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

NÁVRH A OVĚŘENÍ ŠIROKOPÁSMOVÉ BEZDRÁTOVÉ TECHNOLOGIE VYUŽÍVAJÍCÍ LONG-RANGE MODULACI

DESIGN AND EXPERIMENTAL VERIFICATION OF BROADBAND WIRELESS TECHNOLOGY USING LONG-RANGE MODULATION

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR
Ondřej Pospíšil

VEDOUCÍ PRÁCE
SUPERVISOR
Ing. Radek Fujdiak

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Teleinformatika**
Ústav telekomunikací

Student: Ondřej Pospíšil ***ID:*** 174382
Ročník: 3 ***Akademický rok:*** 2016/17

NÁZEV TÉMATU:

Návrh a ověření širokopásmové bezdrátové technologie využívající long-range modulaci

POKYNY PRO VYPRACOVÁNÍ:

Student vypracuje kvalitní základ pro problematiku a terminologii v rámci rádiových sítí (různé frekvence, modulace, šířka pásmo, potřebné licence, standardy, technologie, aj.). Blíže se pak zaměří na komunikační technologii Long-Range (WAN) a to i na využití různých cloudových možností (z cloudových možností bude vybrána jedna nejvhodnější, kterou student bude dále používat ve své síti). Teoretická část bude podložena značným množstvím kvalitní odborné literatury. V praktické části student sestaví a ověří komunikační síť Long-Range WAN za pomocí dodaných HW prvků (brány LORANK s vybranými koncovými prvky) a cloudu. V této síti následně proběhnou jednotlivá experimentální měření technologie a to i v různých prostředích – podzemí, vnitřní i venkovní prostory, aj. (s přihlédnutím na možnosti měření – tedy zpoždění, síla signálu, odstup signálu od šumu, aj.). Praktická měření budou teoreticky podložena např. výpočty max. síly signálu či simulacemi. Výstupem by měl být kvalitní teoretický základ, funkční síť, experimentální výsledky z měření prokazující vlastnosti technologie a příp. vybrané teoretické výpočty či simulace.

DOPORUČENÁ LITERATURA:

[1] LoRa Alliance. „NOTICE OF USE AND DISCLOSURE“. LoRa Specification, 2015.

[2] Orange. „LoRa Device Developer Guide“. Orange Connected Objects and Partnerships, 2016.

Termín zadání: 1.2.2017 ***Termín odevzdání:*** 8.6.2017

Vedoucí práce: Ing. Radek Fujdiak
Konzultant:

doc. Ing. Jiří Mišurec, CSc.
předseda oborové rady

ABSTRAKT

Bakalářská práce se zabývá využitím bezdrátové Low Power WAN technologie LoRaWAN v IoT. V práci je rozebrána jak fyzická vrstva, na které pracuje modulace LoRa, tak protokol LoRaWAN a jeho limity. V práci je navrhnuta a zrealizovaná síť na technologii LoRaWAN. Funkčnost této sítě je v reálném provozu ověřena v několika scénářích.

KLÍČOVÁ SLOVA

IoT, Low power, LPWAN, Long range, LoRa, LoRaWAN, Loriot

ABSTRACT

This bachelor thesis deals with the use of wireless Low Power WAN technology LoRaWAN in IoT. The thesis also describes both the physical layer on which the LoRa modulation works and the LoRaWAN protocol with its limits. The main goal of thesis was to design and realize network on LoRaWAN technology. The functionality of this network is verified in several scenarios in real traffic.

KEYWORDS

IoT, Low power, LPWAN, Long range, LoRa, LoRaWAN, Loriot

POSPÍŠIL, Ondřej *Návrh a ověření širokopásmové bezdrátové technologie využívající long-range modulaci*: semestrální projekt. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, Rok. 74 s. Vedoucí práce byl Ing. Radek Fujdiak

PROHLÁŠENÍ

Prohlašuji, že svůj semestrální projekt na téma „Návrh a ověření širokopásmové bezdrátové technologie využívající long-range modulaci“ jsem vypracoval(a) samostatně pod vedením vedoucího semestrálního projektu a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

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

Brno ....

podpis autora(-ky)

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu diplomové práce panu Ing. Radku Fujdiakovi za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci. Dále bych chtěl poděkovat rodičům za dlouhodobou podporu při studiu. Také bych chtěl poděkovat Janu Školařovi za pomoc při měření, Ondřeji Kopáčovi za kontrolu práce a Jaroslavu Hájkovi za podnětné rady.

