmi nízkou latenciou. Pre Broadband IoT by postačovala súčasná technológia LTE (Long Term Evolution) na základe jej pomerne veľkého pokrytia a vyšších rýchlostí prenosu. Naopak pre potreby Massive IoT, by bolo vhodné využiť technológie LTE-M, NB-IoT a NR-Light (RedCap). A to vďaka ich jednoduchšej implementácii oproti klasickému LTE a iným ďalším dôvodom dopodrobna rozobratým v nasledujúcich kapitolách. Toto rozdelenie je vhodné považovať len orientačné, tak ako aj samotné rozdelenie do kategórii. Každé IoT riešenie má svoje špecifiká, nedá sa tak

definitívne určiť jedinú technológiu pre pomerne rozsiahle kategórie využitia [6].



Obr. 2.1: Vlastnosti komunikačných technológii dôležitých pre rôzne aspekty IoT[7].

2.3 Massive IoT

Súčasné technológie ako GSM a LTE majú určité vlastnosti, ktoré sú vhodné a prínosné pre tvorbu IoT zariadení. Avšak pre tvorbu malých, nekomplexných a vysoko úsporných zariadení však nie sú tou najvhodnejšiu voľbou. A z tohto dôvodu sa na základe potreby vlastností ako veľký dosah, nízka spotreba a nepotrebnej okamžitej odozvy sa rôzne svetové spoločnosti začali zamýšľať nad vývojom komunikačných štandardov založených na princípoch mobilných sietí. Berú ohľad na požiadavky a tvoria technológie s danými predpokladmi a s možnosťou integrovať ich do už existujúcich štruktúr bez veľkých investícii. A aj preto jedna z najznámejších a najvýznamnejších organizácii pre vývoj v oblasti mobilných technológii, organizácia 3GPP sa začala pohrávať s myšlienkou vývoja technológii s danými parametrami. Výsledky jej dlhodobého snaženia stáli za vznikom technológii LTE-M a NB-IoT. Neskoršie bola pridaná aj tretia technológia NR-RedCap vychádzajúca z 5G, však je menej zložitá a pokrýva všetky tri vetvy pre 5G. Tieto technológie sa od seba výrazne líšia. Pre ich čo najlepšie pochopenie vzniku a vývoja, je vhodné si popísať organizáciu 3GPP, jej činnosť a podstatnú časť,a to vývoj jej technológii [4].

2.4 Organizácia 3GPP

Vyššie spomenutá organizácia The 3rd Generation Partnership Project známa pod skratkou 3GPP, vznikla v roku 1998 kvôli potrebe vytvorenia jednotných, konzistentných technických špecifikácii a štandardov pre nadchádzajúcu tretiu generáciu mobilnej siete. Neskôr sa však zamerala na nadchádzajúce generácie mobilnej komunikácie.

Práca 3GPP zahŕňa vývoj technických špecifikácií pre rôzne aspekty mobilných sietí vrátane RAN (Radio Access Network) rádiového prístupu, CT (Core Network and Terminals) jadro siete a terminály a SA (Services and Systems Aspects) služieb. Tento veľký rozsah a spolupráca zabezpečuje, že mobilné zariadenia a siete od rôznych výrobcov/operátorov môžu spolupracovať a poskytovať bezproblémové pripojenie pre užívateľov po celom svete [8].

V súčasnej dobe sú pre širokú verejnosť hlavným popisom technologického vývoja v mobilných komunikáciach ich generácie. Slúžia pre hlavne pre marketing a jednoduchú orientáciu zákazníkom. Ako príklad je možné uviesť technológie piatej generácie tzv. 5G. Hoci sa tieto generácie stali dostatočným opisom pre širokú verejnosť, skutočný pokrok vo vývoji sa v štandardoch 3GPP uvádza na dosiahnutých míľnikoch v konkrétnych jej tzv. Releases. 3GPP pracuje na niekoľkých vydaniach súčasne. Pri vývoji pracujú paralelne na viacerých vydaniach súčasne. Jednotlivé vylepšenia a technológiách na ktorých pracuje sú tzv. ”zamrznuté”, teda nie je ich možné implementovať. Takto je to až do momentu, kedy sú dokončené pripravené na použitie. To je indikované ich uvedením v niektorom z jej vydaní. Teda prí svojom vývoji pracuje na viacerých vydaniach zároveň. Mohlo by sa zdať, že takýto postup práce pridáva určitú zložitosť do práce skupín, avšak takýto spôsob práce zabezpečuje, že pokrok je nepretržitý a stabilný [8].

3 Technológie Mobilného IoT

3.1 NB-IoT

Narrowband Internet of Things (NB-IoT), teda v preklade Internet vecí prevádzkovaný v úzkom pásme, vznikol pre potreby využitia mobilného pripojenia v rámci internetu vecí. Svoje využitie nachádza v aplikáciách s veľkým množstvom pripojených zariadení, pri ktorých sa kladie dôraz na nízku nákupnú cenu, celkovú nízku spotrebu a dlhú výdrž v rámci daného riešenia IoT. NB-IoT je technológia patriaca k LPWAN (Low-power wide-area network), pretože umožňuje efektívne pracovať v podmienkach, kde pomer signálu a šumu je veľmi nízky. Bola predstavená v 13. vydaní 3GPP (Release 13). Aj keď je technológia súčasťou LTE, je považovaná za úplne nové rádiové rozhranie [14].

Táto technológia bola špecificky navrhnutá pre dobrú koexistenciu s existujúcimi technológiami, ktoré 3GPP špecifikuje a vyvíja. Dosiahnuté to bolo použitím rovnakých časových a frekvenčných prostriedkov z existujúcich štandardov. Jej základ tvorí LTE, avšak pri vývoji bol primárne kladený dôraz na zjednodušenie jednotlivých komunikačných modulov a modemov s cieľom znížiť náklady oproti LTE. Z dôvodu rýchlejšieho a jednoduchšieho nasadenia využíva a zdieľa sieťovú architektúru EPS (Evolved Packet System). Taktiež so štandardom zdieľa rovnaké komunikačné pásma, numerológiu, multiplexné prístupové techniky, modulácie, kanálové kódovanie, symbolovú rýchlosť, prekladanie a iné. Príkladom dobrej koexistencie je implementácia v tzv. LTE Guardbande. Výhodou je dosiahnutie efektívneho prenosu a nemožnosť vzniku kolízií s dátovým a hlasovým prenosom [14, 5].

Pre splnenie výkonnostných kritérií uvedených pre mMTC (massive Machine Type Communications) od 3GPP bolo NB-IoT ďalej upravené v Release 15. Vďaka týmto úpravám dokáže naplniť potreby 5G IoT, ako sú zvýšené prenosové rýchlosti a spoľahlivá komunikácia. Týmto pomáha 5G zvýšiť kapacitu a IoT konektivitu [5].

Obr. 3.1: Logo NB-IoT [7].

3.1.1 Definícia vrámci Release 13

Release 13., bol uvedený v prvom kvartáli roku 2016. Keďže NB-IoT vychádza z LTE, z tohto dôvodu zdieľajú rovnaké prvky v RAN sieti. Vďaka tomu operuje so šírkou pásma 180 kHz, čo predstavuje šírku jedného Resource Blocku (RB) využívaných v LTE. V smere downlink využíva OFDMA (Orthogonal Frequency Division Multiple Access) rovanko ako pri LTE. Avšak v smere uplink zavádza SC-FDMA (Single Carrier - Frequency Division Multiple Accesss) pre podporu jednoduchých zariadení, a taktiež z dôvodu podpory veľkého množstva simultánnych prístupov [9, 10].

NB-IoT zavádza možnosť využitia vzdialenosti 3,75 kHz medzi subnosnými okrem klasických 15 kHz používaných v LTE systémoch. Pri použití 15 kHz môže NB-IoT prideliť buď jednotónový (8 ms) alebo viactónový (3 tóny, 6 tónov a 12 tónov) režim rôznym zariadeniam s trvaním 4 ms, 2 ms a 1 ms. Avšak pri 3,75 kHz podporuje iba pridelenie jednotónového režimu rôznym zariadeniam s 48 podnosnými frekvenciami trvajúcimi 32 ms [9, 10, 11].

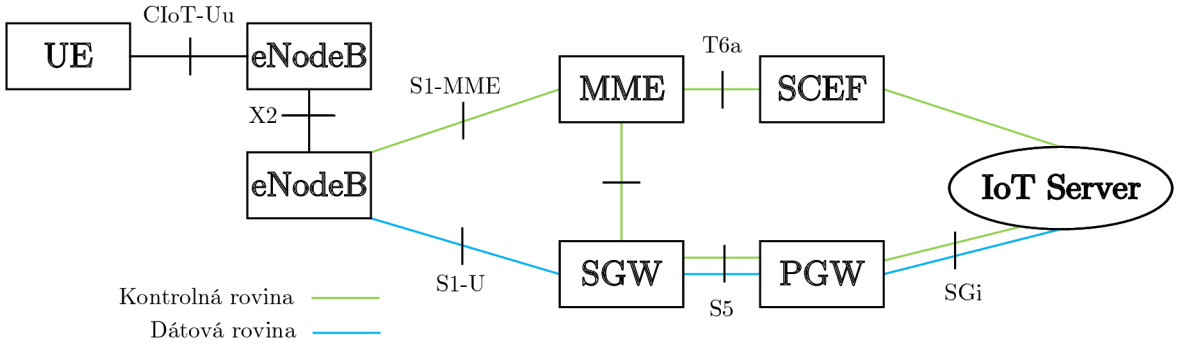
Taktiež poskytuje širšie pokrytie až do 164 dB MCL (Maximum Coupling Loss) čo predatvuje nárast o 20 dB oproti GPRS (General Packet Radio Service). Aby zvýšilo svoje pokrytie, NB-IoT používa až 128 retransmisií v uplinku a 2048 retransmisií v downlinku. To robí NB-IoT vhodným pre aplikácie, ktoré sú menej citlivé na latenciu a môžu tolerovať až 10 sekundové oneskorenie prenosu [11].

Ďalej pre zníženie ceny zariadenie dovoľuje NB-IoT iba HD (half-duplex) FDD (frequency-division duplex) a jednu prijímaciu anténu. Pre downlink sa používajú len QPSK (kvadratúrna fázová modulácia) a konvolučné kódy, čo dovoľuje zjednodušiť zariadenia oproti turbo kódu v LTE. Dosahuje prenosové rýchlosti 26 kb/s v smere uplink a 66 kb/s v smere downlink [9, 10].

Pre svoje potreby prebral aj EPS, avšak s určitými úpravami a optimalizáciami. Konkrétne modifikuje Control a User plane, teda používateľskú a kontrolnú rovinu. Jedným z dôvodov zmeny bola možnosť prenášať dáta ako NIDD (Non-IP Data Delivery), teda bez požitia IP protokolu. Takáto možnosť v prípade LTE neexistuje [9, 10].

Typicky sa na prenos dát využíva User plane. Novinkou je však možnosť dáta prenášať dáta po Contol plane. V tomto prípade prenosu prichádzajúce dáta s IP protokolom putujú na SGW (Serving Gateway) a ďalej na PGW (Packet Data Network Gateway) odkiaľ putujú už po internete k svojmu cieľu. Druhou možnosťou je smerovanie dát na nové rozhranie SCEF (Service Capability Exposure Function),

kedy sú dáta zapuzdrené do NAS správ. Využívaná hlavne pre malé nepravidelné objemy typicky vyskytujúce sa v strojovej komunikácii. Podstatou je smerovanie na jednu predurčenú IP adresu serveru, ktorý dáta ďalej spracováva. Výhodou použitia je zníženie prenášania nadbytočných dát a využitie plného potenciálu Control plane. V prípade použitia User plane, je prenos rovnaký ako v prípade LTE technológie, kde vznikajú nadbytočné dáta a oneskorenie spôsobené potrebou nadviazať spojenie. V tomto prípade je opäť možné dáta dva typy dát využívajúce a nevyužívajúce IP protokol. Pre lepšiu predstavu jednotlivých blokov tvoriacich EPS upravených pre NB-IoT je pod textom uvedený obrázok 3.2. UE (User Equipment) predstavuje koncové zariadenie, zvislé čiary križujúce sa vodorovnými predstavuje označenie jednotlivých prepojení a rozhraní medzi blokmi. MME (Mobility Management Entity) zabezpečuje autentifikáciu v sieti, roaming a ďalšie [9, 10].



Obr. 3.2: Architektúra NB-IoT [7].

NB-IoT zavádza ECL (Coverage Enhancement Levels), ktoré sa určujú na základe sily signálu prijatého od koncového zariadenia a sily signálu, ktorú uvádza koncové zariadenie. Následne eNodeB zhodnotí spojenie a určí kategóriu zariadenia. V princípe označuje počet opakovaní v uplinkovom kanále. Existovať môžu až tri úrovne [12]:

- ECL 0 – normálne pokrytie s maximálnou stratou spájania (MCL) do 144 dB,
- ECL 1 – robustné pokrytie s MCL do 154 dB,
- ECL 2 – extrémne pokrytie s MCL do 164 dB.

Nevýhodou technológie NB-IoT je nemožnosť využiť handover, teda možnosť predania prebiehajúcej komunikácie z jednej eNodeB druhej bez je prerušenia, ako je v prípade LTE možné. Handover je využívaný a potrebný najmä pri pohyblivých zariadeniach. Z tohto dôvodu je NB-IoT primárne určené pre statické zariadenia. Avšak existuje možnosť selekcie inej eNodeB počas toho ako sa zariadenie nachádza v Idle móde. Táto možnosť je umožnená na základe toho, že susediace eNodeB sú

medzi sebou prepojené X2 rozhranie, vďaka ktorému je umožnené rýchle nadviazanie komunikácie po tom ako zariadenie bolo neaktívne [9].

Keďže NB-IoT využíva frekvenčné pásmo so šírkou pásma 180 kHz, čo vrámci LTE predstavuje jeden resource blok, dokáže pracovať vo viacerých prevádzkových režimoch. Sú to nasledujúce tri režimy [4]:

- **Stand alone** - NB-IoT dokáže fungovať aj vrámci pásiem GSM, kde dokáže využívať volné pásma.
- **Guard Band** - pásmo pre NB-IoT je umiestený v ochrannom pásme LTE sietí, kde vyžíva práve tieto nevyužité resource bloky.
- **In-band** - kanál je umiestnený vrámci jednej z nosných použitých v LTE pásme. Využíva však len bloky, ktoré sú dopredu určené aby viacej neblokoval komunikáciu v LTE.

Vrámci Release 13. boli určené vysielacie pásma na ktorých môže technológia NB-IoT operovať. V tabuľke 2.1 sú zhrnuté všetky tieto pásma aj s frekvenčnými rozsahmi.

Tab. 3.1: Frekvenčné pásma pre NB-IoT podľa dokumentu 3GPP Release 13 [13].

Označenie pásma	**Rozsah frekvencií pre uplink [MHz]**	**Rozsah frekvencií pre downlink [MHz]**
B1	1920 - 1980	2110 - 2170
B2	1850 - 1910	1930 - 1990
B3	1710 - 1785	1805 - 1880
B5	824 - 849	869 - 894
B8	880 - 915	925 - 960
B12	699 - 716	729 - 746
B13	777 - 787	746 - 756
B17	704 - 716	734 - 746
B18	815 - 830	860 - 875
B19	830 - 845	875 - 890
B20	832 - 862	791 - 821
B26	814 - 849	859 - 894
B28	703 - 748	758 - 803
B66	1710 - 1780	2110 - 2200

Keďže cieľom NB-IoT je vytvoriť IoT zariadenia s malou spotrebou a veľkou vý-

držou na batériu, ktorá by mohla dosiahnuť až 10 rokov, bolo nevyhnutné optimalizovať ich spotrebu energie. Zariadenie v rámci IoT strávi veľkú časť času v nečinnom Idle móde, a preto bolo dôležité práve túto časť optimalizovať. V Release 13 boli uvedené dve techniky pre optimalizáciu spotreby: eDRX (extended Discontinuous Reception) a PSM (Power-Saving Mode) [4].

V režime eDRX zariadenie prechádza do Idle módu, kde zostáva určitý čas, a následne prechádza do DRX módu, kde prijíma paggingové okná. Rozdielom oproti klasickému DRX je čas, počas ktorého zariadenie pretrváva v Idle móde. Pri klasickom DRX je to maximálne 10,24 s a pri eDRX až 10 485,76 s [4].

V PSM režime zariadenie prechádza do spánkového módu, má nastavený určitý čas, vypnuté sú prijímacia aj vysielacia časť a udržiava si len časovú referenciu. Po uplynutí nastaveného času zariadenie odosiela dáta alebo vykonáva TAU (Tracking Area Update) a následne môže prejsť do DRX módu alebo opäť do spánkového režimu. Časovú hodnotu je možné nastaviť až na 413dní [4].

V oboch režimoch, PSM aj eDRX, si zariadenie udržiava kontext potrebný pre opätovné pripojenie, čo umožňuje ďalšie zníženie energie, ktorá by inak bola potrebná na znovupripojenie k sieti [4].

3.1.2 Definícia vrámci Release 14

Vydanie Release 14. bolo uvedené v druhom kvartáli roku 2017. Dôležitou časťou bolo vylepšenie funkcionality pre určovanie polohy. Pribudli dve nové možnosti určenia polohy. Prvým z nich je ECID (Enhanced Cell Identifier), ktoré je založené na hodnote TA (Time Advance). TA predstavuje dobu odozvy medzi zariadením a eNodeB, na základe čoho je možné určiť vzdialenosť medzi nimi. Pôvodne bolo možné určiť polohu len pomocou základe pripojenej základňovej stanice. Druhý spôsob, OTDOA (Observed Time Difference of Arrival), sa spolieha na meraní ToA (Time of Arrival) hodnoty zmeranej po prijatí referenčného signálu od eNodeB. Hodnoty sa následne posielajú na server, ktorý vyhodnocuje polohu zariadenia. Táto hodnota môže byť odmeraná medzi viacerými eNodeB a zariadením, na základe čoho vie server určiť presnejšiu polohu [4, 10].

Medzi ďalšie dôležité vylepšenie patrí zvýšenie prenosových rýchlostí. Táto rýchlosť bola jednou zo slabín NB-IoT v Release 13. Rýchlosť v smere downlink sa zvýšila až na 127 kb/s a v smere uplink až na 158,5 kb/s, čo predstavuje nárast o 101 kb/s v smere downlink a 94 kb/s v smere uplink. Vďaka tomu bolo nutné vytvoriť nový typ zariadenia Cat-NB2 [4].