Brno . . . .

podpis autora(-ky)

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

V dnešní době se stále více mluví o Internetu věcí (IoT) [1] v rámci usnadnění lidského života, každodenních činností a zefektivnění práce. Pro IoT se jeví jako jedna z velmi vhodných možností komunikace bezdrátová komunikace [2], a to hlavně z důvodů implementace do hotových staveb a objektů. Tento typ komunikace je vhodný pro senzorické měření v těžce dostupných místech. A zde ke slovu přichází Low Power WAN technologie, která právě v těchto těžce přístupných oblastech vydrží na jeden zdroj energie velmi dlouhou dobu (v rámci několika roků) bez zásahu člověka [3]. Nepředpokládá se, že by byla používána pouze jedna LPWAN technologie [4], ale více pro různé účely, jako je real-time provoz, nebo pouze přenos několika dat během dne.

Cílem práce je seznámení se s problematikou Low Power WAN sítí v rámci IoT, a to především s technologií LoRaWAN, která je v IoT využívána především pro sběr malého objemu dat v různých senzorech, u kterých je třeba přenést malý objem dat jen párkrát denně, nebo při kontrole stavu různých zařízení [5]. Dále analyzovat možnosti této technologie a porovnat její parametry s ostatními LPWAN technologiemi. Na této technologii je v práci navržena a sestavena vlastní síť. Je nutné analyzovat všechny části a prvky sítě a zvolit nejvhodnější použití. Poté je takto navržená síť testována s různými koncovými zařízeními v různých podmínkách a je testována provozuschopnost celé sítě.

Hlavním přínosem práce je rozbor technologie LoRaWAN a její proprietární modulace s rozprostřeným spektrem (Chirp Spread Spectrum) LoRa, popsání funkčnosti a zdůraznění limitů této technologie. Dále vlastní sestavení sítě za použití cloudu a testování provozu této sítě a její schopnosti v reálných podmínkách.

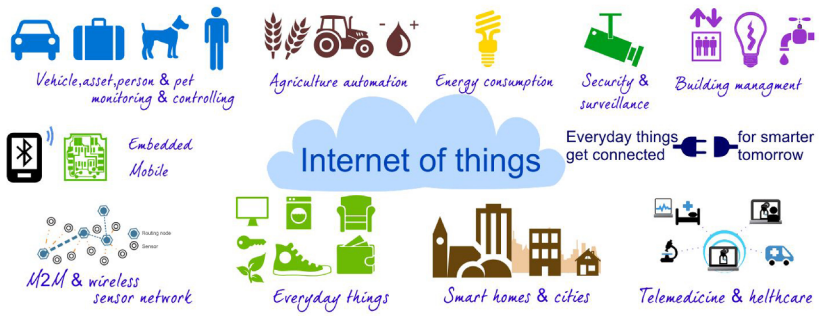
Práce je rozdělena do šesti částí. V první části je popsána problematika Internetu věcí z důvodu použití LPWAN technologií právě v této oblasti. V druhé části je vzhledem k použití bezdrátové technologie přiblížena více problematika radiových komunikací a začlenění LPWAN do této problematiky. Ve třetí části jsou popsány jednotlivé LPWAN technologie a jsou následně porovnány oproti LoRaWAN technologii. Čtvrtá část se detailně zabývá samotným protokolem LoRaWAN a jeho fyzickou vrstvou LoRa, jsou zde řešeny vlastnosti, limity a bezpečnost této technologie. Pátá část analyzuje zařízení této technologie a její síťové prvky, zde jsou zvoleny všechny důležité prvky pro realizaci sítě. Šestá část se zabývá samotným návrhem sítě, jejím zprovozněním a testováním v reálných podmínkách.