Súčasťou bolo taktiež možnosť využívať typ komunikácie multicast, kde dáta adresované pre skupinu zariadení sú odoslané jedným prenosom. Hlavým využitím môže byť pre aktualizáciu firmvéru zariadenia. Vďaka využitiu multicastu je možné znížiť odozvu, keďže dáta sú adresované viacerým zariadeniam [10].

Pôvodné vydanie uviedlo dva typy zariadení na základe vysielacieho výkonu s 20 a 23 dBm. Keďže cieľom NB-IoT je vytvoriť zariadenia s čo najnižšou spotrebou, prípadne aj rozmermi, vznikla potreba využívať malé batériové články. Tieto články by však pri aktuálnych vysielacích výkonoch nedokázali napájať zariadenie dlhodobo. Preto bolo v tomto vydaní uvedený nový typ s vysielacím výkonom 14 dBm. Znížením výkonu sa síce zhoršilo pokrytie, avšak aj napriek tomu dostatočné a v porovnaní s technológiou GSM alebo LTE je stále o 10 dB vyššie. Tento typ nájde svoje primárne uplatnenie v miestach hustým pokrytím. Súčasťou tohto rozšírenia boli pridané aj nové pásma použiteľné pre technológiu NB-IoT. Jednotlivé pásma sú rozpísané v tabuľke 2.2 [4].

Tab. 3.2: Frekvenčné pásma pre NB-IoT podľa dokumentu 3GPP Release 14 [13].

Označenie pásma	**Rozsah frekvencií pre uplink [MHz]**	**Rozsah frekvencií pre downlink [MHz]**
B11	1427,9 - 1447,9	1475,9 - 1495,9
B25	1850 - 1915	1930 - 1995
B31	452,5 - 457,5	462,5 - 467,5
B70	1695 - 1710	1995 - 2020

3.1.3 Definícia vrámci Release 15

Vydanie Release 15. bolo uvedené v roku 2018, bolo to prvé vydanie s uvedením 5G štandardu. Medzi hlavné vylepšenia technológie NB-IoT partia: väčšia spektrálnu efektivitu, EDT (Early Data Transmission), mechanizmus prebudenia WUS (Wake-up signals) a prístup k sieti na požiadanie SR (Scheduling request), zvýšenie spoľahlivosti a dosahu, podporu malých buniek a technológie LTE Device to Device. Uvedená bola podpora TDD, ktorá doteraz v NB-IoT chýbala čo dopomôže ku koexistencii s 5G a eMTC (enhanced Machine Type Comunication. Vďaka tomu je zaručená podpora zariadení do budúcnosti, keďže sa počíta že životnosť je okolo 10 rokov [5].

Prvou spomenutou bolo znížené odozvy. Hlavnú úlohu v znížení malo upravenie vyhľadávania základňový staníc a získavaniu informáciach o systéme vo všetkých režimoch prevádzky. Docielené to bolo pomocou [5]:

- Ďalšieho opakovania NPSS/NSSS/NPBCH tak, aby sa minimalizovala falošná detekcia a zlepšili korelačné vlastnosti.
- Ďalšieho opakovania SIB1-NB v iných podrámcoch alebo na iných nosných.
- Nové mechanizmy ako sú nový signál prebudenia, ktoré umožnia zariadeniu vynechať čítanie MIB-NB, SIB1-NB a SI-správ.

Podstatou Early Data Transmission, teda skorého prenosu dát umožniť prenos v oboch smeroch už v tvz. Správe 3 (Msg3) a Správe 4 (Msg4). Tieto správy sú prenášané počas RA (Random access), teda procedúry náhodného postupu. Vďaka tomu znižuje réžiu signalizácie pre nastavenie spojenia a skracuje tak celkový čas prenosu. Výhodou je, že ak je celý prenos údajov dokončený v Msg3, sieť môže následne presunúť zariadenie do režimu RRC_IDLE (Radio Resource Control Idle). To znižuje náklady na signalizáciu pri uvoľňovaní RRC. Výsledkom zníženie celkového času prenosu a prijímania a to vedie k zlepšeniu životnosti batérie zariadenia. Skoré vysielanie a prijímanie tiež zlepšuje latenciu správ [5].

WUS (Wake-up signals), teda signál na prebudenie umožňuje eNodeB poslať signál prebudenia, aby inštruovalo zariadenie, aby monitoroval NPDCCH pre paging. V prípade, že takýto signál nedostane umožní zariadeniu preskočiť procedúry pagingu. To umožňuje udržiavať časti hardvéru vypnuté dlhšiu dobu a šetriť energiu potrebnú na dekódovanie NPDCCH a NPDSCH [5].

Oproti NB-IoT v starších vydaniach umožňoval SR len ako procedúru vyššej vrstvy a slúži procedúru RA na požiadanie dostatočného zdrojov na odoslanie správy o stave vyrovnávacej pamäte BSR (Buffer Status Report). V Release 15. pridal možnosť efektívnejšie implementáciu priamo v eNodeB [5].

Jedným z posledných vylepšením je BEST (Battery Efficiency Security for low Throughput). Je to typ šifrovania, ktorý umožňuje zašifrovať dáta z veľmi malou réžiou. Využitie je vhodné pri prenose na control plane s použitím symetrickej kryptografie 3GPP AKA [5].

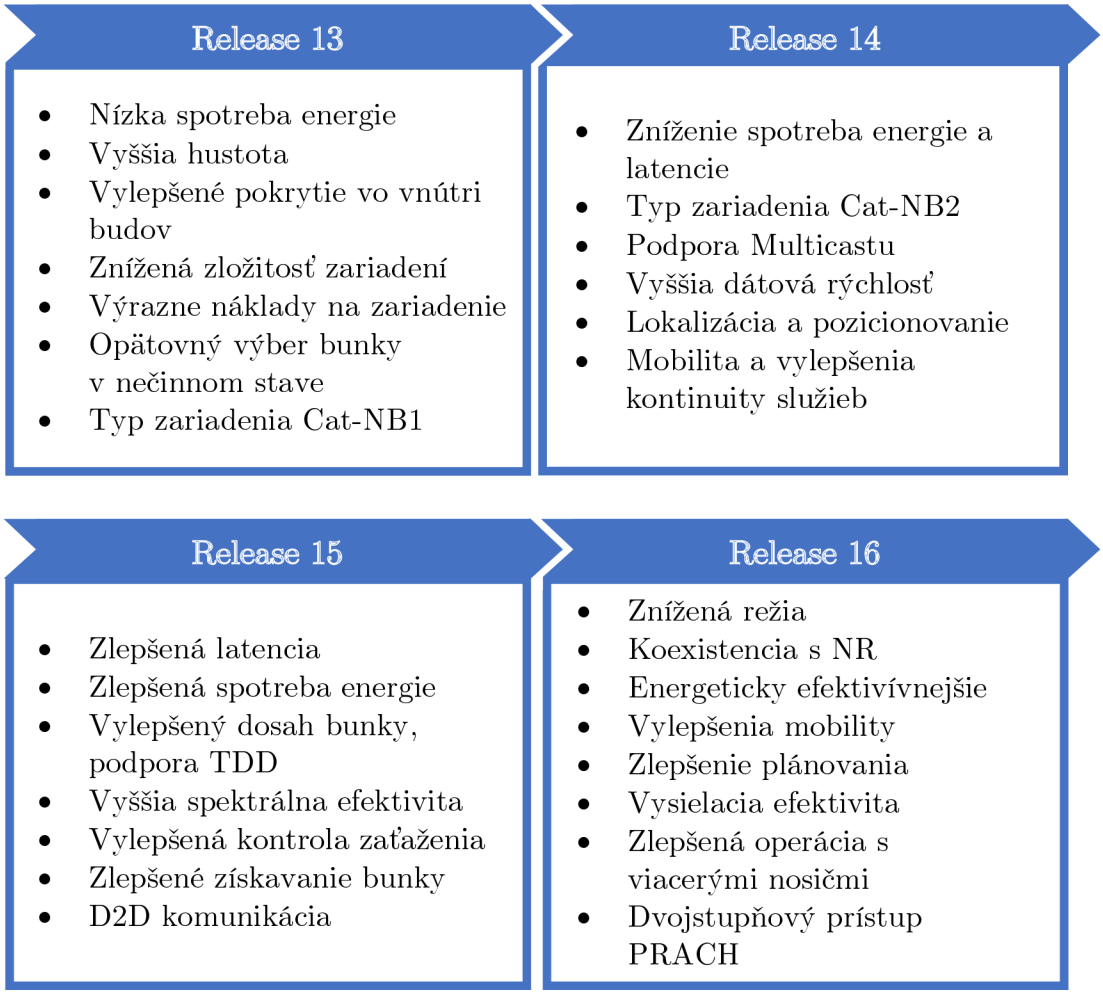
3.1.4 Definícia vrámci Release 16

Vydanie bolo uvedené v júny 2020. Medzi mnohé vylepšenia patria zamerané na vylepšenia predchádzajúcich funkcií: zlepšená efektivita prenosu a spotreba energie,zlepšené fungovanie pri fungovaní s viacerými nosnými, vylepšenie schedulingu,

vylepšenie spočívajúce v správe siete, vylepšenia týkajúce sa mobility. Taktiež sa jedná o prvé vydanie, kedy bolo NB-IoT integrované do 5G infraštruktúry [5].

Súčasťou tohto vydania bolo pridaná možnosť kedy zariadenia môžu vysielať v režime RRC-Idle bez prístupového grantu a v režime RRC connected bez grantu alebo s jednoduchým kontrolným grantom. Vďaka tomu sa zníži spotreba energie a latencia znížením prebytočných signálových správ [11].

Uvedené boli taktiež nové schémy ako CDM (Code division multiplexing) a MU-MIMO (m´Multi-User-Multiple Inputs Multiple Outputs) dovoľujúce simultánne prenosy viacerými užívateľmi pomocou zdieľania zdrojov v časovej ako aj frekvenčnej doméne. Umožnené je tak bez navýšenia bez zvýšenia počtu antén [11].



Obr. 3.3: Zhrnutie vylepšení jednotlivých vydaní.

3.2 LTE-M

Technológia Long-Term Evolution Machine Type Communication, bola špeciálne navrhnutá pre potreby IoT. LTE-M je skôr marketingový názov tejto technológie, avšak v technických dokumentoch a hlavne od vydania Release 13. je vhodnejšie ju označovať ako LTE Cat-M. Stretnúť sa taktiež môžeme s termínom eMTC (enhanced Machine Type Communication). Oproti NB-IoT prináša radu výhod a bližšiemu porovnaniu týchto dvoch technológii sa venuje kapitola 3.5. Za štandardizáciou stojí opäť skupina 3GPP. Zárodok technológie bol uvedený v rámci 3GPP Release 12., kde sa prvýkrát objavila kategória Cat-0. Vznikla s myšlienkou využiť technológiu LTE, kde by nevyužívala jeho pokročilé funkcionality a vysoké prenosové rýchlosti dosahujúcich stovky Mb/s. Cieľom bolo redukovať komplexnosť, spotrebu a náklady za komunikačný modem. Výsledkom je štandard, ktorý umožňuje prenosové rýchlosti približne 1 Mb/s v oboch smeroch, používa jednu anténu namiesto štandardného počtu dvoch a podporuje komunikáciu v half-duplex móde, pričom v danom momente môže komunikovať len jedna strana. V neskorších vydaniach sa, konkrétne v 13. objavila kategória Cat-M1, ktorá ďalej upravovala fyzickú vrstvu LTE pre potreby MTC (Machine Type Communication). Následne sa LTE - Cat-M rozvíjalo v každom nasledujúcom vydaní až po to súčasné. Vrámci tejto kapitoly sa práca venuje 13. až 16. vydaniu [4].

LTE Cat-M bola primárne navrhnutá rovnako ako NB-IoT pre zariadenia s nízkou spotrebou, dlhodobou výdržou umožňujúcou posielať väčšie množstva dát, s možnosťou väčšej mobily a Roamingu. Z LTE si taktiež prebrala dôležité aspekty zabezpečenia medzi ktoré paria identifikácia UE (User Equipment), čiže daného zariadenia, autentifikáciu, integritu prenášaných dát [14].

Využitie nájde v IoT riešeniach, kde medzi dôležité aspekty patria vlastnosti ako: veľký dosah, nízka odozva, mobilita, možnosť prenášať hovory vďaka podpore VoLTE (Voice over LTE), teda možnosť prenášať hlasové hovory. Vďaka týmto vlastnostiam, ako veľký dosah, dostatočná prenosová rýchlosť a využitie LTE technológii, patrí LTE Cat-M medzi typy LPWAN sietí s najväčším potenciálom a možnosťou využitia v každom odvetví IoT [14].

Obr. 3.4: Logo NB-IoT [7].

3.2.1 Definícia vrámci Release 13

Release 13 bol uvedený v prvom kvartáli roku 2016, predstavujúc štandard LTE Cat-M1. Podobne ako LTE, aj LTE Cat-M1 v rádiovej prístupovej sieti RAN využíva eUTRAN/eNodeB. V smere od zariadenia (uplink) využíva multiplexový prístup SC-FDMA a v smere k zariadeniu (downlink) OFDMA. Dátové kanály využívajú resource bloky s frekvenciou jedného resource bloku 180 kHz [14].

LTE Cat-M1 operuje s najmenšou možnou šírkou pásma pri LTE 1,4 MHz, umožňuje operáciu samostatne v standalone móde, alebo ako súčasť väčších pásiem s veľkosťou 3, 5, 10 a 20 MHz. Pre potreby zvýšenia výdrže batérie môže využívať tzv. PSM (Power Saving Mode) režim. V klasickom LTE existuje možnosť, kedy zariadenie na určitú dobu vypne svoju rádiovú časť. To má však za následok, že pri následnej ďalšej komunikácii je potrebné opäť nadviazať spojenie. V prípade využitia PSM, je pripojené a registrované neustále. Avšak prestane periodicky zisťovať pagging. V takomto režime zostane až do momentu, zasielania dát iniciované zariadení. Energetická efektívnosť je ďalej zvýšená využitím iba jednej antény [14].

Vďaka nižším prenosovým rýchlostiam je potrebná výpočtová sila procesoru a nároky na pamäť výrazne znížené. Možnosť znížiť vysielací výkon až na 3 dBm, najmä prípadoch s nízkym objemom prenosu, ďalej dopomáha znižovať energetické nároky zariadenia [14].

Jedným z hlavných cieľov vývoja bolo maximalizovať pokrytie pomocou viacerých techník. Patrí medzi ne zvýšenie vysielacieho výkonu dátových a referenčných signálov, ako aj možnosť opätovného vysielania v prípade detekcie strát alebo chýb. Ďalšou stratégiou bolo zníženie požiadaviek na prenosové rýchlosti, čo umožňuje efektívnejšie využívanie dostupného spektra [14].

Opätovné vysielanie, realizované v rámci jedného resource bloku pomocou TTI (Transmission Time Interval) balenia, minimalizuje potrebu prenosu veľkých dátových objemov tým, že odosiela len redundantné bity. Táto metóda umožňuje zariadeniu dopočítať chýbajúce bity a zlepšiť tak spoľahlivosť doručenia [14].

Medzi ďalšiu možnosť zvýšenia pokrytia pokrytia a zabezpečenie úspešného doručenia sa tiež využíva modulácia QPSK (Quadrature Phase-shift Keying) namiesto 16 QAM (Quadrature Amplitude Modulation), ktorá je štandardom pre LTE Cat 8. Vďaka tomu sa pokrytie rozšírilo teoreticky až sedemkrát. Aj keď by použitie QPSK mohlo teoreticky znížiť efektívnosť prenosu, pri LTE Cat-M, ktoré má nižšie nároky na objem a rýchlosť prenášaných dát, toto neprináša významnú nevýhodu [14].

Pre rôzne možnosti použitia LTE Cat-M dokáže fungovať v dvoch režimoch rozšírenia pokrytia [14]:

- **Režim A** - Tento režim umožňuje opätovné odoslanie správ až 32-krát. Je predvoleným režimom a odporúča sa pre situácie, kde je potrebný prenos väčšieho objemu dát, mobilita a využitie VoLTE.
- **Režim B** - V tomto režime je možné opätovné odoslanie zvýšiť až na 2048-krát. Je ideálny pre maximalizáciu dosahu, napríklad pri umiestnení zariadenia v rušených oblastiach alebo vo vnútri budov. Jeho nevýhodami sú vyššia latencia a nižšia prenosová rýchlosť, čo ho robí vhodným pre prípady, keď sa zariadenie pohybuje minimálne alebo je stacionárne.

Medzi ďalšie ciele patrí možnosť zníženia potrebného napájania a tým predĺženia výdrže batérie. Využíva k tomu viaceré techniky: eDRX (extended Discontinuous Reception), upravený pripojovací mechanizmus, využitie časti pre kontrolné dáta na prenos obyčajných dát, a už vyššie spomínané použitie jednoduchších modulačných techník [14].

DRX je definovaný v klasickom LTE štandarde. Pozostáva z dvoch stavov On duration, vrámci ktorého zariadenie zisťuje paging pripojenia a DRX stav kedy je zariadenie v spánkovom režime. Mechanizmus eDRX upravuje stav On duration, vrámci ktorého je zariadenie stále pripojené ale nezisťuje neustále paging. Hlavnou nevýhodou tohoto prístupu je zvýšenie latencie, nakoľko nie je možné okamžite komunikovať s takým zariadením a to v prípade kedy tzv. spí alebo nezisťuje paging. Maximálna možná dĺžka DRX cyklu môže dosiahnuť až 43,69 minúty [14].

Posledná možnosť zahŕňa využívanie segmentu určeného pre kontrolné dáta na odosielanie bežných dát. Tento prístup je ideálny pre zariadenia, ktoré odosielajú iba malé objemy dát, keďže kapacita tohto kanálu je limitovaná jeho šírkou [14].

Tým že LTE Cat-M využíva šírku kanálu len 1,08 MHz, tak využíva na prenos dátovej a kontrolnej časti iba rovnakú šírku pásma 1,4MHz. Tým dokáže prenášať dát v rýchlostiach od desiatok kb/s až do 1 Mb/s v plne duplexnom móde. Najčastejšie je však implementovaný len v half-duplex móde [14].

Služby založené na lokalizácii LBS (Location-based services) prinášajú významnú hodnotu ekosystému CIoT. Príkladom využitia môže byť sledovanie logistiky, nositeľná elektroniku a chov zvierat. LTE Cat-M pre túto funkcionalitu podporuje dva hlavné typy lokalizačných technológií: [10].

- **ECID** - Rozšírená identifikácia bunky, táto metóda využíva informácie o identifikácii bunky na určenie obslužnej oblasti zariadenia. Doplnkové rádiové merania, ako sú rozdiely v čase prijímania a vysielania od zariadenia a eNodeB, uhol príchodu signálu, a prijatý výkon referenčného signálu (RSRP)/kvalita prijatého referenčného signálu (RSRQ), umožňujú zvýšiť presnosť určenia polohy.
- **OTDOA** - Pozorovaný časový rozdiel príchodu, pri tejto metóde zariadenie odhaduje časový rozdiel medzi referenčnými signálmi prijatými z rôznych eNodeB. Server polohy potom využíva techniky multilaterácie na určenie polohy zariadenia na základe týchto rozdielov.