1 INTERNET OF THINGS

Česky Internet věcí je označení, které v sobě nese myšlenku propojení všedních věcí jako jsou myčky, pračky, světla, různé příslušenství jako kávovary, dále různé senzory a vlastně jakékoliv běžné každodenní zařízení. Komunikace je založena na standardizovaných komunikačních protokolech, které umožňují výměnu, sdílení dat a informací. Díky IoT můžeme komunikovat se stroji a stroje mohou komunikovat navzájem spolu (M2M komunikace) bez potřeby lidského zásahu. Jde tedy o sběr dat z různých zařízení a senzorů, která jsou sdílena, zpracována a poté vyhodnocena. Nejde zde tedy o běžnou komunikaci lidí, jak je tomu u internetu, ale o komunikaci zařízení mezi sebou bez lidského zásahu. Hlavním důvodem vzniku IoT je zefektivnění výroby a práce, ke zlepšení monitorování lidí v oblasti zdravotnictví, efektivní využití elektrické energie a také kvůli pohodlnosti lidí [1].

1.1 Využití

IoT má obrovské využití v mnoha oblastech jak je vidět na Obr. 1.1. Hlavní směry využití jsou průmyslový internet věcí a internet věcí pro spotřebitele. V těchto směrech se uvažuje nejvíce o chytrých domácnostech, kde je využití pro elektroniku v domácnosti a možnosti její měření (odběry energie). Dále použití v chytrých městech, zde je využití pro odpady, parkování, sledování provozu a kvality ovzduší. Dalším využitím je ve zdravotnictví takzvané eHealth, kde je využití pro vzdálené sledování zdraví. V neposlední řadě je zde využití i v zemědělství pro zjištění kvality půdy a nebo množství srážek. V IoT je mnoho směrů využití, zde byly shrnuty ty nejvíce diskutované v této době [2].



Obr. 1.1: Oblasti využití IoT [6].

Průmyslový Internet věcí

V rámci průmyslu 4.0 [7] se jedná o začlenění IoT do průmyslu energetického (Smart Grid), zdravotnictví, automatizace, zemědělství a další. V této oblasti jde hlavně o efektivnější využití zdrojů, zefektivnění výroby, snížení nákladů na provoz, monitorování provozu, a tím snížit riziko chyb a díky monitorování jim i předcházet což ušetří finance. Díky M2M komunikaci a následném zpracování v cloudu nebude třeba lidské síly a stroje budou komunikovat mezi sebou a budou si předávat informace o stavu, popřípadě samy zajistí chybějící komponenty. Toto je hlavní a důležitý směr pro vývoj IoT.

Smart city U chytrých měst je dnes hlavně zaměření na optimalizaci dopravy (provoz, parkování), sběr odpadu a také distribuce vody. Dále může řešit problémy s nadměrným hlukem, nebo také znečištění vzduchu [1].

Smart grids Takzvané chytré rozvodné sítě. Slouží ke zefektivnění dodávky energie a snížení její spotřeby. Zapojují daleko efektivněji obnovitelné zdroje do rozvodné sítě a je tak vyvážen a zefektivněn odběr energie. Pomocí automatizovaných odečtů energie dochází k dalšímu zefektivnění [8].

Zdravotnictví Chytré zdravotnictví umožňuje nepřetržité sledování životních funkcí jednotlivých osob. Doktor dostává informace o zdraví člověka v reálném čase - předcházení zdravotních komplikací [1].

Chytré zemědělství Pro zemědělství je IoT velice významné, a to z důvodů senzorů vlhkosti půdy (úspora na zavlažování), slunečního svitu, monitorování strojů, dále také hlídání objektů, zvířat a plodin. Díky datům získaných v této oblasti může v budoucnu docházet k velkému zefektivnění celého zemědělství [1].

Internet věcí pro spotřebitele

Tato oblast je zaměřena hlavně na domácnost a vlastní zařízení spotřebitele. Jde o zařízení jako pračky, myčky, kávovary, osvětlení, termostaty a jiné. Tyto zařízení v chytré domácnosti budou moct komunikovat s internetem, kde budou dostupny pro uživatele, a také komunikují spolu navzájem pro usnadnění požadavků spotřebitele. Tento směr je hlavně pro pohodlnost spotřebitele a pro usnadnění každodenních běžných věcí.