Vrámci tohto vydania môže LTE Cat-M využívať pásma spomenuté v tabuľke 3.2.1 pod textom.

Tab. 3.3: Frekvenčné pásma pre LTE Cat-M podľa dokumentu 3GPP Release 13 [14].

Označenie pásma	**Rozsah frekvencií pre uplink [MHz]**	**Rozsah frekvencií pre downlink [MHz]**
B1 (2100 MHz)	1920 - 1980	2110 - 2170
B2 (1900 MHz)	1850 - 1910	1930 - 1990
B3 (1800 MHz)	1710 - 1785	1805 - 1880
B4 (1700 MHz)	1710 - 1755	2110 - 2155
B5 (850 MHz)	824 - 849	869 - 894
B7 (2600 MHz)	2500 - 2570	2620 - 2690
B8 (900 MHz)	880 - 915	925 - 960
B11 (1500 MHz)	1427,9 – 1447,9	1475,9 – 1495,9
B12 (700 MHz)	699 - 716	729 - 746
B13 (700 MHz)	777 - 787	746 - 756
B18 (800 MHz)	815 - 830	860 - 875
B19 (800 MHz)	830 - 845	875 - 890
B20 (800 MHz)	832 - 862	791 - 821
B26 (850 MHz)	814 - 849	859 - 894
B28 (700 MHz)	703 - 748	758 - 803
B31 (450 MHz)	452,5 – 457,5	462,5 – 467,5
B39 (1900 MHz)	1880 – 1920	1880 – 1920
B41 (2500 MHz)	2496 – 2690	2496 – 2690

3.2.2 Definícia vrámci Release 14

Vydanie Release 14. bolo uvedené v druhom kvartáli roku 2017. Jeho súčasťou boli uvedené aj iné technológie zahrňujúce 5G a vylepšenie typu zariadenia LTE Cat-M2 pre LTE Cat-M. Jeho hlavným zameraním bolo zvýšenie priepustnosti a to až na rýchlosť v smere downlink na 10 Mb/s a uplink na 4 Mb/s. Reálne hodnoty downlinku sa pohybujú okolo 7 Mb/s. To bolo dosiahnuté rozšírením pásma z 1,4 na 5 MHz a zväčšením veľkosti transportných blokov. Pásmo sa využíva len v prípade kedy je použitý režim A. V režim B zostáva nezmenený. Upravený bol aj VoLTE, ktorý lepšie funguje v half-duplex móde. Pridaná bola možno multicastu pre potreby OTA (Over-The-Air) aktualizácii firmvéru [15, 16].

Toto vydanie taktiež upravuje OTDOA funkcionalitu pre určovanie polohy. Zariadenie LTE Cat-M môže prijímať dlhšie prenosy PRS, aby získalo potrebný počet podrámcov PRS na presné meranie časových rozdielov príchodov.Niektoré pokročilejšie zariadenia môžu tiež využívať viaceré konfigurácie prenosu PRS na dosiahnutie vyššej presnosti polohy [16].

3.2.3 Definícia vrámci Release 15

Vydanie Release 15. bolo uvedené v roku 2018. Medzi vylepšenia tohto vydania patria: zníženie latencie a spotreby energie, zlepšenie spektrálnej efektivity pomocou podpora 64-QAM, a vlastností zariadení ako podpora vyššej rýchlosti, zníženie výkonovej triedy, zlepšenie riadenia v nečinnom stave, a vylepšenia eDRX [15].

Medzi iné vylepšenia možno spomenúť: Podpora zlepšenia pokrytia pri pohybe pre vyššie rýchlosti okolo 200 km/h, špecifikácia novej výkonovej triedy zariadení 14 pre nositeľné prístroje, uvedenie wake-up signálu a kanálu, EDT teda prenos dát počas techniky RA rovnako ako pri NB-IoT [16].

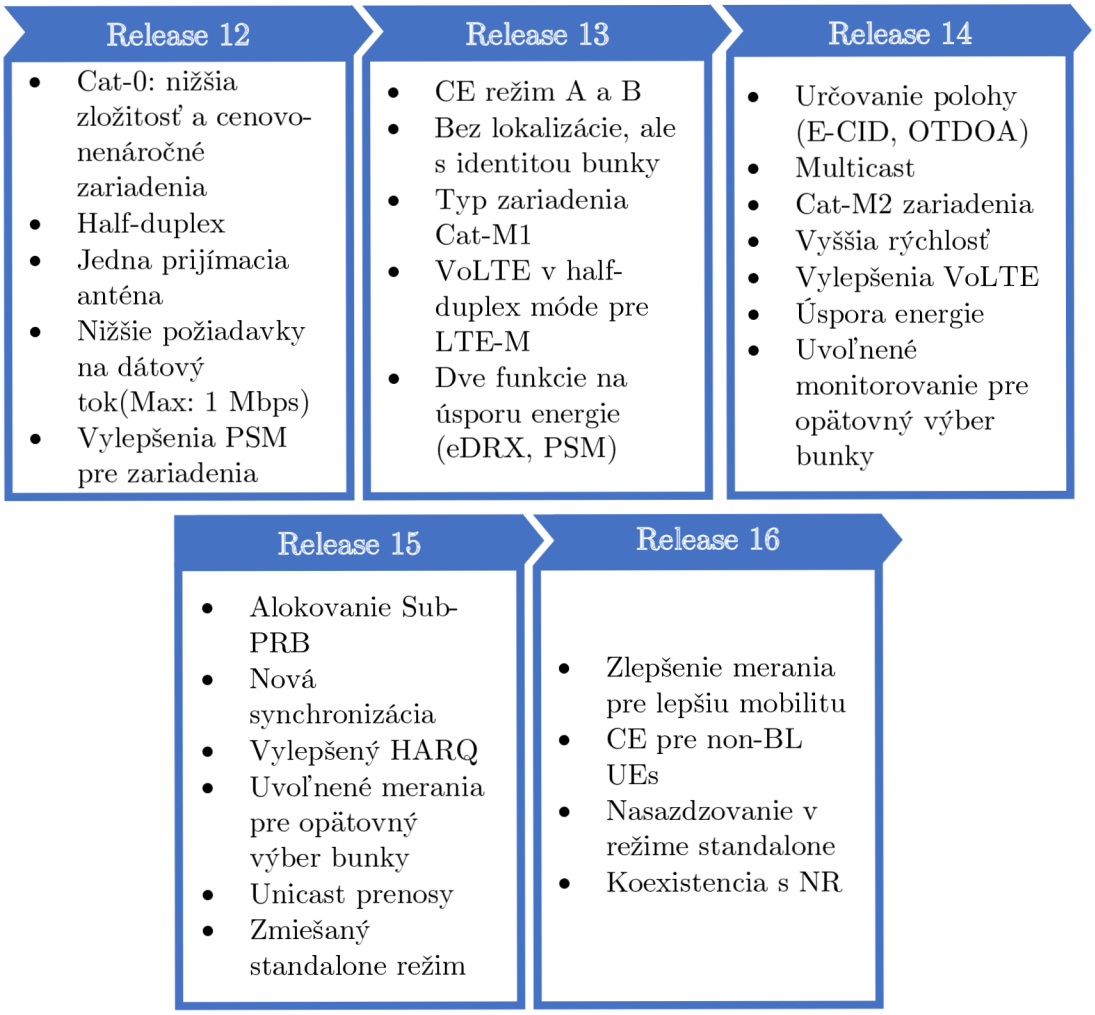
3.2.4 Definícia vrámci Release 16

Vydanie bolo uvedené v júny 2020. Súčasťou bola integrácia 5G za účelom zdieľania schopností 5G, zlepšenia pokrytia pre jednoduchšie zariadenia bez redukcie šírky pásma, vývoj možností v standalone móde a vylepšenia mobility.

ETD bola ďalej vylepšená zavedením uplink prenosu pomocou PUR (Preconfigured Uplink Resources) teda predkonfigurovaných uplink zdrojov. PUR je primárne určený pre stacionárne zariadenia s buď pravidelným alebo pseudo-meniacim sa tokom dát. Pri použití PUR, prenos dát môže byť dokončený len pomocou dvoch

správ (t. j. Msg3 a Msg4.) a obidve, prenos prístupovej predvolby náhodného prístupu (Msg1) a odpoveď na náhodný prístup (Msg2) môžu byť vynechané. Vo verzii Release 16 boli zavedené dve formy PUR: dedikovaný PUR a zdieľaný PUR [5].

Zhrnutie najvýznamnejších a najpodstatnejších vylepšení LTE Cat-M v jednotlivých vydaní sa nachádza v obrázku 3.5 pod textom.



Obr. 3.5: Zhrnutie vylepšení jednotlivých vydaní pre LTE-M [7].

3.3 NR-RedCap

New Radio - Reduced capability, skrátene RedCap, bola prvýkrát uvedená v Release 17. Jedná sa o technológiu postavenú na 5G NR s obmedzenými možnosťami, vzniknutú s cieľom zaplniť medzery medzi existujúcimi IoT technológiami [5].

Reflektuje na špecifické potreby, ktoré súčasné štandardy 3GPP, ako LTE Cat-M a NB-IoT, nedokázali v plnej mierne naplniť. Patria medzi ne vyššia prenosová rýchlosť, spoľahlivosť a nižšia odozva v porovnaní s už spomínanými štandardmi. Avšak, v porovnaní s už existujúcimi 4G a 5G technológiami si zachováva a spĺňa špecifické požiadavky CIoT, ako nižšia komplexnosť, cena a výdrž jednotlivých zariadení [5].

Vzhľadom na to, že je RedCap postavený na základoch 5G NR technológie, zdieľa s ňou viacero spoločných špecifických aspektov. Umožňuje tak možnosť pripojenia k 5G Core sieti, ďalej dovoľuje pripojenie na veľkom rozsahu frekvenčných pásiem, taktiež podpora tzv. milimeter-wave pásiem, čo predstavuje frekvenčné pásma od 24GHz do 100 GHz. Vďaka svojmu ultra-flexibilnému dizajnu, RedCap zaručuje vysokú energetickú efektivitu na úrovni sieťového rozhrania. Systém je navrhnutý tak, aby bol kompatibilný s budúcimi štandardmi a normami iba s pomocou softvérovej aktualizácie. Navyše, využíva technológiu založenú na smerovaní lúčov (beamforming), ktorá umožňuje cielené smerovanie a zosilňovanie signálu priamo k zariadeniu, čím zvyšuje efektivitu prenosu a kvalitu signálu [5].

Oproti doterajším technológiám využívaných pre CIoT, RedCap poskytuje významné zvýšenie prenosových rýchlostí. Dosiahnuté je tak vďaka využitiu rôznych pokročilých techník. Príkladom je využitie dvoch antén, umožňujúca implementáciu technológie Multiple-input multiple-output (MIMO), ktorá dovoľuje zvýšenie kapacity prenosu dát. Taktiež sa využívajú pokročilé techniky modulácie pre zlepšenie efektivity využitia frekvenčného spektra [5].

Technológia RedCap sa tak pomaly stáva ideálnym riešením pre široké spektrum aplikácií v oblasti priemyselného IoT, bezpečnostných kamerových systémov a pokročilej nositeľnej elektroniky, kde je potrebná kombinácia vyššej dátové prenosovej rýchlosti, spoľahlivosti a energetické efektivity. RedCap tak umožňuje využiť IoT v nových oblastiach a predstavuje tak novú generácie IoT zariadení, ktoré využívajú výhody 5G technológie pri zachovaní nízkych prevádzkových nákladov a dlhej výdrže na jedno nabitie [5].

3.4 Techniky zabezpečenia prenosu

V dnešnej dobe, kedy je využitie mobilných sietí na prenos citlivých a osobných údajov bežné, je zabezpečenie týchto dát kriticky dôležité. Mobilné siete umožňujú prístup k rôznym službám, od komunikácie po finančné transakcie, čo zvyšuje riziko kybernetických útokov a krádeží dát. Zabezpečenie integrity a dôvernosti dát chráni používateľov a podniky pred neoprávneným prístupom a zneužitím informácií. Na-

vyše, v oblastiach s prísnymi reguláciami, ako sú zdravotníctvo a financie, je správne zabezpečenie prenosu dát nevyhnutné pre súlad s bezpečnostnými normami. S ohľadom na tieto predpoklady je dôležité poznať mechanizmy zabezpečenia prenosov pri NB-IoT a LTE Cat-M. Vychádzajú a veľmi pripomínajú tie využité pri LTE. Proces zabezpečenia od samotného pripojenia k sietí, zabezpečení v NAS a AS môže byť popísaný nasledovne [18]:

- **Identifikačné prvky zariadení a ich správa** - V NB-IoT je autentifikácia zariadení založená na tom, že každé zariadenie má určité poverenia, ktoré možno overiť unikátnym identifikátorom. Príkladom identifikátora môže byť IMEI (International Mobile Equipment Identity), avšak ten vie byť ľahko zneužiteľný. Preto je odporúčané využívať IMSI (International Mobile Subscriber Identity), ktorý je bezpečne uložený na SIM karte spoločne s autentifikačnými kľúčmi.
- **Zabezpečenie identity** je dosiahnuté nevyužívaním priamo IMSI, ale TMSI (Temporary Mobile Subscriber Identity), udelené sieťou, vďaka čomu nedôjde k zneužitiu IMSI.
- **Autentifikácia zariadenia, odberateľa a siete** - Proces overovania údajov zariadenia v NB-IoT, ale aj celkovo v LTE sieťach, je vykonávaný procedúrou AKA (Authentication and Key Agreement), teda autentifikácia a dojednanie kľúčov. Celý proces je možné rozdeliť do troch krokov overovania: 1. zariadenia a dojednanie kľúčov, 2. pre NAS, 3. pre AS. Avšak popis celej autentifikácie je nad rámec tejto práce.
- **Zabezpečenie integrity dát a kontrolných správ** - Využívajú sa tri možné algoritmy: SNOW3G, AES, ZUC, kde každá z použitých kľúčov má 128 bitov. Vďaka použitiu šifrovania je zabezpečený prenos medzi zariadením a eNodeB, ako pri dátach, tak pri kontrolných správach. Šifrovanie však nie je povinné, čo nie je doporučené.
- **Dôveryhodnosť dát** je riadená cez NAS a využíva rovnaké algoritmy
- **End-to-Middle a End-to-End zabezpečenia** - využíva rovnaký AKA proces pre ustavenie kľúčov. Avšak v prípadoch, kedy sa zariadenia pripájajú k sieti cez non-LTE prístupovú sieť, je táto procedúra pozmenená. V takýchto prípadoch je zabezpečenie overované AAA serverom, alebo je vytvorený IPsec tunel.
- **Spoľahlivosť doručenia** - Využívajú sa techniky HARQ (Hybrid Automatic Repeat Request), avšak v prípade NB-IoT je taký proces povolený len jeden.

3.5 Porovnanie technológii LTE Cat-M a NB-IoT

3.5.1 Zhodnotenie

NB-IoT nájde svoje uplatnenie v aplikáciách, pre ktoré je potrebné čo najvyššie pokrytie, čo najväčšia výdrž batérie, malé rozmery a schopnosť obsluhovať veľké množstvo zariadení pomocou jednej bunky. Avšak tieto aplikácie nemôžu požadovať možnosti mobility, nízku latenciu a veľké dátové prenosy.

Tab. 3.4: Porovnanie parametrov NB-IoT a LTE Cat-M [14, 24].

	NB-IoT (LTE Cat-NB1)	**LTE Cat-M (LTE Cat-M1)**
Pokrytie (MCL)	164 dB	155 dB
Technológia	LTE	LTE
Spektrum	Licencované	Licencované
Maximálny vysielací výkon	23 dBm = 200 mW	23 dBm = 200 mW
Dosah	11 km	10 - 15 km
Downlink Prenosová rýchlosť	0,5 - 27,2 kb/s	<375 kb/s
Uplink Prenosová rýchlosť	0,3 - 32,25 kb/s	<1000 kb/s
Výdrž	10+ rokov	10+ rokov
Cena modulu	<$6 (2023)	<$20 (2023)
Zabezpečenie	Rovnaké s LTE	Rovnaké s LTE

Využitie LTE Cat-M sa hodí pre viaceré prípady použitia, kedy technológia NB-IoT narazí na svoje limity. Jedným z prípadov je možnosť mobility v prípade LTE Cat-M, ktorá poskytuje prechod medzi bunkami bez prerušenia komunikácie, pričom zariadenie sa môže pohybovať rýchlosťami až 200 km/h. Ďalším prípadom je potreba vyšších dátových prenosov s takmer real-time komunikáciou. Súčasťou je aj možnosť využitia pre prenos hovorov pomocou VoLTE. Príklady použitia jednotlivých technológií sú zhrnuté a popísané v ďalších podkapitolách. Porovnanie jednotlivých parametrov oboch technológií je uvedené v tabuľke 2.3 [14].

Pri porovnaní týchto dvoch technológií je možné konštatovať, že ani jednu nemožno označiť za víťaza, pretože obe majú svoje špecifiká a každá je vhodnejšia pre iný prípad použitia. Dôležitým faktorom v prípade oboch štandardov bude bezpečnosť prenášaných dát, zabezpečenie zariadenia voči útokom na hardvér a v ne-

poslednom rade implementácia a podpora od jednotlivých mobilných operátorov v danom štáte. Len od ich úsilia pri rozširovaní pokrytia a poskytovaní výhodných služieb nielen firemným zákazníkom, ale časom aj jednotlivcom, závisí úspech oboch technológií.

3.5.2 Použitie NB-IoT

Hlavné využitie NB-IoT sa nájde v použití pre nezávislé senzory, teda pre také, ktoré nemajú možnosť neustáleho napájania z elektrickej siete. Ich úlohou je meranie teploty, hladín tekutín v určitých nádobách alebo spotreby plynu, vody a elektrickej energie. Preto je vhodný pre novo vznikajúci koncept „Smart Cities“ (inteligentných miest), kde by jednotlivé senzory slúžili pre rôzne aktivity v mestách. Medzi takéto činnosti patria manažment a čistenie miest po časoch najväčšej vyťaženosti s cieľom zabezpečiť hygienické štandardy, monitorovanie množstva odpadu v nádobách na odpad, meranie spotreby v domácnostiach, sledovanie počtu voľných parkovacích miest a mnohé ďalšie [14].

3.5.3 Použite LTE Cat-M

Vhodný pre aplikácie pri ktorých je potrebná mobility zariadenia, nižšej odozvy a vyššie dátové prenosy. Medzi takéto aplikácie hlavne patria [14]:

- **Monitorovanie hnuteľného majetku** - vypožičané náradie a zariadenia,
- **Monitorovanie automobilov** - spotreba pohonných hmôt, poloha a prejdená trasa automobilov,
- **Monitorovanie zvierat** - poloha a pohyb domácich, sťahovavých zvierat,
- **Monitorovanie životných funkcii** - krvný tlak, hodnota cukru v krvi, teplota...
- **Inteligentné meracie zariadenia** - monitorovanie aktuálnej spotreby elektriny, vody, plynu,
- **Platobné terminály** - pre komunikáciu platobných terminálov v obchodoch/stánkoch.

3.6 Nasadzovanie technológii mobilnými operátormi

3.6.1 NB-IoT

Pripojenie NB-IoT je v Českej republike poskytované troma operátormi: O2, T-Mobile a Vodafone. Podľa GSMA (Global System for Mobile Communications) sú

pre O2 obmedzené len na Moravsko-slezský kraj. Taktiež T-Mobile, má sieť dostupnú len v niektorých krajských mestách na frekvencii B20 (800MHz). Vodafone sa prezentuje s 100% pokrytím, využívajúc frekvencie B20 a B8 (900 MHz).

Na Slovensku je situácia ovládaná troma hlavnými operátormi s nasledujúcim pokrytím na základe ich webových stránok: Telekomom (96%), využíva frekvenciu B20, Orangeom (95%) na rovnakej frekvencii a O2 s pokrytím 52%.

3.6.2 LTE Cat-M

Rovnako ako pri NB-IoT sú v Českej republike služby LTE Cat-M prevádzkované tromi operátormi. O2 pokrýva 98,5% územia v pásmach B3 (1800 MHz), B7 (2600 MHz) a B20, Vodafone má pokrytie 93%, využívajúc pásma B1 (2100 MHz), B3, B7, B8 a B20, T-Mobile poskytuje služby LTE Cat-M avšak nezverejňuje k tomu žiadne dalšie informácie.

Na Slovensku sú služby LTE Cat-M ponúkané Orangeom a Telekomom. Orange operuje v pásmach B3, B7 a B20, zatiaľ čo Telekom neponúka informácie o využívaných frekvenciách ani o percentuálnom pokrytí.

3.7 Doporučenia pre implementáciu mobilného IoT

Asociácia GSMA je lobistická organizácia reprezentujúca záujmy viac ako 750 mobilných operátorov po celkom svete. Uviedla dokument, príručku pre implementáciu mobilných IoT technológii. V nej sa zameriava na vlastnosti a vylepšenia uvedené v konkrétnych vydaniach od 3GPP zameraných na CIoT. Dokument uvádza doporučenia pre podporu interoperability medzi rôznymi operátormi a sieťami. Následne uvádza doporučenia pre vlastnosti a vylepšenia pre LTE Cat-M a NB-IoT. Tie rozdeľuje do troch kategórii [17]:

- **Minimálne základné vlastnosti** - sú široko podporované a adaptované operátormi a výrobcami zariadení, príkladom sú režimy šetrenia PSM a eDRX),
- **Novo vznikajúce vlastnosti a vylepšenia**- novo uvedené vlastnosti, na ktorých implementáciu nebol dostatočný čas, typický čas implementácie sú 2 až 3 roky, napr.: VoLTE,
- **Vlastnosti s minimálnou implementáciou**- patria sem vlastnosti a zariadenia, ktoré už boli štandardizované ale neboli implementované, príkladom je adaptácia Cat M2 kategórie.

3.7.1 Minimálne základné vlastnosti

Táto kategória zahŕňa [17]:

- **Podpora pásiem** mobilnými operátormi je rôzno. Odporúčaním pre operátorov je aby využívali minimálne jedno pásmo v okolí 1 GHz a aby využívané pásma zverejňovali v GSMA Deployment mape, z dôvodu jednoduchšieho výberu zariadenia s podporovanými pásmami užívateľom.
- **Možnosti prenosu dát cez sieť**, pre LTE Cat-M je podpora prenosu IP dát skrz užívateľskú rovinu minimum, ktoré musí podporovať a to hlavne pre prípady využívania roamingu, zároveň je odporúčané využívať CIoT optimalizácie užívateľskej roviny. Podpora prenosu dát skrz kontrolnú rovinu nie je podporovaná u väčšiny operátorov, preto sa neodporúča pre nasadenie. V prípade NB-IoT je to podobné avšak, aktuálne nasadenie operátormi nepodporuje prenos cez užívateľskú rovinu preto odporúčania platia pre kontrolnú rovinu. Podpora prenosu dát bez IP záhlavia opäť nie je vo veľkom využívané, avšak ak je tu tá možnosť tak by dáta mali byť smerované skrz SGi rozhranie.
- **Podpora režimov PSM a eDRX** implementácia týchto režimov by mali byť bez obmedzení časovačov. Mali by tiež umožňovať ukladanie dátových paketov do medzipamäte, ak sa zariadenie nachádza v jednom z týchto spánkových režimov. V prípadoch využitia PSM a eDRX zároveň, je veľmi dôležité si dať pozor na nastavenia hodnôt časovačov pre správny pagging.
- **Nastavenie hodnôt GTP časovaču** je kľúčové najmä v prípadoch, keď sa zariadenie nachádza v roamingu a komunikuje cez GTP tunel. Hodnota určuje dobu, počas ktorej je tunel aktívny aj keď zariadenie spí. Odporúčané minimálne hodnoty sú 31 dní pre NB-IoT a 24 hodín pre LTE Cat-M.
- **Využívanie režimu A pre rozšírenie pokrytia** je povinný pre zariadenia a veľmi odporúčaný pre implementáciu operátormi. Režim B, dobrý pre prenos nízke množstva dát avšak sa skoro vôbec nevyužíva a do roku 2022 nebol implementovaný žiadnym s výrobcov alebo operátorov.
- **Podpora režimov rozšíreného pokrytia pre NB-IoT** odporučenie je aby operátori podporovali všetky 3 režimy rozšíreného pokrytia,
- **Podpora SMS správ** je na užívateľovi, či sa rozhodne využívať SMS alebo využije alternatívu v podobe prenosu cez UDP poprípade NIDD (Non-IP Data Delivery), ktoré však nie je nasadzované.
- **Podpora a nastavenie C-DRX (Connected-mode DRX) a C-eDRX (Connected-mode eDRX)**režimov v stave pripojeného zariadenia. Tieto režimy umožňujú zariadeniam aj počas aktívneho pripojenia k sieti prejsť do úsporného režimu a to v prípade C-DRX až na 2,54 sekundy a v C-eDRX až na 10,24 sekúnd.

- **Deaktivácia UICC** by mala byť podporovaná a to aj v prípadoch, kedy sa zariadenie nachádza v eDRX režime.
- **Podpora rôznych tried vysielacieho výkonu**, minimum ktoré by operátori mali podporovať je 23dBm, prípadné použitie nižších výkonov je na zvážení aj zo strany operátorov aj užívateľov, zvolenie zlej triedy môže viesť k nižšej cene zariadení avšak možným problémov v prípadoch nedostatočného pokrytia.
- **Podpora RAT typov**, pre využitie NB-IoT v roamingu je zásadné implementovať podporu RAT typy určenému pre NB-IoT na S6a rozhraní, rovnako tak aj pre LTE Cat-M ktoré dostalo špecifické RAT, ktoré však ešte čaká na väčšiu implementáciu.
- **Zvoľnenie monitoringu používaného pre znovuzvolenie pripojenej bunky** je odporúčané hlavne pre statické zariadenia NB-IoT pre zlepšenie výdrže batérie.
- **Podpora rýchle odpojenia od siete pomocou Release Assistance Indication (RAI)** v prípade kedy zariadenie ukončilo vysielanie v smere uplink a pre úsporu energie odosiela RAI, čím urýchli odpojenie od siete. Podpora RAI by mala byť dostupná na zariadení a rovnako aj na sieti.
- **Podpora mechanizmov pre prístup k sieti pre zariadenia v režimoch rozšíreného pokrytia.** Tradičné mechanizmy prístupu ako ACB a EAB nedokážu rozlíšiť prítomnosť zariadení v režimoch rozšíreného pokrytia, čo môže v prípade vysokého zaťaženia siete viesť k opakovaniu prenosu. Podpora nových mechanizmov umožňuje odloženie prenosu na dobu menšieho zaťaženia siete.
- **Špecifické funkcie LTE Cat-M** medzi ne patria [17]:
  - Podpora half-duplex režimu,
  - Mobilita v pripojenom režime, nevyhnutá pre VoLTE,
  - Podpora väčších TBS v uplinku,
  - Podpora 10 HARQ procesov v downlinku, je nevyhnutné pre full-duplex režim avšak prináša výhody aj pre half-duplex režim,
  - Podpora posielania HARQ-ACK potvrdenia pre viaceré prenesené bloky v prípade half-duplex režimu.
- **Špecifické funkcie NB-IoT** zahŕňajú [17]:
  - Podpora všetkých režimov nasadenia,
  - Podpora novej kategórie zariadení NB2,
  - Možnosť informovanie o kvalite kanálu v downlink smere v NB-IoT, vďaka ktorej môže eNodeB optimalizovať pripojenie, dôsledkom čoho sa znížia energetické požiadavky zariadenia,
  - Podpora úprav pre zlepšení meraní.

3.7.2 Novo vznikajúce vlastnosti a vylepšenia

Patria sem [17]:

- **Podpora prenosu dát bez IP hlavičky NIDD** je aktuálne technicky možná pri LTE Cat-M, avšak ani v prípade NB-IoT nie je táto možnosť prenosu operátormi a výrobcami implementovaná. Preto nie je možné určiť, či sa táto funkcia stane bežne používanou.
- **Implementácia SCEF funkcií**, umožňujú bezpečný prístup k službám a možnostiam siete, avšak podpora je od operátorov je zatiaľ minimálna.
- **Optimalizácie užívateľskej roviny pre CIoT**, ktoré znižuje nadbytočnosť signálnych informácii o 75%.
- **Podpora zabezpečenia dát pomocou BEST** má potenciál predĺžiť výdrž batérie zariadení, čo predstavuje významný potenciál. Napriek tomu je príliš skoro na odporúčanie tohto typu zabezpečenia, keďže mnohí výrobcovia a operátori túto možnosť zatiaľ neimplementovali.
- **Podpora WUS signálov** pre zobudenie zo spánkových režimov,
- **Skorý prenos dát EDT**, umožňuje posielať dáta o veľkosti 328 až 1000 bitov pomocou správy Msg3 v procedúre náhodného prístupu. Túto možnosť by operátory a výrobcovia mali implementovať keďže má obrovský potenciál v znížení energetickej náročnosti na prenos.
- **Pred nastavenie EARFCN a geografických oblastí**, má potenciál znížiť čas potrebný na pripojenie v prípade roamingu,
- **Špecifické funkcie LTE Cat-M,** ktoré zatiaľ nie sú viacmenej implementované patria: VoLTE, podpora pre rýchlo-pohybujúce sa zariadenia, techniky pre zlepšenie využívania spektra,
- **Špecifické funkcie NB-IoT,** zahŕňajú úpravy pri použití FDD, ukladanie informácii v MME o zariadení a jeho prevádzkovom profile, zväčšenie rozsahu bunky, zmiešaného standalone režimu a podporu malých buniek.

Medzi ďalšie vylepšenia, ktorých implementácia je zatiaľ otázna, zahŕňa tie uvedené v Release 16. Medzi ne partia: možnosť poslania hromadného wake-up signálu GWUS, možnosť skorého prenosu EDT vyvolaného z MME, vylepšenie reportovania kvality signálu na downlink kanály, možnosť EDT v smere uplink vďaka PUR, pripojenia k 5G core sieti a vylepšenia v mobilite pri využití LTE Cat-M [17].

3.7.3 Vlastnosti s minimálnou implementáciou

Zaradiť sem môžeme [17]:

- **Podpora multicastového prenosu a prenosu skupinových správ** je zatiaľ minimálna.
- **Špecifické funkcie LTE Cat-M**, zahŕňa podporu novej kategórie Cat-M2 zariadení, podpora širších kanálov 5 MHz alebo 20 MHz, výber vysielacej antény riadené eNodeB.
- **Špecifické funkcie NB-IoT**,pratí sem mobility v connected režime, pagging a náhodného prístupu v prípade použitia non-anchor nosnej, podpora TDD režimu.

4 Komunikačné protokoly vhodné pre IoT

4.1 Adaptované protokoly pre využitie v IoT

Podstatou IoT je komunikácia cez internet, konkrétne prostredníctvom sady komunikačných protokolov známych ako TCP/IP. Základom tejto sady sú protokoly Transmission Control Protocol (TCP) a Internet Protocol (IP), zahrnuté priamo v jeho názve. Pre plnohodnotnú komunikáciu je nevyhnutné implementovať aj viaceré základné protokoly, medzi ktoré patria už vyššie spomenuté IP a TCP, UDP (User Datagram Protocol) a mnohé ďalšie. IoT zariadenia sa vo veľkej miere nelíšia od typických zariadení komunikujúcich pomocou internetu. Pre rôzne komunikačné požiadavky sú už k dispozícii adekvátne protokoly a nie je tak nevyhnutné vytvárať nové. Dobrým príkladom je protokol Secure Shell (SSH), ktorý pre svoju univerzálnosť môže byť využitý pre rôzne aplikácie.

4.1.1 UDP

Protokol UDP tvorí základný kameň v moderných komunikačných sieťach. Jedná sa o tzv. nespoľahlivý protokol, pretože pri prenose dát pomocou správ zvaných datagramy nie je zabezpečené ich potvrdenie o korektnom doručení. Datagram je jednoduchý v porovnaní s inými typmi správ u protokolov, vďaka čomu je vhodný na použitie pri prenosoch, kde je potrebné rýchle doručenie s čo najnižšou odozvou a nie je potrebné úspešné doručenie každého z nich. Hlavička obsahuje len potrebné informácie, ako sú zdrojový a cieľový port, dĺžka datagramu a kontrolný súčet, ktorý slúži na zistenie chýb v prenesených dátach. Jej veľkosť je len 8 bajtov. Najčastejšie je využívaný pre prenos videa a hlasu [19].

4.1.2 TCP

Protokol TCP je ešte starší ako protokol UDP. Patrí k skupine spojovo orientovaných protokolov so spoľahlivým doručením správ, známych ako pakety. To znamená, že pred začatím prenosu dát sa medzi komunikujúcimi stranami vytvorí spojenie, pričom si dohodnú určité parametre potrebné pre samotný prenos. Výhodou protokolu je, že v prípade doručenia chybného paketu, TCP zabezpečí jeho opätovné zaslanie a následne pakety usporiada do poradia v prípade ich rozhodenia. Taktiež umožňuje riadiť tok dát pre zabránenie zahltenia príjemcu alebo v prípade zmeny kapacity prenosovej siete. Oproti UDP je minimálna veľkosť hlavičky až 20 bajtov. Najčastejšie sa využíva pre aplikácie, kde nie je potrebná okamžitá odozva, príkladom je prenos webových stránok a prenos väčších dát [19].

4.1.3 SSH

SSH je veľmi rozšírený komunikačný protokol pre vzdialenú správu a ovládanie zariadení cez nezabezpečenú sieť. Vznikol ako bezpečnejšia varianta staršieho protokolu. Medzi jeho popredné vlastnosti patrí spôsob výmeny informácií; tie pred odoslaním zašifruje a po doručení automaticky dešifruje, vďaka čomu vytvorí transparentné šifrovanie. Je postavený na architektúre klient-server. Existujú dve verzie SSH-1 a SSH-2. Vo svete je najviac používaná softvérová implementácia OpenSSH [20].

Medzi jeho kľúčové vlastnosti patria [20]:

- **Vzdialený prístup** - slúži primárne ako príkazová konzola zariadení bez priameho prístupu, ako sú vzdialené servery alebo sieťové prvky.
- **Náhrada zastaralých protokolov** - vznikol z dôvodu možnosti odpočúvania starších protokolov, ako Telnet, rlogin a rsh.
- **Šifrovanie** - využíva moderné a bezpečné šifrovacie algoritmy, zabráni tak odpočúvaniu na prenosovej trase.
- **Autentizácia** - Podporuje viaceré možnosti autentizácie klienta, nielen pomocou hesla ale aj kryptografických kľúčov.
- **Tunelovanie** - Skrz SSH je možné tunelovať, teda presmerovávať komunikáciu pomocou iných protokolov a takto ich bezpečne prenášať.
- **Prenos súborov** - umožňuje prenos súborov cez bezpečný kanál s použitím protokolov SCP (Secure Copy Protocol) a SFTP (SSH File Transfer Protocol).

4.2 Protokoly navrhnuté pre IoT

Ako už bolo spomenuté, vrámci IoT využívame už existujúce komunikačné protokoly, pre rôzne účely. Ale vďaka pokroku, zmenou uvažovania nad prenosom a spracovávaním dát, začala vznikať potreba navrhnúť a vytvoriť nové komunikačné protokoly. Vďaka čomu ich vzniklo a bolo štandardizovaných viacero takých, ktoré uspokojujú potreby jednotlivých oblastí IoT. Medzi hlavné potreby patrí najmä jednoduchosť a ľahkosť. Medzi ne partia protokoly ako MQTT (MQ Telemetry Transport), CoAP (L), LwM2M (Lightweight M2M) a mnohé ďalšie.

4.2.1 MQTT

Protokol MQTT je nenáročný a jednoduchý protokol určený pre M2M (Machine-to-Machine) a IoT (Internet of Things). Prenos informácií (správ) je zabezpečený pomocou transportného protokolu TCP a slúži na výmenu akýchkoľvek dát medzi zariadeniami. Historicky vznikol pre potreby zariadení IBM MQ, neskôr bol pretvorený a štandardizovaný firmou OASIS. Momentálne existuje viacero verzií, najviac využívané sú verzie 3.1.1 a 5.0. Protokol MQTT je pomerne veľmi rozšírený a pre implementáciu jeho klientov existuje viacero knižníc využívajúcich všetky populárne programovacie jazyky [21].

Medzi jeho kľúčové vlastnosti patria:

- **Jednoduchosť** - protokol je nenáročný na implementáciu.
- **Ľahkosť a efektívnosť** k prenášaným dátam nepridáva zložité záhlavia, vďaka čomu je energeticky úsporný a najmä vhodný pre použite v prostrediach s nízkou šírkou prenosového pásma.
- **Spoľahlivosť** - umožňuje nastavenie spoľahlivé prenosy správ.
- **Bezpečnosť dát** - využívať šifrovanie dát pomocou SSL/TLS a taktiež umožňuje autentizáciu jednotlivých klientov.
- **Nízka latencia** - vďaka jeho nenáročnom fungovaní, vie fungovať v reálnom čase.
- **Škálovateľnosť** - je vhodný pre požitie veľkého množstva zariadení.