Chytré domy Jde o zautomatizování běžných věcí v domě a přizpůsobení místností jednotlivým obyvatelů. Jsou to věci jako intenzita světla v místnosti, hudba

v místnosti, spotřebič hlídající stav, například lednice hlídá zda je dostatek určité potraviny. Díky aplikaci v telefonu, nebo pomocí vlastního ovládacího panelu, lze celý dům ovládat (světla, teplo a další) [1].

Wearebles Takzvané nositelná elektronika a oblečení jako jsou chytré náramky, brýle nebo hodinky. Tyto zařízení dokáží měřit tep, kroky, usnadní komunikaci a jiné. Chytrým se stává i samotné oblečení, které v sobě má zabudované různé senzory [9].

1.2 Komunikační protokoly a standardy

Internet věcí pokrývá širokou škálu průmyslových odvětví. Zabývá se jak propojením jen jednotlivých malých zařízení, tak i masivním propojením v rámci obrovského množství zařízení napojených na cloud. K tomuto je potřeba zvolit správné protokoly pro komunikaci jednotlivých zařízení v rámci celé sítě. Současně vznikají různé organizace v naději, že sjednotí různé části IoT. Zde jsou představeny některé protokoly v rámci IoT a jsou rozděleny do několika vrstev pro lepší organizaci [10].

1.2.1 Struktura

Základem struktury IoT je senzor, ten je umístěn v zařízení, které chceme připojit do IoT. Senzory měří vlastní data (teplota a jiné) a digitalizují tyto data, většinou neprovádí žádné procesy, měly by mít malou spotřebu dat. Senzory mohou dále posílat data do lokální sítě a nebo, což nastává ve většině případů, jsou data posílána přímo do sítě na Gateway (data koncentrátor). Data jsou dále přenášena na síťový server cloudu, kde jsou zpracována, data jsou odesílány pomocí protokolů kompatibilních s IoT (HTTPS (Hypertext Transfer Protocol Secure), XMPP (Extensible Messaging and Presence Protocol), MQTT (MQ Telemetry Transport), CoAP (Constrained Application Protocol) a další) a jsou přenášena pomocí Ethernetu či LTE. Data po zpracování pokračují do cloudu, kde jsou již dostupné pro uživatele.

1.2.2 Protokoly

Infrastrukturní

Jsou to protokoly zajišťující komunikaci napříč infrastrukturou.

- **IPv6** (Internet Protocol version 6): Protokol pracující na síťové vrstvě ISO/OSI modelu a zajišťuje přepojování paketů v rámci této vrstvy podle IP adres.

- **6LoWPAN** (IPv6 over Low-Power Wireless Personal Area Networks): Protokol využívající IPv6 v osobních sítích (PAN) s nízkým výkonem pracující na bázi standardu IEEE 802.15.4[1].
- **UDP**(User datagram protocol): Protokol pracující na transportní vrstvě modelu ISO/OSI k přenosu datagramů v režimu klient - server. UDP protokol je nejčastěji používán pro real-time komunikace.
- **TSMP** (Time Synchronized Mesh Protocol): Komunikační protokol pro samoorganizaci sítě se senzorickými zařízeními. Zařízení jsou vzájemně synchronní a komunikují v časových úsecích.

Datové protokoly

Protokoly pro správu zařízení a pro přenesená data ze sítě na zařízení na aplikační vrstvě.