Bol postavený na návrhovom vzore Observer. Podstatou tohto vzoru je existencia entít - vydavateľ a predplatiteľ. Vzťah medzi týmito entitami je N:1, teda existuje jeden vydavateľ s jedným alebo viacerými odberateľmi. Vydavateľ pri vzniku udalosti alebo jej zmene informuje odberateľa. V MQTT existujú tiež dva typy entít. Klient je prvou z nich, môže správy odoberať alebo informovať ostatných klientov. Pre fungovanie MQTT klienta nie je potrebné veľké množstvo výpočtového výkonu a môže byť implementovaný na najjednoduchších zariadeniach. Druhou entitou je tzv. broker. Ide o centrálny bod, server, ktorý zabezpečuje prijímanie správ, ich ukladanie a posielanie vybraným entitám. Taktiež zabezpečuje autentifikáciu a autorizáciu klientov [21, 22].

Každá zo správ je zaradená k určitej téme, tzv. „topic“. Entita, napríklad zariadenie so senzorom, môže v rámci určitej témy plniť dve funkcie. Prvou je publish, teda možnosť vysielať alebo vydávať správy. Druhou je subscribe, kedy sa prihlási k odberu a informácie iba prijíma. Vďaka príslušnosti zariadení k danej téme vie server, komu má správy posielať. Tém môže byť samozrejme viacero, pričom každé zariadenie môže byť v rámci jednej témy publisher a v inej téme subscriber. Každá

správa môže patriť len k jednej téme, pričom príslušnosť k danej téme je zapísaná v záhlaví paketu. Jednotlivé témy sú radené hierarchicky a oddelené pomocou lomky. Hierarchia nie je nijako daná a je len na užívateľovi, ako si ju zvolí.

Jedným z dôvodov, prečo je MQTT jednoduchým protokolom, je aj to, že užívateľ nemusí nijako komplikovane vytvárať nové témy. Stačí, ak nové zariadenie pošle správu s novou témou, server správu prijme a v prípade, že téma neexistuje, ju vytvorí. Následne čaká na správu, ktorou sa nejaké zariadenie prihlási k odberu správ [21, 22].

Aby mohlo zariadenie odosielať alebo prijímať správy, musí na začiatku nadviazať spojenie pomocou TCP na porte 1883. Ak sa bude využívať šifrovanie, spojenie bude ďalej zabezpečené pomocou protokolu TLS na porte 8883. Treťou možnosťou je spojenie pomocou WebSocketu na porte 8080.

Ďalším krokom v komunikácii je výmena tzv. kontrolných paketov, ktoré sú súčasťou MQTT. Týchto paketov je niekoľko, pričom prvý z nich je s názvom CONNECT. Tento paket nesie najdôležitejšie informácie. Jeho súčasťou sú príznakové bity (flags) pre špecifické nastavenie spojenia, ako napríklad overovanie klienta, nastavenie dĺžky spojenia a možnosť zanechať správu po odpojení. Ďalej obsahuje voľné pole Payload, teda samotné dáta, v ktorom sa nachádzajú údaje ako meno a heslo alebo špecifická správa.

Odpoveďou servera na správu CONNECT je správa CONNACK. Táto správa slúži primárne na potvrdenie spojenia alebo v prípade chyby obsahuje sekciu s dôvodom, prečo spojenie nemôže nastať.

Ak je spojenie nadviazané, klient môže poslať typ správy PUBLISH, čo je najdôležitejšia správa v rámci komunikácie cez MQTT [21, 22].

4.2.2 CoAP

Constrained Application Protocol, v preklade protokol pre obmedzené aplikácie, slúži, ako už z názvu vyplýva, na prenos aplikačných dát z jednoduchých, možnostiam obmedzených zariadení. Typicky sú to 8-bitové zariadenia s malými pamäťami RAM či ROM, ako sú rôzne senzory alebo aktuátory. Pre čo najmenšiu veľkosť správ využíva transportný protokol UDP, ale môže využívať aj metódy, ktoré umožňujú vytvoriť komunikáciu podobnú ako v prípade použitia TCP. Protokol patrí k skupine protokolov navrhnutých pre M2M komunikáciu a je založený na modeli požiadavka/odpoveď (request/response). Definovaný je v rámci RFC 7252 [23, 19].

Medzi jeho kľúčové vlastnosti patria:

- **Integrácia s HTTP** - navrhnutý pre integráciu s HTTP (Hypertext Transfer Protocol) protokolom, využíva podobné metódy ako sú GET, POST, PUT a DELETE. Taktiež je možné ho integrovať s inými IETF štandardmi.
- **Ľahkosť a efektívnosť** - k prenášaným dátam nepridáva zložité záhlavia, vďaka čomu je energeticky úsporný a vhodný pre pamäťovo obmedzené zariadenia.
- **Spoľahlivosť** - môže pracovať v dvoch režimoch: s potvrdzovaním, teda spoľahlivým doručením dát, alebo bez potvrdzovania doručenia, teda nespoľahlivým spôsobom.
- **Bezpečnosť dát** - v kombinácii s DTLS (Datagram Transport Layer Security) môže zabezpečiť prenos dát rovnako ako pri protokole TCP s použitím TLS.
- **Multicast** - umožňuje implementáciu multicastu, vďaka čomu efektívne zasiela rovnaké správy viacerým zariadeniam.

4.2.3 LwM2M

Protokol LwM2M je pomerne nový komunikačný protokol vytvorený a navrhnutý pre použitie v IoT. Uvedený bol v roku 2017 alianciou OMA (Open Mobile Alliance) s cieľom štandardizovať a zjednotiť dátové modely používané rôznymi výrobcami IoT zariadení a pridať možnosť jednoduchého manažmentu do jedného protokolu. Od uvedenia prvej verzie 1.0 boli do protokolu pridané viaceré vylepšenia, pričom aktuálna verzia je 1.2, uvedená v roku 2020 [19, 24, 25].

Ku kľúčovým vlastnostiam môžme zaradiť:

- **Jednoduchá integrácia** – využíva model objektov a zdrojov pre fungovanie nezávisle na platforme zariadenia,
- **Ľahká konfigurácia** – pred prvotným spustením, získa informácie o spojení z Bootstrap serveru,
- **Efektívnosť** – vhodný pre aplikácie s nízkou šírkou prenosového pásma,
- **Flexibilita** – podpora rôznych sieťových spojení,od WiFi k mobilným sieťam,
- **Bezpečnosť** – umožňuje šifrovanie prenášaných dát.

Postavený bol na základe protokolu CoAP, kde využíva jeho vstavanú schému posielania správ pre interakciu so zariadením. V prvej verzii bol prenos zabezpečený transportným protokolom UDP s podporou zabezpečenia DTLS. Taktiež umožňuje posielanie pomocou SMS správ. Nad komunikačnou vrstvou sprostredkovanou CoAP protokolom vytvára objektovo orientovaný dátový model, ktorý umožňuje posielanie dát a manažment zariadenia. Vrámci manažmentu je možné vzdialene ustanoviť a zmeniť údaje k zabezpečeniu komunikácie, aktualizovať firmvér, nastaviť parametre pripojenia k sieti, diagnostikovať a riešiť vzniknuté problémy [24, 25].

Vrámci protokolu sú definované 3 typy entít a to [24, 25]:

- **Bootstrap Server** – slúži pre prvotné nastavenie klienta, ktorému poskytuje všetky potrebné informácie pre pripojenie k serveru,
- **Server** – jeho úlohou je manažovanie klientov a zhromažďovanie získaných dát od klientov,
- **Klient** – stará sa o zber dáta na manažment objektov.

Dátový model je založený na objektoch, kde každý objekt má vždy definované svoje špecifické ID. V rámci svojej štruktúry obsahuje zdroje (Resources), ktorých obsah a počet závisí na použití objektu. Niektoré zdroje sú povinné. Keďže využívame objekty, ktoré môžu existovať vo viacerých inštanciách, každý objekt obsahuje aj ID inštancie. Pre prístup k dátam sa využíva tzv. URI (Uniform Resource Identifier), teda uniformný zdrojový identifikátor s daným formátom [24, 25]:

/<Object_ID>/<Instance_ID>/<Resource_ID>

Pre komunikáciu definuje štyri rôzne rozhrania: Bootstrap rozhranie, Registračné rozhranie, Rozhranie pre manažovanie zariadení a správu služieb a Rozhranie pre report informácií. Prvé slúži v prvotnej fáze počas Bootstrap procedúry. Registračným rozhraním dochádza k napojeniu klienta na server a periodickému zisťovaniu pripojeného zariadenia. Rozhranie pre manažovanie a správu služieb slúži na čítanie a zapisovanie dát a na spúšťanie rôznych úloh. Posledným rozhraním sa zisťuje stav objektov [24, 25].

V rámci verzie 1.1 bola pridaná možnosť používať transportný protokol TCP so zabezpečením pomocou TLS. Pridaná bola aj možnosť zabezpečenia aplikačnej vrstvy pomocou OSCORE, zabezpečujúce end-to-end šifrovanie. Vylepšená bola tiež podpora LTE Cat-M a NB-IoT technológií. Hlavným vylepšením verzie 1.2 bola možnosť posielať správy pomocou protokolu MQTT a HTTP. Pridaná bola aj LwM2M brána, ktorá umožňuje pridať zariadenia, ktoré nevyužívajú LwM2M. Aktualizovaná bola aj podpora protokolu TLS a DTLS vo verzii 1.3. V tejto verzii sa už počíta aj s podporou 5G technológií [24, 25].

4.2.4 Porovnanie MQTT, CoAP a LwM2M

Tab. 4.1: Porovnanie protokolov MQTT, CoAP a LwM2M [19].

	MQTT	**CoAP**	**LwM2M**
Transportný protokol	TCP	UDP, SMS	UDP
Port	1883, 8883	5683, 5684	5683, 5684
Min. veľkosť záhlavia	2 B	4 B	4 B
Max. veľkosť správy	256 MB	1024 B	1024 B
Potvrdzovanie	Áno	Áno	Áno
Round trip time	0,54 ms	0,1145 ms	0,1145 ms
QoS/Vrstva	Áno/Transportná	Áno/Aplikačná	Áno/Aplikačná
Mód posielania	Synchrónny	Asynchrónny	Asynchrónny
Zabezpečenie	TLS	DTLS	DTLS, OSCORE

5 IoT platformy

IoT platformy sú cloudové alebo lokálne aplikácie a služby, ktoré obsahujú vstavané nástroje a možnosti pre pripojenie zariadení do IoT ekosystému. Umožňujú programátorom zefektívniť a automatizovať procesy, spravovať veľké množstvo zariadení využívajúcich rôzne technológie alebo komunikačné protokoly. Poskytujú nástroje na zbieranie, spracovanie a analýzu dát z rôznych zdrojov, podporujú vzdialenú správu zariadení, automatizujú procesy a umožňujú používateľom vytvárať prispôsobené IoT aplikácie. Dôležitými aspektmi IoT platforiem sú podpora pre rôzne protokoly, zabezpečenie dát, integrácia s inými systémami a škálovateľnosť, aby vyhovovali rozličným potrebám aplikácií IoT. Každá z IoT platforiem obsahuje kombináciu viacerých kategórií poskytovaných funkcií [26].

Medzi ne patria [26]:

- **Dátové centrum** – Zahŕňajú lokálne a cloudové možnosti výpočtového výkonu a dátového úložiska. V IoT aplikáciach sú cloudové centrá veľmi využívané a tvoria ich neoddeliteľnú súčasť. Medzi najznámejších cloudových poskytovateľov patria: Amazon Web Services, Microsoft, Google...
- **Manažment dát** – zameraný na riadenie toku a kombinovanie dát z strojov a senzorov s už existujúcimi systémami dát,
- **Implementácia aplikácii** – dáva možnosť vývojárom jednoducho, rýchlo a efektívne skúšať, vytvárať a spravovať IoT aplikácie, sú poskytované samostatne alebo aj súčasťou IoT platformy,
- **Manažment pripojení** – primárne slúži pre správu zariadení pripojených pomocou mobilných služieb, ale využíva sa aj pre rozsiahle lokálne siete. V prípade mobilných pripojení sa tieto platformy nazývajú CMP (Connectivity Management Platform). Implementované sú väčšinou mobilnými operátormi a slúžia pre správu SIM kariet, vzdialenú správu pripojenia a zabezpečenia, jednoduchú fakturáciu za služby.
- **Manažment zariadení** – väčšinou poskytované výrobcami komunikačných modulov alebo celých zariadení, a slúžia pre ich správu, diagnostiku a optimalizáciu.

5.1 Prieskum a porovnanie platforiem

V roku 2023 každá z veľkých technologických firiem poskytuje minimálne určité služby pre použitie s IoT alebo ponúka celú radu služieb zaobalených do jednej IoT platformy. Medzi najvýznamnejšie firmy poskytujúce IoT služby a platformy patria

Microsoft, Amazon Web Services, Siemens, IBM, Cisco, Oracle, PTC a MongoDB [27].

Jednotlivé firmy sa snažia s ich IoT platformami presadiť na trhu, vďaka čomu sa predháňajú v rôznych aspektoch, či už ide o podporu rôznych služieb, možnosti a v neposlednom rade aj cenu. Veľké množstvo firiem ponúka na prvý rok prístup k platforme zdarma, aby nalákali nových potenciálnych zákazníkov. Neskôr je platba za poskytnuté služby realizovaná vo forme predplatného alebo závisí od počtu pripojených zariadení, posielaných správ, veľkosti úložiska a podobne.

Ďalej sa jednotlivé platformy snažia odlíšiť pomocou podporovaných komunikačných protokolov, možnosti ďalšieho spracovania dát, poskytovaného zabezpečenia pre služby a možnosti programovať a testovať aplikácie priamo v prostredí platformy.

Tab. 5.1: Porovnanie IoT Platforiem s najväčším počtom zákazníkov.

	Microsoft Azure IoT Hub	**AWS IoT Core**	IBM Watson IoT
Hlavné funkcie	Integrácia s Azure, Edge Computing	Integrácia s AWS, Správa zariadení	AI a analýzy, Real-time Insights
Škálovateľnosť	Vysoká	Vysoká	Vysoká
Podpora Protokolov	HTTPS AMQP MQTT Websocket	HTTPS MQTT Websocket	MQTT JMS
Implementácia vlastných protokolov	Áno	Áno	Áno
Možnosť vyskúšania	Áno (1 rok)	Áno (1 rok)	Nie

6 Testovanie protokolov

6.1 Testovací scenár a používané nástroje

Testovanie vybraných komunikačných protokolov sa uskutočňuje pomocou komunikačného modulu BG77. Je osadený na doske, ktorá umožňuje zmeniť rozhranie mini-PCIe (Peripheral Component Interconnect Express) na USB (Universal Serial Bus), vďaka čomu dovoľuje pripojenie tohto devkitu, teda vývojového zariadenia, k počítaču.

Pre potreby merania je zvolený malý počítač Raspberry Pi 4B s operačným systémom založeným na jadre Linux, konkrétne Raspberry Pi OS. Tento systém vychádza z distribúcie Debian. Pre komunikáciu s devkitom je potrebné na Raspberry Pi nainštalovať potrebné ovládače pre jeho správnu funkčnosť. Pre prvotné nastavenie parametrov je využitý program Minicom na komunikáciu s modulom cez sériovú linku, bežiacu cez USB rozhranie. Následne je využitý skript, pomocou ktorého je ukladaný čas odoslania do súboru.

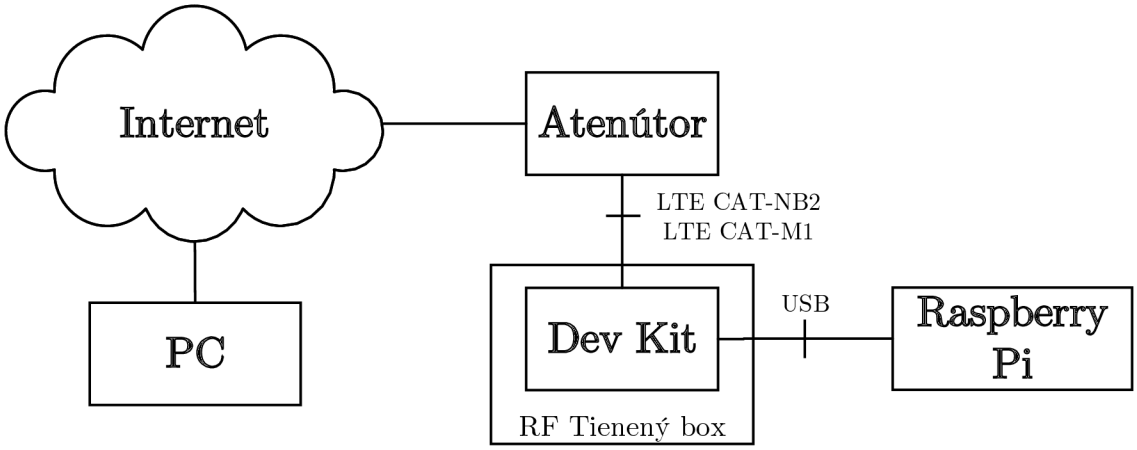
Ako server pre testovanie komunikačných protokolov je využitý počítač s operačným systémom Windows 11 Pro. Taktiež na tomto počítači prebieha zachytávanie odoslaných paketov/datagramov z daných serverov, kde hlavným sledovaným údajom je čas odoslania. To sa deje pomocou programu Wireshark vo verzii 4.0.4. Tento nástroj slúži na zachytávanie sieťovej prevádzky na rôznych sieťových rozhraniach. Vďaka Wiresharku, ktorý pakety/datagramy zachytáva priamo zo sieťovej karty, je možné minimalizovať oneskorenie, ktoré by mohlo vzniknúť spracovávaním dát, či už samotným systémom, alebo programom na ukladanie záznamov o prijatí.

Pred každým testovaním sa na každom zo zariadení, či už na Raspberry Pi alebo na počítači s Windows, vykoná synchronizácia s NTP (Network Time Protocol) serverom, konkrétne so serverom tak.cesnet.cz. Vďaka tomu sa dosiahne, aby obe zariadenia mali rovnaký presný čas. To umožňuje minimalizovať čas, teda odozvu, ktorá by mohla mať negatívny vplyv na merania a testy.

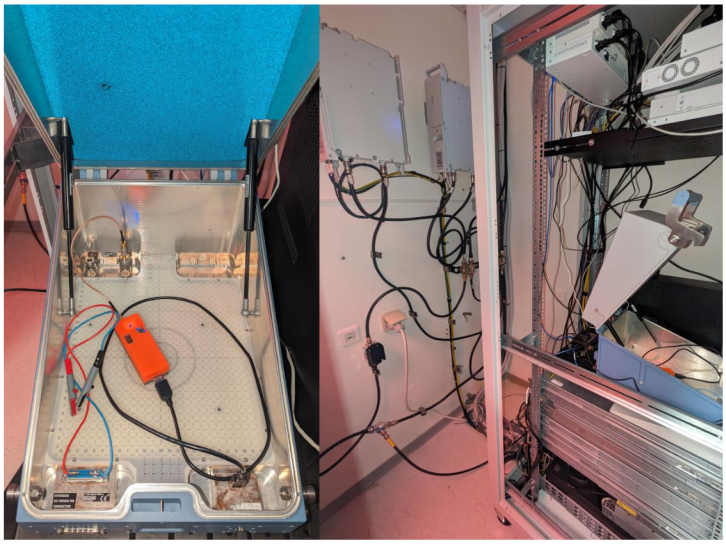
Merania prebiehajú v Unilabe v budove Fakulty elektrotechniky a komunikačných technológií. Unilab je vybavený vlastnou sieťou pre technológie LTE, 5G NSA, NB-IoT a LTE Cat-M. Sieť je tam prevádzkovaná operátorom Vodafone. Pre svoje potreby využíva dve RRU (Remote Radio Unit) jednotky, kde prvá vysiela vo frekvenčnom pásme B20 800 MHz a druhá v pásme B8 900 MHz. Siete NB-IoT a LTE Cat-M vysielajú práve vo frekvenčnom pásme 800 MHz. Z RRU jednotky je vyvedený

koaxiálny kábel, ktorý je vyvedený do rozdeľovača, ktorý väčšinu vysielacieho výkonu smeruje do antén rozmiestnených po miestnosti a približne 10 % ďalej do pevného útlmového článku s útlmom -30 dB. A to z dôvodu, aby bolo možné priamo pripojiť výstup antény zariadenia k výstupu z RRU. Pre možnosť simulácie rôznych signálových prostredí je ďalej využitý nastaviteľný útlmový článok AD-USB1AR36G95, ktorý dovoľuje nastaviť útlm signálu od hodnoty 0 dB až do 95 dB s krokom 0,25 dB.

K výstupu útlmového článku je pripojený vstup antény vyvedený na RF tieniacom boxe. Následne je už k RF boxu pripojený komunikačný modul.



Obr. 6.1: Schéma testovacieho scenáru.



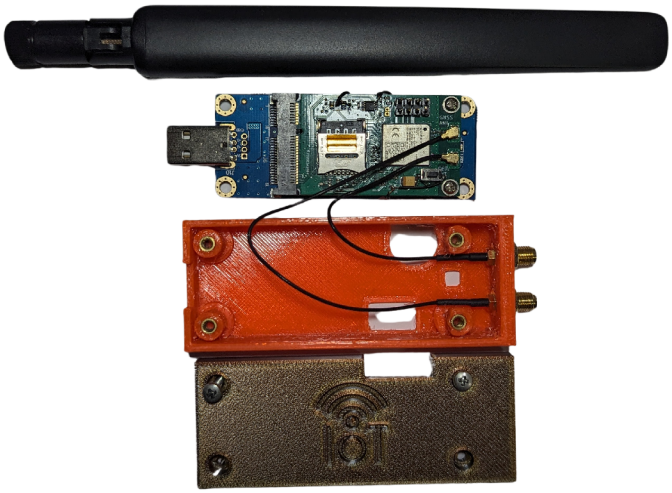
Obr. 6.2: Fotky z testovania.

6.1.1 Komunikačný modul

Pre testovanie bol použitý komunikačný modul BG77 od spoločnosti Quectel. Podporuje štandardy LTE Cat M1, LTE Cat NB2 (NB-IoT) a plne zodpovedá špecifikáciám z 3GPP Release 14.

Pri použití LTE Cat M1 dosahuje prenosové rýchlosti až 588 kb/s v smere downlink a 1119 kb/s v smere uplink a pri LTE Cat NB2 rýchlosti až 127 kb/s v smere downlink a 158,5 kb/s v smere uplink.

Súčasťou modulu je aj úsporný procesor ARM (Advanced RISC Machines) Cortex A7, vstavaná operačná pamäť a úložisko. Vďaka tomuto čipu natívne podporuje viaceré komunikačné protokoly: CoAP, MQTT, LwM2M, HTTPS, TCP/IP, SSL, FTP, PING, IPv6. Taktiež obsahuje mnohé možnosti zabezpečenia a to priamo v hardvéri. Je možné ho pripojiť k externým zariadeniam pomocou viacerých rozhraní: USB 2.0, UART, PCM, I2C, ADC a GPIO.



Obr. 6.3: Použitý komunikačný modul BG77.

6.1.2 Prvotné nastavenie modulu

Pred prvotnou komunikáciou modulu cez sieť operátora je potrebné nastaviť pomocou AT príkazov parametre a údaje pre pripojenie modulu k sieti operátora. Pre jednotlivé testovania a merania boli využité nasledujúce príkazy:

```
Nastavenie APN určené pre VUT, ktoré má prístup
do vonkajšej siete iba podla whitelistu

AT+CGDCONT=1,"IP","lpwa.vodafone.iot"

Nastavenie požadovanej RAT: NB-IoT

AT+QCFG="iotopmode",1,1

alebo LTE Cat-M.

AT+QCFG="iotopmode",0,1

Manuálne zadanie príkazu pre vyh adanie a registráciu
mobilného operátora Vodafone CZ v formáte MCC+MNC.

AT+COPS=1,2,"23003"

Zadanie rozšíreného výpisu pre výpis registrácie k
mobilnej sieti. Týmto príkazom sa taktiež aktivujú
automatické (nevyžiadané) výpisy o zmene registrácie.

AT+CEREG=4

Výpis stavu registrácie mobilnej siete

AT+CEREG?

Jeden zo sp sobov výpisu signálových parametrov.
Pre kompletné info o ServingCell vrátane CellID, pásma...

AT+QENG="servingcell"

Uzamknutie bunky na základe physical cell ID.
AT+QNWCFG="pci_lock","eMTC",1,0,147
AT+QNWCFG="pci_lock","NBIoT",1,0,147

Nastavenie režimu pre Release 14.
AT+QNWCFG="3gpp_rel_control","eMTC",1,B0
AT+QNWCFG="3gpp_rel_control","NBIoT",1,B0
```

6.2 Metodika testovania protokolu MQTT a LWM2M

Metodika merania bola nasledovná. Pred zvoleným testom bolo na zariadení nastavené, či pre pripojenie k sieti operátora bude využívať technológiu LTE Cat-M alebo NB-IoT. Tento skript je používaný na:

- obsluhu komunikácie s modulom,
- zasielanie potrebných AT príkazov,
- výpis vykonaných operácií a odpovedí na zadané AT príkazy,
- zachytávanie a ukladanie času odoslania správy,
- nastavenie parametrov protokolu,
- úpravu času odosielania medzi jednotlivými správami.

Následne pred začatím každého testu bolo pomocou skriptu zabezpečené, aby devkit bol nanovo pripojený k MQTT serveru pomocou AT príkazov. To bolo realizované nasledovne:

- nastavenie adresy a portu servera,
- prihlásenie klienta k serveru,
- odosielanie správ do určitej témy v podobe náhodnej hodnoty predstavujúcej teplotu,
- po úspešnom odoslaní zistené aktuálne hodnoty RSSI, RSRP, SINR, RSRQ.

Na Raspberry Pi sa údaje o čase odoslania, informácie o signále a Cell ID zaznamenávali do súboru. Na počítači pre potreby záznamu času prijatia a celkovej veľkosti prijatých dát prebiehalo zaznamenávanie sieťovej prevádzky pomocou programu Wireshark. Ten mal nastavený filter pre filtrovanie len IP adresy devkitu a protokolu. Výsledky o veľkosti správ a celkovom množstve prijatých dát sú vyhodnocované pomocou tohto programu.

Po dokončení boli dáta z Raspberry Pi skopírované na PC, kde skript získal zo záznamov len potrebné časové údaje, hodnoty RSRP a SINR a informáciu o Cell ID. Následne boli dáta vložené do tabuľkového programu Excel pre vizuálnu kontrolu a výpočet priemerných hodnôt. Výpis hodnota

6.2.1 NB-IoT

Testy vykonávané s technológiou NB-IoT prebehli ako prvé. Pri každom z testov bolo na server odoslaných 50 správ, pričom po každej odoslanej správe boli získavané údaje o RSRP a SINR. Taktiež bolo pre overenie konzistentnosti testovania zisťované Cell ID, aby bolo zachované pripojenie k rovnakej bunke a nedošlo k prepojeniu, ktoré by mohlo nastať pri vysokých hodnotách nastaveného útlmu.

Čas medzi odoslanými správami bol nastavený na 1 minútu s ohľadom na technológiu NB-IoT, ktorá má nastavený časovač neaktivity (Inactivity timer) na hodnotu 30 sekúnd. Po jeho pretečení dôjde k RRC Release. Z tohto dôvodu bol čas medzi správami nastavený na 1 minútu.

6.2.2 LTE Cat-M

Ovplyvňované parametre boli rovnaké aj pri technológii LTE Cat-M. Rozdielne boli hodnoty času medzi posielanými správami. Rovnako boli nastavené s ohľadom na inactivity timer, ktorý je v prípade LTE Cat-M 5 sekúnd. Preto boli časové rozostupy nastavené na 30 sekúnd a celkovo bolo poslaných 50 správ.

6.3 Testovanie protokolu MQTT

Použitý server, realizovaný lokálne na počítači, bol realizovaný s použitím implementácie MQTT brokeru od spoločnosti Eclipse s názvom Mosquitto, podporujúceho aktuálne verzie MQTT. Server je zviditeľnený do verejného internetu pre potreby pripojenia komunikačného modulu. Využitý je z dôvodu možnosti nastavenia bezpečnosti pri pripájaní MQTT klienta. Možnosť nadviazania spojení je poskytovaná bez akéhokoľvek overenia klienta, so základným overením pomocou mena, hesla a umožňuje zapnúť alebo vypnúť potreby šifrovaného spojenia.

6.3.1 Použité AT príkazy

```
Príkazy pre nastavenie SSL/TLS
AT+QFUPL="cacc.pem",1262,100
AT+QFUPL="key.pem",1732,100
AT+QFUPL="client.pem",1258,100
AT+QSSLCFG="cacert",2,"cacc.pem"
AT+QSSLCFG="clientcert",2,"client.pem"
AT+QSSLCFG="clientkey",2,"key.pem"

AT+QMTCFG="ssl",0,1,2
AT+QSSLCFG="seclevel",2,2
AT+QSSLCFG="sslversion",2,3
AT+QSSLCFG="ciphersuite",2,0XFFFF
AT+QSSLCFG="ignorelocaltime",2,1
```

6.3.2 Parametre MQTT využité pre testovanie protokolov

Pri testovaní protokolu MQTT boli ovplyvňované určité parametre s cieľom zistiť aký vplyv budú mať pri prenose MQTT správ, ktoré bolo realizované pomocou NB-IoT a LTE Cat-M.

Ovplyvňované parametre:

- **QoS 0,**
- **QoS 1,**
- **QoS 2,**
- **Použitie TLS.**

Celkovo prebehlo niekoľko testov, ktoré otestovali viacero faktorov, ktoré by mohli ovplyvniť úspešné doručenie. Na základe testov by malo byť možné určiť vhodné nastavenie protokolu MQTT a zároveň zistiť, za akých podmienok dokáže pracovať s technológiami LTE Cat-M a NB-IoT.

6.3.3 Výsledky testovaní a meraní pre NB-IoT

Pre prehľadné a jednoduché porovnanie rôznych nastavení parametrov sa výsledky testov a meraní nachádzajú v tabuľkách pod textom. Ich rozborom a vyhodnotením sa zaoberá nasledujúca podkapitola.

Tabuľka 6.1 obsahuje výsledky pri prihlásení bez overenie, s nastaveným východzím QOS 0.

Tab. 6.1: Tabuľka testov bez nastavenia akýchkoľvek parametrov.

RSRP [dBm]	**SINR [dB]**	**ECL**	**Priemerná odozva [ms]**	**Počet MQTT správ**	**Počet retransmisií**	**Množstvo dát**
−100	18,92	0	769	52	0	8151
−110	13,00	0	879	52	0	8151
−115	9,76	1	1014	52	0	8151
−125	−0,28	2	1207	52	0	8151

Tabuľka 6.2 obsahuje výsledky pri prihlásení bez overenie, s nastavený QOS 1.

Tab. 6.2: Tabuľka testov s QOS 1.

RSRP [dBm]	**SINR [dB]**	**ECL**	**Priemerná odozva [ms]**	**Počet MQTT správ**	**Počet retransmisií**	**Množstvo dát**
−100	16,60	0	1063	52	0	8151
−110	14,60	0	1090	52	0	8151
−115	11,53	1	1173	52	0	8151
−125	1,85	2	1200	52	0	8151

Tabuľka 6.3 obsahuje výsledky pri prihlásení bez overenie, s nastavený QOS 2.

Tab. 6.3: Tabuľka testov s QOS 2.

RSRP [dBm]	**SINR [dB]**	**ECL**	**Priemerná odozva [ms]**	**Počet MQTT správ**	**Počet retransmisií**	**Množstvo dát**
−100	19,40	0	844	52	0	7531
−110	12,53	0	1199	52	0	7669
−115	8,24	1	1165	52	0	7669
−125	2,45	2	1262	52	2	10477

Tabuľka 6.2 obsahuje výsledky pri prihlásení s overením na základe certifikátov, s použitím šifrovania TLS 1.2, s nastaveným východzím QOS 0.

Tab. 6.4: Tabuľka testov s TLS.

RSRP [dBm]	**SINR [dB]**	**ECL**	**Priemerná odozva [ms]**	**Počet retransmisií**	**Množstvo dát**
−100	19,20	0	903	0	9948
−110	14,90	0	1027	0	9948
−115	9,93	1	1282	1	10038
−125	2,45	2	1307	1	10038

6.3.4 Výsledky testovaní a meraní pre LTE Cat-M

Tabuľka 6.5 obsahuje výsledky pri prihlásení bez overenie, s nastaveným východzím QOS 0.

Tab. 6.5: Tabuľka testov bez nastavenia akýchkoľvek parametrov.

RSRP [dBm]	**SINR [dB]**	**Priemerná odozva [ms]**	**Počet MQTT správ**	**Počet retransmisií**	**Množstvo dát**
−90	27,36	269	52	0	8151
−100	22,48	282	52	0	8151
−110	12,8	299	52	0	8151
−115	10,7	535	52	0	8151
−120	7,22	894	52	0	8151
−125	1,04	987	52	0	8151

Tabuľka 6.6 obsahuje výsledky pri prihlásení bez overenie, s nastavený QOS 1.

Tab. 6.6: Tabuľka testov s QOS 1.

RSRP [dBm]	**SINR [dB]**	**Priemerná odozva [ms]**	**Počet MQTT správ**	**Počet retransmisií**	**Množstvo dát**
−90	25,42	237	102	0	11750
−100	20,86	252	102	0	11750
−110	12,40	300	102	0	11750
−115	11,10	303	102	0	11750
−120	6,84	443	102	0	11750
−125	1,48	966	102	1	11820

Tabuľka 6.7 obsahuje výsledky pri prihlásení bez overenie, s nastavený QOS 2.

Tab. 6.7: Tabuľka testov s QOS 2.

RSRP [dBm]	**SINR [dB]**	**Priemerná odozva [ms]**	**Počet MQTT správ**	**Počet retransmisií**	**Množstvo dát**
−90	17,30	277	202	0	11374
−100	15,33	295	202	0	11374
−110	11,28	308	202	0	11374
−115	7,14	337	202	0	11374
−120	4,84	419	202	0	11374
−125	−0, 28	1111	202	0	11374

Tabuľka 6.2 obsahuje výsledky pri prihlásení s overením na základe certifikátov, s použitím šifrovania TLS 1.2, s nastaveným východzím QOS 0.

Tab. 6.8: Tabuľka testov s TLS.

RSRP [dBm]	**SINR [dB]**	**Priemerná odozva [ms]**	**Počet retransmisií**	**Množstvo dát**
−90	22,33	299	0	10732
−100	20,22	310	0	10959
−110	14,33	368	0	11127
−115	15,00	363	0	10995
−120	12,33	613	0	10863
−125	3,28	1149	8	29714

6.3.5 Vyhodnotenie

Pri pohľade na tabuľky 6.1 až 6.4, ktoré sa týkajú prenosu MQTT protokolu pomocou NB-IoT, môžeme pozorovať, že hodnoty odozvy sa v priemere pohybujú okolo 1200 ms.

Pri LTE Cat-M je možné konštatovať, že pri každej sérii meraní sa priemerná odozva pri odosielaní správ na MQTT server zvyšovala. Pri hodnote RSRP -125 dBm dosahovala hranicu jednej sekundy, čo nie je práve najlepšia hodnota. Oproti hodnote RSRP -90 dBm, čo je typická hodnota nameraná v mestskom prostredí, bola hodnota odozvy priemerne až štyrikrát nižšia. Je potrebné konštatovať, že RSRP -125 dBm sa v meraní ukázala ako hraničná hodnota pri nastavenom útlme. V prípade nastavenia väčšieho útlmu bolo spojenie nestabilné. Hodnota RSRP -125 dBm je priemerom hodnôt pri meraní. RSRP pri snahe dosiahnuť RSRP -125 dBm kolísalo, ale slúži ako dobrá ukážka hraničných rádiových podmienok pre obe technológie.

Celkovo najnižšie oneskorenie mal protokol MQTT v prípade, keď neboli nastavené žiadne parametre pri prenose, klient sa prihlasoval k serveru bez akéhokoľvek overenia a nemal nastavenú žiadnu možnosť QOS. Toto bolo aj očakávané, keďže v takomto prípade je potrebné odoslať len minimum dát a paketov.

Pri nastavení QOS na hodnotu 1 alebo 2 v kombinácii s NB-IoT sa odozva zvýšila oproti použitiu QOS 0 v prvej sérii testov. Pri rovnakých nastaveniach QOS 1 alebo 2 je možné pozorovať, že latencia stúpala menším tempom ako v prípade

NB-IoT, a v prípadoch dobrých signálových podmienok stúpala v priemere o 20 ms so stúpajúcim útlmom signálu.

Parametrom protokolu MQTT, ktorý mal za následok najväčšie zvýšenie priemernej odozvy, bolo použitie šifrovania pomocou protokolu TLS, konkrétne verzia TLS 1.2. Použitie tejto verzie bolo nutné z dôvodu nepodpory aktuálnej verzie TLS 1.3 samotným komunikačným modulom, ktorá je oproti verzii 1.2 o niečo rýchlejšia.

Celkovo bolo pre výpočet každej priemernej hodnoty odozvy vykonaných väčšie množstvo meraní, a to z dôvodu väčšieho počtu hodnôt pre výpočet priemernej odchýlky. To sa ukázalo ako vhodný spôsob, pretože v niektorých prípadoch bola hodnota odozvy pri odosielaní dvakrát, vo výnimočných prípadoch až trikrát vyššia. Faktory, ktoré mohli ovplyvniť jednotlivé vyššie hodnoty, mohli byť rôzne. Na jednej strane odosielania sa nachádzal malý počítač Raspberry Pi, ktorý, rovnako ako technológie NB-IoT a LTE Cat-M, je navrhnutý pre malé rozmery a nízku cenu. Z tohto dôvodu nemá najvyšší výpočtový výkon, čo mohlo v občasných prípadoch spôsobiť vyššiu odozvu. Taktiež osobný počítač, na ktorom bežali servery aj samotné zachytávanie dát pomocou programu Wireshark, sa nemôže rovnať výkonu serverového hardvéru. Na počítači bola navyše zachytávaná sieťová prevádzka nielen z komunikácie medzi modulom a serverom, ale aj bežná sieťová prevádzka z iných aplikácií bežiacich na danom počítači.

Hodnoty oneskorení sa však medzi jednotlivými meraniami nedajú porovnávať na 100 %, keďže hodnotu RSRP bolo možné nastaviť pomocou útlmu, avšak hodnota SINR sa v niektorých prípadoch odlišovala. Tieto odchýlky mohol spôsobiť čas, v ktorom boli jednotlivé merania vykonávané, keďže RRU typicky prispôsobuje svoj vysielací výkon na základe času a taktiež na základe dňa v týždni.

6.4 Testovanie protokolu LWM2M

Celkovo prebehlo niekoľko testov na otestovanie viacerých faktorov, ktoré by mohli ovplyvniť úspešné doručenie. Na základe testov by malo byť možné určiť vhodné nastavenie protokolu LWM2M a zároveň zistiť, za akých podmienok je ideálne pre fungovanie s technológiami LTE Cat-M a NB-IoT. Ako server pre aplikačný protokol boli testované dve varianty:

- **Thingsboard Cloud** - je cloudová platforma, ktorá implementuje viaceré protokoly. Je navrhnutá na relatívne jednoduché pridávanie zariadení pripojených práve cez rôzne protokoly ako MQTT, LWM2M a ďalšie. Taktiež dovoľuje pre-

pojenie s inými platformami. Avšak pre potreby testovania bola nevyhovujúca. Nevýhodou je aj nutnosť platenia mesačného predplatného.

- **Eclipse Leshan** - je open source serverová implementácia pre protokol LWM2M a samotný Thingsboard ho implementuje vo svojej platforme. Výhodou je možnosť spustiť ho lokálne na vlastnom hardvéri a upravovať nastavenia podľa potrieb.

Použitý bol server Eclipse Leshan. Pre jeho spustenie je potrebné stiahnuť zdrojový kód z GitHub stránok a následne ho skompilovať. Leshan je naprogramovaný v jazyku JAVA. Z tohto dôvodu je v počítači potrebné mať nainštalovanú JAVU verzie 8 a vyššiu. Následne je možné spustiť server ako službu alebo pomocou PowerShellu pre podrobný výpis informácií.

Následne pre automatizáciu odosielania update správ na LWM2M server boli využitý skript napísaný v jazyku Python. Ktorý zabezpečil synchronizáciu času voči NTP serveru a taktiež pred každým z testov nové pripojenie k LWM2M serveru. Pomocou skriptu bolo aj zachytávané časové razítko odoslania správy.

6.4.1 Použité AT príkazy

```
Príkazy pre prihlásenie klienta k serveru

AT+QLWCFG="security",1,1,lwm2\_server,0,3
AT+QLWCFG="epns",0,NB-IoT,NB-IoT
AT+QLWSVC="reg"

Príkazy pre odoslanie správy

AT+QLWCFG="device","Quectel","BG77","","04",
"BG77LAR02A04","Quectel\_BG77"

Príkazy pre odhlásenie klienta z serveru

AT+QLWSVC="dereg",1
```

6.4.2 Výsledky testovaní a meraní pre NB-IoT

Tab. 6.9: Tabuľka testov bez nastavenia akýchkoľvek parametrov.

RSRP [dBm]	**SINR [dB]**	**ECL**	**Priemerná odozva [ms]**	**Počet retransmisií**
−100	19,6	0	615	0
−110	16,6	0	649	0
−115	9,7	1	825	0
−125	5,45	2	876	0

6.4.3 Výsledky testovaní a meraní pre LTE Cat-M

Tab. 6.10: Tabuľka testov bez nastavenia akýchkoľvek parametrov.

RSRP [dBm]	**SINR [dB]**	**Priemerná odozva [ms]**	**Počet retransmisií**
−90	27.87	92	0
−100	19.2	127	0
−110	8.2	140	0
−115	8,0	224	0
−125	2	504	0

6.4.4 Vyhodnotenie

V porovnaní s MQTT vykazuje LwM2M využívajúci protokol CoAP nižšiu latenciu pri rovnakých podmienkach, čo z neho robí vhodnejšiu voľbu pre aplikácie vyžadujúce nižšiu odozvu. Hlavným rozdielom je použitie iných transportných protokolov. MQTT využíva TCP, zatiaľ čo LwM2M/CoAP používa UDP. Okrem nižšej latencie ponúka LwM2M aj lepšiu stabilitu spojenia a efektívnejšie spracovanie dát, čo prispieva k jeho vyššej celkovej efektivite prenosu v prostrediach s hraničnými rádiovými podmienkami. Bolo by však vhodné porovnať tieto dva protokoly aj v prípade, že

oba šifrujú svoj prenos. Takéto porovnanie by umožnilo lepšie zhodnotiť výhodnosť LwM2M/CoAP v porovnaní s MQTT, keďže šifrovanie môže mať výrazný vplyv na latenciu a celkový výkon prenosu dát.

6.5 Metodika testovania protokolu SSH

Metodika testovania protokolu SSH sa oproti predošlým testom s protokolmi odlišuje. Testovací scenár je upravený tak, že počítač so serverom Windows zostáva, avšak bolo do neho nainštalované rozšírenie systému umožňujúce pripojenie pomocou OpenSSH servera. Pripojenie k sieti pomocou technológií NB-IoT a LTE Cat-M zostalo rovnaké. Zmenilo sa len zariadenie pripojené ku komunikačnému modulu. Pre potreby týchto testov bol využitý notebook s operačným systémom Windows. Táto zmena nastala z dôvodu využitia komunikačného modulu v inom režime. V tomto prípade bolo medzi notebookom a modulom vytvorené vytáčané pripojenie pomocou protokolu PPP, ktoré dovoľuje notebooku využiť modul ako modem pre pripojenie do internetu.

Z dôvodu nastaveného APN je prístup obmedzený iba na IP adresy nastavené na whiteliste. Avšak to nezabránilo systému posielať zbytočnú sieťovú prevádzku, ktorá zbytočne zaťažuje prenosový kanál a skresľuje výsledné hodnoty. Z tohto dôvodu bolo potrebné zmeniť smerovaciu tabuľku tak, aby smerovala iba pakety potrebné pre meranie. Pre výpis smerovacej tabuľky na operačnom systéme Windows sa používa príkaz *>route print*. Pre odstránenie defaultnej cesty je možné použiť príkaz *>route DELETE 0.0.0.0 0.0.0.0*. Následne bolo nutné pridať jednu novú statickú cestu, príkazom *>route ADD IP adresa serveru 255.255.255.255 IP adresa modulu*. Tá smeruje na počítač, kde sa nachádza SSH server.

Následne bolo z notebooku realizované pripojenie k SSH serveru pomocou aplikácie Putty. Pre testovanie prenosu súboru cez SSH je využívaný protokol SCP (Secure File Copy). Ten je založený na protokole SSH a je najčastejšie používaný pre prenos súborov v kombinácii s SSH. Pre potreby testovania bol využitý program PSFTP, spúšťaný pomocou príkazového riadku. V prípade oboch technológií bol posielaný jeden textový súbor. Súbor obsahoval skript na testovanie protokolu MQTT. Jeho veľkosť bola 2164 bajtov. Pri LTE Cat-M bol prenášaný aj ďalší súbor v podobe MP3 súboru s veľkosťou 3498696 bajtov.

Počas celého merania prebiehalo zachytávanie pomocou programu Wireshark pre zachytenie prípadných strát pri prenose. Pre odfiltrovanie pre meranie potrebných paketov bol využitý filter *ip.addr == 46.0.0.0/8*. Nebola špecifikovaná iba jedna adresa, keďže adresa modulu sa dynamicky mení pri každom novom pripojení k sieti.

6.6 Testovanie protokolu SSH

Pri testovaní protokolu bola pozornosť zameraná na subjektívne porovnanie oneskorenia oproti bežnému pripojeniu cez Ethernet alebo Wi-Fi. Boli sledované dve hodnoty času, ktoré majú vplyv na používateľskú prívetivosť používania vzdialeného prístupu k terminálu zariadenia pomocou SSH.

Keďže v takomto prípade je najčastejšie využívaná textová interakcia s terminálom, prvou a najciteľnejšou hodnotou pre používateľa je čas, za aký je zobrazený/interpretovaný vstup klávesnice na terminále. Hodnota času zobrazenia vstupu bola meraná orientačne, keďže ide len o niekoľkosekundové intervaly, pri ktorých by presná hodnota bola obtiažne merateľná a výsledné hodnoty by nevypovedali viac ako približná hodnota a subjektívny pocit z používania používateľa.

Druhou meranou hodnotou bol čas, za ktorý sa zobrazí výpis súborov v jednom priečinku na SSH serveri. Tieto dve sledované hodnoty sú jedny z najpodstatnejších pri využívaní protokolu a majú ohromný vplyv na celkovú používateľskú spokojnosť pri prístupe na vzdialený terminál cez SSH.

Ďalej bol sledovaný čas, za ktorý sa prenesú súbory. Poslednými sledovanými hodnotami boli celková stratovosť prenosu, ktorá môže nastať pri vyšších útlmoch, vyšších hodnotách RSRP a SINR, a taktiež aj celkové množstvo prenesených dát.

6.6.1 Výsledky testovaní a meraní pre NB-IoT

Tab. 6.11: Tabuľka oneskorenia pri rôznych intenzitách signálu.

RSRP [dBm]	**SINR [dB]**	**ECL**	**Oneskorenie písania [s]**	**Oneskorenie výpisu [s]**	**Doba prenosu [s]**
−100	16,4	0	2	8	10
−110	15,4	0	3	14	17
−115	15,0	1	3	38	25
−120	3,8	2	4	40	30
−123	1,4	2	4	46	36

6.6.2 Výsledky testovaní a meraní pre LTE Cat-M

Tab. 6.12: Tabuľka oneskorenia pri rôznych intenzitách signálu.

RSRP [dBm]	**SINR [dB]**	**Oneskorenie písania [s]**	**Oneskorenie výpisu [s]**	**Doba prenosu [s]**	**Doba prenosu [s]**
−90	20,1	>1	>1	2,40	102,30
−100	18,4	1	1,15	2,47	104,28
−110	16,6	2	1,25	2,57	106,46
−115	10,2	2	1,46	2,93	107,13
−120	7,4	2	2,07	3,30	110,33
−125	1,2	3	2,33	4,26	127,94
−130	−8, 6	5	10,24	43,83	1019,43

6.6.3 Vyhodnotenie

Keďže testovanie a meranie časových hodnôt v prípade rýchlosti výpisu bolo skôr subjektívne a má len približne ukázať, ako sa tieto hodnoty menia pri rôznych intenzitách signálu, bude aj vyhodnotenie len subjektívne a opísané z hľadiska komfortu a užívateľskej prívetivosti používania vzdialeného prístupu k terminálu cez protokol SSH.

NB-IoT

Pri použití technológie NB-IoT bolo aj pri optimálnych hodnotách RSRP zaznamenané väčšie oneskorenie v porovnaní s bežným pripojením cez ethernet. Celkovo je však použiteľnosť tohto riešenia stále v medziach akceptovateľnosti. V prípadoch, kde by bol použitý protokol SSH na prístup k určitému zariadeniu a využívaný len na malé zmeny v nastavení alebo parametru kódu, je táto technológia aplikovateľná. Hoci to nie je ideálne riešenie, stále je to použiteľné. Avšak treba zohľadniť aj to, že v prípadoch s vyššími hodnotami RSRP by sa práca v terminály výrazne predĺžila.

Taktiež v prípadoch, kde zariadenie slúži napríklad ako senzor a je potrebné odoslať nový upravený program pre zber dát, je rýchlosť, akou by sa program dostal na zariadenie, dostatočná. Avšak, pri odosielaní väčších súborov by už časová náročnosť dosahovala niekoľko desiatok minút, čo už nie je úplne vhodné.

LTE Cat-M

Oproti NB-IoT je použitie protokolu SSH s pripojením cez LTE Cat-M o poznanie lepšie. Celkový dojem pri používaní je na dobrej úrovni a v porovnaní s pripojením cez ethernet len o niečo menej komfortný. Čas výpisu, či už pri zadaní príkazu alebo výpise súborov, bol na dobrej úrovni. Iba v prípade RSRP -130 dBm, čo už je hraničná úroveň, dosahoval podobné hodnoty ako v prípade použitia NB-IoT.

Doba prenosu súborov sa pri rôznych intenzitách signálu zvyšovala, avšak iba v jednotkách sekúnd. Takže v prípadoch použitia, kedy sa zariadenie nachádza v miestach s relatívne dobrou intenzitou signálu, je použitie protokolu SSH vhodné. V prípadoch, kedy by sa zariadenie nachádzalo v hraničných podmienkach pre pripojenie k sieti, sa oneskorenie niekoľkonásobne zvýšilo a nejedná sa teda o vhodný prípad využitia protokolu SSH.

Takisto sa aj čas na prenos súborov menil iba minimálne, v rádoch sekúnd. A je teda možné konštatovať, že použitie protokolu SSH spolu s protokolom SCP je vhodné aj na prenos väčších súborov, napríklad ako sú nový firmvér pre komunikačný modul. Avšak rovnako pri hraničných hodnotách signálu sa čas prenosu zvýšil niekoľkonásobne.

6.7 Porovnanie intenzity signálu pri rôznych hodnotách útlmu

Pre lepšie porovnanie oboch technológií, ktoré podporuje komunikačný modul BG77, je vhodné porovnať intenzity signálu pri rovnakých hodnotách nastaveného útlmu. To umožní presne určiť, ako sa každá technológia správa v rovnakých podmienkach a aký vplyv má útlm na kvalitu signálu a spoľahlivosť prenosu dát.

Merania intenzity signálu sú vykonávané pri rôznych úrovniach útlmu, aby sa mohlo sledovať, ako sa signál mení v závislosti od týchto hodnôt. Použitím rôznych úrovní útlmu sa dokážu simulovať rôzne prostredia a podmienky, v ktorých sa zariadenia môžu nachádzať.

Tab. 6.13: Tabuľka testov so šifrovaním DTLS.

	LTE Cat-M1		**LTE Cat-NB1**	
Útlm [dB]	**RSRP [dBm]**	**SINR [dB]**	**RSRP [dBm]**	**SINR [dB]**
5	−101	22,08	−91	21,8
10	−106	16,92	−96	16,64
15	−111	12,92	−100	15,4
20	−116	9,72	−106	15,4
25	−122	4,48	−111	11,6
30	−126	0,44	−115	10,4
35	−131	-3,6	−120	5,4

Porovnanie výsledkov z Tabuľky 6.1 pre LTE Cat-M1 a LTE Cat-NB1 ukazuje rozdiely v citlivosti na útlm a kvalitu signálu. Pri LTE Cat-M1 sa hodnota RSRP zhoršuje od -101 dBm pri útlme -5 dB až po -131 dBm pri útlme -35 dB. Toto naznačuje vysokú citlivosť LTE Cat-M1 na útlm, pričom signál sa rýchlo zhoršuje so zvyšujúcim sa útlmom. Na druhej strane, pri LTE Cat-NB1 sa hodnota RSRP tiež zhoršuje, avšak v menšom rozsahu, od -91 dBm pri útlme -5 dB po -120 dBm pri útlme -35 dB.

Podobne sa hodnota SINR pri LTE Cat-M1 znižuje so zvyšujúcim sa útlmom, od 22,08 dB pri útlme -5 dB po -3,6 dB pri útlme -35 dB. To naznačuje, že interferencie a šum výrazne ovplyvňujú kvalitu signálu pri vyšších útlmoch. LTE Cat-NB1 vykazuje menšie zhoršenie hodnôt SINR, ktoré klesajú z 21,8 dB pri útlme -5 dB na 5,4 dB pri útlme -35 dB. Tento rozdiel ukazuje, že LTE Cat-NB1 je odolnejšie voči interferenciám a šumu a vykazuje lepšiu stabilitu signálu v podmienkach vyššieho útlmu.

Z týchto výsledkov vyplýva, že LTE Cat-M1 je viac citlivé na útlm, čo vedie k výraznejšiemu zhoršeniu kvality signálu. LTE Cat-NB1, naopak, vykazuje lepšiu odolnosť a stabilitu signálu, čo ho robí vhodnejším pre aplikácie a prostredia s vyššou pravdepodobnosťou útlmu. Táto analýza poskytuje cenné informácie pre rozhodovanie o nasadení rôznych LTE technológií v závislosti od podmienok prenosu.

6.8 Celkové vyhodnotenie

Použitie technológií NB-IoT a LTE Cat-M na pripojenie cez SSH má svoje výhody a nevýhody. NB-IoT je vhodné pre aplikácie s nízkou prenosovou rýchlosťou a menším objemom dát, zatiaľ čo LTE Cat-M ponúka lepší užívateľský komfort a rýchlejšiu odozvu. Pre aplikácie vyžadujúce prenos väčších súborov je LTE Cat-M výhodnejšie, pokiaľ je k dispozícii dobrý signál. V oblastiach s hraničným signálom však môže byť čas prenosu súborov výrazne dlhší, čo treba zohľadniť pri výbere technológie.

Cieľom meraní nebolo dosahovať čo najmenších možných hodnôt pri použití technológii NB-IoT a LTE Cat-M. Cieľom bolo ukázať, ako sa hodnota odozvy mení pri rôznych signálových prostrediach pri LTE Cat-M od RSRP -90, typická nameraná hodnota v prostredí mesta až po málo osídlené miesta, typicky vzdialené niekoľko kilometrov od najbližšej vysielacej stanice, poprípade o miesta vo vnútri budov, kde sú hodnoty RSRP a SINR porovnateľné. Rovnako to bolo aj v prípade NB-IoT, cieľom nebolo odmerať čo najnižšie oneskorenie skôr poukázať akým spôsobom dochádza k jeho zvyšovaniu pri typicky dosiahnutých hodnotách RSRP a SINR v rôznych prostrediach s rôznymi podmienkami útlmu signálu.

Aj z tohto dôvodu nebol čas, pri odoslaní nebol zaznamenaný po odoslaní správy modulom, ale v moment kedy program odoslal príkaz na odoslanie. Táto metóda bola zvolená, z toho dôvodu aby bolo možné poukázať, nie len na oneskorenie vzniknuté pri samotnom prenose skrz sieť NB-IoT a LTE Cat-M, ale taktiež aj samotný čas, za ktorý komunikačný modul spracuje požiadavok a odošle ho. Keďže NB-IoT a LTE Cat-M sú primárne navrhnuté pre malé, nekomplexné, málo výkonné s cieľom minimalizovať cenu zariadenia, bolo vhodné zahnúť aj toto oneskorenie do celkového oneskorenia pri odosielaní. V celkovom dôsledku obe technológie nie sú navrhnuté pre pripojenia s nízkou latenciou. Pre tieto potreby už dnes existujú lepšie, avšak oproti NB-IoT a LTE Cat-M, komplexnejšie avšak drahšie technológie uvedené skupinou 3GPP spolu s 5G.

Záver

Cieľom tejto diplomovej práce bolo uskutočniť rozbor a analýzu dvoch relatívne nových, ale stále málo implementovaných technológií NB-IoT a LTE Cat-M, pričom bola pozornosť zameraná na protokoly využívané pri prenose potrebných dát z IoT zariadení. Ich rozborom a analýzou nastavení sa dospelo k odporúčaniam pre ich použitie.

PPráca sa začína teoretickým úvodom do konceptu internetu vecí, aby bol každý čitateľ uvedený do problematiky a mohol lepšie pochopiť kontext a aplikácie technológií NB-IoT a LTE Cat-M, ktoré sú kľúčovou súčasťou kategórie mobilného IoT. V teoretickej časti boli podrobne predstavené a rozobrané aktuálne využívané technológie podľa požiadaviek IoT, vrátane vlastností a vylepšení technológií NB-IoT a LTE Cat-M, ako sú definované v 3GPP vydaniach 13 až 16. Táto časť práce tiež poskytuje prehľad o budúcom vývoji týchto technológií spolu s 5G a novou technológiou NR-RedCap.

Keďže vydania od 3GPP sú pomerne rozsiahle a nie všetky vylepšenia a možnosti využitia pri technológiách LTE Cat-M a NB-IoT sú skutočne nasadzované výrobcami hardvéru a mobilnými operátormi, boli v práci uvedené odporúčania pre lepšiu orientáciu v možnostiach, ktoré obe technológie ponúkajú v praxi. Práca tiež uvádza perspektívne vylepšenia, s ktorými sa počíta do budúcnosti. Práca nadväzuje na teoretický rozbor viacerých prenosových protokolov, najčastejšie využívaných práve pre potreby IoT. Poslednou teoretickou časťou bol opis IoT platforiem, ktoré sú čoraz viac využívané pre ich jednoduchosť a možnosť implantácie vlastných aplikácií.

Praktická časť je zameraná na mnohé série testovaní troch významných protokolov v oblasti IoT, a to konkrétne protokolu MQTT, LWM2M a SSH. Kde hlavným bodom pozornosti je odozva. Avšak na odozvu sa nepozerá len z hľadiska protokolov samotných, ale aj na ich správanie pri použití NB-IoT a LTE Cat-M a to v rôznych rádiových a signálových podmienkach. Docielené tak bolo sériami automatizovaných testov, s využitím vlastných skriptov a aj manuálnym testovaním a subjektívnym pohľadom. Pre merania je použitý pomerne rozšírený komunikačný modul od firmy Quectel BG77. Na základe výsledkov meraní a testov je možné povedať, že rôzne nastavenie parametrov vplýva na odozvu pri prenose. Pri technológii LTE Cat-M bolo možné pozorovať výrazné zvyšovanie odozvy v hraničných rádiových podmienkach s vysokým útlmom signálu. Na rozdiel od NB-IoT, kde aj pri dobrých podmienkach boli hodnoty odozvy násobne vyššie, avšak nedochádzalo tu ku tak výrazným skokom. Pre tieto aj iné dôvody si každá z technológií nájde svoje uplatnenie v odlišných

aplikáciách. Pre tieto aj iné dôvody je každá z technológii nájde svoje uplatnenie v odlišných aplikáciach.

Celkovým zhrnutím by bolo vhodné konštatovať, že táto práca neposkytuje len praktické odporúčania pre konfiguráciu a použitie komunikačných protokolov v rámci technológií NB-IoT a LTE Cat-M, ale aj konfiguráciu technológií samotných. Vďaka čomu môže prispieť k ich lepšiemu porozumeniu a efektívnejšiemu využitiu týchto technológií v dynamicky sa rozvíjajúcom sektore IoT.

Literatúra

[1] GILLIS, Alexander S. Internet of Things (IoT). Online. In: TechTarget. August, 2023. Dostupné z: https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT. [cit. 2023-12-09].

[2] Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions) [Graph]. Online. In: FORBES. Dostupné z: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.[cit. 2023-11-05].

[3] What is Cellular IoT (Internet of Things)? Online. In: BERNADOU, Belén. September, 2023. Dostupné z: https://freeeway.com/what-is-cellular-iot-internet-of-things/. [cit. 2023-11-06].

[4] LIBERG, O.; SUNDBERG, M.; WANG, Y.; BERGMAN, J. a SACHS, J. Cellular Internet of Things: Technologies, Standards, and Performance. Academic Press, 2018. ISBN 978-0-12-812458-1. [cit. 2024-10-05].

[5] HAILEMARIAM MOGES, Teshager; SHUMEYE LAKEW, Demeke; PHI NGUYEN, Ngoc; DAO, Nhu-Ngoc a CHO, Sungrae. Cellular Internet of Things: Use cases, technologies, and future work. Online. Internet of Things. 2023, č. 24, s. 100910. ISSN 2542-6605. Dostupné z: https://doi.org/10.1016/j.iot.2023.100910. [cit. 2024-03-13].

[6] ERICSSON. IoT connectivity. Online. Dostupné z: https://www.ericsson.com/en/internet-of-things/iot-connectivity.[cit. 2024-05-05].

[7] KUHLINS, Christian; RATHONYI, Bela; ZAIDI, Ali a HOGAN, Marie. Cellular networks for Massive IoT. Online. 2020. Dostupné také z: https://www.ericsson.com/4ac671/assets/local/reports-papers/white-papers/massive_iot_whitepaper.pdf. [cit. 2023-12-12].

[8] About: Introducing 3GPP. Online. In: 3GPP. Dostupné z: https://www.3gpp.org/about-us/introducing-3gpp. [cit. 2023-11-20].

[9] SCHLIENZ, J. a RADDINO, D. Narrowband Internet of Things: Whitepaper. Online. Rohde&Schwarz, 2016. Dostupné také z: https://cdn.rohde-schwarz.com.cn/pws/dl_downloads/dl_application/application_notes/1ma266/1MA266_0e_NB_IoT.pdf.[cit. 2024-04-10].

[10] Overview of 3GPP Release 14 Enhanced NB-IoT. Online. IEEE Network. 2017, č. 31, article 6, s. 16-22. Dostupné z: https://doi.org/10.1109/MNET.2017.1700082. [cit. 2024-03-18].

[11] MWAKWATA, Collins Burton; MALIK, Hassan a MAHTAB ALAM, Muhammad. Narrowband Internet of Things (NB-IoT): From Physical (PHY) and Media Access Control (MAC) Layers Perspectives. Online. Sensors. 19. 2019, roč. 11. ISSN 1424-8220. Dostupné z: https://www.mdpi.com/1424-8220/19/11/2613.[cit. 2024-05-11].

[12] MOZNY, Radek; MASEK, Pavel; STUSEK, Martin; ZEMAN, Krystof; OMETOV, Aleksandr et al. On the Performance of Narrow-band Internet of Things (NB-IoT) for Delay-tolerant Services. Online. 2019. Dostupné také z: https://trepo.tuni.fi//bitstream/handle/10024/129616/On_the_Performance_of_Narrow_band_Internet_of_Things_NB_IoT_for_Delay_tolerant_Services.pdf?sequence=1.[cit. 2024-04-10].

[13] Internet of Things (IoT): CableFree IoT – The Internet of Things. Online. In: CableFree. Dostupné z: https://www.cablefree.net/wirelesstechnology/internet-of-things-iot/. [cit. 2023-12-09].

[14] CHAUDHARI, Bharat S. a ZENNARO, Marco (ed.). LPWAN Technologies for IoT and M2M Applications. Academic Press, 2020. ISBN 978-0-12-818880-4. [cit. 2024-04-10].

[15] ZAYAS, Díaz; TOCADO, Almudena; TOCADO, Rivas; JAVIER, Francisco a RODRÍGUEZ, Francisco. Evolution and Testing of NB-IoT Solutions. Online. Applied Sciences. 2020, roč. 10, č. 21. Dostupné z: https://doi.org/10.3390/app10217903. [cit. 2024-03-19].

[16] RAPEEPAT, Ratasuk; MANGALVEDHE, Nitin; BHATOOLAUL, David a GHOSH, Amitava. LTE-M Evolution Towards 5G Massive MTC. Online. 2017 IEEE Globecom Workshops (GC Wkshps). 2017, s. 1-6. Dostupné z: https://doi.org/10.1109/GLOCOMW.2017.8269112. [cit. 2024-03-19].

[17] Mobile IoT Deployment Guide. Online. 2022. Dostupné také z: https://www.gsma.com/iot/resources/mobile-iot-deployment-guide/.[cit. 2024-04-10].

[18] FUJDIAK, Radek; MIKHAYLOVA, Konstantin; STUSEK, Martin a MASEK, Pavel. *Security in Low Power Wide Area Networks: State-of-the-Art and Development towards the 5G*. 2019. [cit. 2024-04-10].

[19] STUSEK, Martin; ZEMAN, Krystof; MASEK, Pavel; SEDOVA, Jindriska a HOSEK, Jiri. IoT Protocols for Low-power Massive IoT: A Communication Perspective. Online. In: 2019 11th International Congress on Ultra Modern

Telecommunications and Control Systems and Workshops (ICUMT). IEEE, 2019, s. 1-7. ISBN 978-1-7281-5764-1. Dostupné z: https://doi.org/10.1109/ICUMT48472.2019.8970868. [cit. 2023-11-23].

[20] BARRETT, Daniel J.; SILVERMAN, Richard E. a BYRNES, Robert G. SSH, The Secure Shell: The Definitive Guide. Druhé. Sebastopol: O'Reilly Media, 2005. ISBN 0-596-00895-3.[cit. 2024-04-10].

[21] HILLAR, Gastón C. MQTT Essentials - A Lightweight IoT Protocol. Online. Birmingham: Packt Publishing, 2017. ISBN 978-1-78728-781-5. [cit. 2023-11-20].

[22] Protokol MQTT: komunikační standard pro IoT. Online. In: MALÝ, Martin. Root.cz. Dostupné z: https://www.root.cz/clanky/protokol-mqtt-komunikacni-standard-pro-iot/. [cit. 2023-11-20].

[23] SHELBY, Z.; HARTKE, K. a BORMANN, C. The Constrained Application Protocol (CoAP),. 2014. Dostupné z: https://doi.org/10.17487/RFC7252.. [cit. 2023-11-29].

[24] JABLONCIK, Lukas; DVORAK, Radim; MIKULASEK, Michal; STUSEK, Martin; MASEK, Pavel et al. LWM2M for Cellular IoT: Protocol Implementation and Performance Evaluation. Online. [cit. 2023-12-10].

[25] Lightweight Machine to Machine Technical Specification: Open Mobile Alliance. Online. Dostupné také z: https://www.openmobilealliance.org/release/lightweightm2m/V1_0-20160407-C/OMA-TS-LightweightM2M-V1_0-20160407-C.pdf.[cit. 2024-04-10].

[26] LUCERO, Sam. IoT platforms: enabling the Internet of Things. Online. 2016. Dostupné také z: https://cdn.ihs.com/www/pdf/enabling-IOT.pdf.[cit. 2024-04-10].

[27] PARASKEVOPOULOS, Dimitris. The leading IoT software companies 2023. Online. In: IOT ANALYTICS. Dostupné z: https://iot-analytics.com/leading-iot-software-companies/.[cit. 2023-12-11].

Zoznam symbolov a skratiek

Skratky:

3GPP	The 3rd Generation Partnership Project
16QAM	Sixteen Quadrature Amplitude Modulation
ACB	Access Class Barring
ADC	Analog to Digital Converter
AES	Advanced Encryption Standard
API	Application Programming Interface
ARM	originally Acorn RISC Machine, later Advanced RISC Machine
AT	AT Command Set
BEST	Bandwidth Efficient Simple TDD
BSR	Buffer Status Report
C-DRX	Connected Mode Discontinuous Reception
C-eDRX	Connected Mode Extended Discontinuous Reception
CDM	Code Division Multiplexing
Cell ID	Cell Identifier
CIoT	Consumer Internet of Things
CMP	Certificate Management Protocol
CoAP	Constrained Application Protocol
CT	Circuit Switched/Telecommunications
DRX	Discontinuous Reception
DTLS	Datagram Transport Layer Security
EAB	Extended Access Barring
ECL	Coverage Enhancement Level

ECID	Enhanced Cell ID
EDT	Early Data Transmission
eDRX	Extended Discontinuous Reception
eMBB	enhanced Mobile Broadband
EIoT	Enterprise Internet of Things
eMTC	enhanced Machine Type Communication
eNodeB	Evolved Node B
EPS	Evolved Packet System
eUTRAN	Evolved Universal Terrestrial Radio Access Network
EARFCN	E-UTRA Absolute Radio Frequency Channel Number
FTP	File Transfer Protocol
FDD	Frequency Division Duplexing
GAN	Global Area Network
GPIO	General-Purpose Input/Output
GPRS	General Packet Radio Service
GSMA	Global System for Mobile Communications Association
GSM	Global System for Mobile Communications
GTP	GPRS Tunneling Protocol
HARQ	Hybrid Automatic Repeat reQuest
HARQ-ACK	Hybrid Automatic Repeat Request Acknowledgment
HD	Half-Duplex
HTTP	Hypertext Transfer Protocol
I2C	Inter-Integrated Circuit

ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IIoT	Industrial Internet of Things
IP	Internet Protocol
IPv6	Internet Protocol version 6
IoT	Internet of Things
LBS	Location-Based Services
LPWAN	Low-power Wide-area Network
LTE	Long Term Evolution
LTE Cat-M	LTE Category M for Machine-type Communication
LwM2M	Lightweight M2M
M2M	Machine to Machine Communication
MCL	Maximum Coupling Loss
MIB-NB	Master Information Block for NB-IoT
mini-PCIe	mini Peripheral Component Interconnect Express
MIMO	Multiple-input multiple-output
MQTT	Message Queuing Telemetry Transport
MU-MIMO	Multi-User, Multiple Input, Multiple Output
NAS	Non Access Stratus
NB-IoT	Narrowband Internet of Things
NIDD	Non-IP Data Delivery
NPBCH	Narrowband Physical Broadcast Channel
NPDSCH	Narrowband Physical Downlink Shared Channel

NPSS	Narrowband Primary Synchronization Signal
NSSS	Narrowband Secondary Synchronization Signal
NTP	Network Time Protocol
OFDMA	Orthogonal Frequency-Division Multiple Access
OMA	Open Mobile Alliance
OSCORE	Object Security for Constrained RESTful Environments
OTA	Over-The-Air
OTDOA	Observed Time Difference of Arrival
PC	Personal Computer
PCM	Pulse-Code Modulation
PING	Packet InterNet Groper
PPP	Point-to-Point Protocol
PRACH	Physical Random Access Channel
PSM	Power Saving Mode
PUR	Possibly Unicast Ranging
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RA	Random Access
RAI	Routing Area Identity
RAM	Random Access Memory
RAN	Radio Access Network
RAT	Radio Access Technology
RB	Resource Block

ROM	Read-Only Memory
RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
RSSI	Received Signal Strength Indicator
RRC	Radio Resource Control
RRC IDLE	Radio Resource Control IDLE
SCEF	Service Capability Exposure Function
SCP	Secure Copy Protocol
SC-FDMA	Single-Carrier Frequency-Division Multiple Access
SGW	Serving Gateway
SIM	Subscriber Identity Module
SINR	Signal to Interference Plus Noise Ratio
SFTP	Secure File Transfer Protocol
SMA	SubMiniature version A
SMS	Short Message Service
SSL	Secure Sockets Layer
SSH	Secure Shell
TA	Timing Advance
TAU	Tracking Area Update
TCP	Transmission Control Protocol
TDD	Time Division Duplexing
TLS	Transport Layer Security
TMSI	Temporary Mobile Subscriber Identity
TTI	Transmission Time Interval
UE	User Equipment

URI	Uniform Resource Identifier
UICC	Universal Integrated Circuit Card
USB	Universal Serial Bus
VoLTE	Voice over LTE
WUS	Wake-Up Signal
ZUC	ZUC Encryption Algorithm

Symboly:

B	Byte
dB	Decibel
dBm	Decibels relative to one milliwatt
GHz	Gigahertz
km	Kilometer
km/h	Kilometers per hour
kb/s	Kilobits per second
kHz	Kilohertz
Mb/s	Megabits per second
MHz	Megahertz
ms	Milliseconds
mW	Milliwatts
s	Seconds
%	Percent

A Obsah elektronickej prílohy

- `/` ..... koreňový adresár priloženého archívu
  - `skripty` ..... Použité skripty pre odosielanie správ.
    - `LTE_MQTT_QOS0.py`
    - `LTE_MQTT_QOS1.py`
    - `LTE_MQTT_QOS2.py`
    - `LTE_MQTT_TLS.py`
    - `LTE_LWM2M.py`
    - `NB_IOT_MQTT_QOS0.py`
    - `NB_IOT_MQTT_QOS1.py`
    - `NB_IOT_MQTT_QOS2.py`
    - `NB_IOT_MQTT_TLS.py`
    - `NB_IOT_LWM2M.py`
  - `skripty` ..... Použité skripty pre filtrovanie.
    - `QOS_filter.py`
    - `TLS_filter.py`
    - `LWM2M_filter.py`
    - `Filter.py`