- **SSI** (Simple Sensor Interface): Jednoduchý aplikační protokol pro data přenesená mezi počítači nebo terminály mezi chytré senzory.
- **LWM2M** (Lightweight M2M): Je to protokol Open Mobile Alliance pro IoT neb M2M. Zajišťuje komunikaci na aplikační vrsvě mezi klientem a serverem. Je vytvořen ke správě senzorů, pro přenos dat ze sítě k zařízení, je rozšířený tak, aby vyhovoval požadavkům většiny aplikací.
- **SOAP** (Simple Object Access Protocol): JSON/XML, WebHooks, Jelastic, MongoDB.
- **HTTP/2** (Hypertext Transfer Protocol Version 2): Protokol pro výměnu hypertextových dokumentů (HTML). Umožňuje efektivnější využití síťových prostředků s nižším zpožděním a umožňuje více souběžných výměn dat na jednom spojení.
- **Websocket**: Definuje plně duplexní připojení s jedním soketem, přes které mohou být odesílány zprávy mezi klientem a serverem.
- **MQTT** (Message Queuing Telemetry Transport): Jde o jednoduchý a lehce implementovaný protokol od společnosti IBM. V IoT velmi používaný protokol pro zařízení s malou spotřebou energie.
- **CoAP** (Constrained Application Protocol): Využívaný především s protokolem UDP (není zaručen spolehlivý přenos). Je primárně využíván pro komunikaci jednoho zařízení s jedním. Je navržen tak, aby byl možný snadný překlad do protokolu HTTP.
- **XMPP** (Extensible Messaging and Presence Protocol): Jde o open-source protokol pro komunikaci v reálném čase. Využíván hlavně k instant messagingu. Pracuje jako klient-server.

[1] `http://standards.ieee.org/findstds/standard/802.15.4-2011.html`

Komunikační a přenosové protokoly

Protokoly které zaručují samotný přenos na úrovni linkové vrstvy.

- **Ethernet:** Standard IEEE 802.3 používající pro drátový přenos kabely s kroucenou dvojlinkou, optické kabely zvládající rychlost až stovky Gb/s.
- **NFC:**(Near field communication)- Radiová bezdrátová komunikace na velmi malé vzdálenosti (maximálně 4 cm) rychlost přenosu do 424 kb/s.
- **Bluetooth:** Pracuje na frekvenci 2.4 GHz bezlicenčního pásma na vzdálenost až 240 m s rychlostí až 50 Mb/s.
- **Wi-fi:** Standard IEEE 802.11 pro bezdrátovou komunikaci na frekvencích 2.4 a 5 GHz. Komunikace ve vzdálenosti jednotek kilometrů s rychlostí přenosu podle použitého typu IEEE 802.11.
- **LPWA:** Jde o komunikaci s nízkou spotřebou energie na velké vzdálenosti s malým objemem přenesených dat řadí se zde protokoly jako LoRaWAN, Sigfox, Weightless, NB-IoT atd...
- **Celulární technologie:** GPRS/2G/3G/4G/LTE

Bezpečnost

Protokoly pro zajištění bezpečnosti v IoT.

- **OTrP**(Open Trust Protocol) - Protokol k mazání, instalaci a updatu aplikací a ke správě konfigurace zabezpečení v prostředí Trusted Execution Environment (TEE).
- **X.509** Standard definující formát veřejného klíče (PKI), pro správu digitálních certifikátů a šifrování. Je důležitou součástí transportní vrstvy používá se pro zabezpečení komunikace na webu a emailu.

Komunikace

Pro IoT se vzhledem k mobilitě uvažuje hlavně o komunikaci pomocí radiového přenosu. Je to dáno hlavně velkým množstvím koncových zařízení a propojení drátem by bylo velmi neekonomické a také nepohodlné. Dále nastává i problém přístupu do některých míst pomocí drátu. Bezdrátovou komunikaci lze i lépe implementovat do již hotových budov a oblastí.

2 RADIOVÁ KOMUNIKACE

Jak již bylo řečeno pro IoT se jeví jako nejvhodnější použití radiové komunikace, bude zde lehce objasněna problematika tohoto typu přenosu. Radiové bezdrátové komunikace přenáší informaci ve volném prostředí. Přenos informace probíhá pomocí radiových vln. Radiovými vlnami nazýváme elektromagnetické vlnění v kmitočtovém pásmu 10 kHz až 3000 Ghz, což odpovídá vlnovým délkám v rozsahu 30 km až 0,1 mm [11]. V této práci bude nejvíce využíváno kmitočtové pásmo 300–3000 kHz, které náleží ultra krátkým vlnám viz Tab. 2.1.

Tab. 2.1: Kmitočtová pásma radiových vln [11].

Číslo pásma N	**Kmitočet**	**Délka vkny**	**Název pásma**	**Metrické zkratky**	**Symboly**	**Český název**
4	3–30 kHz	100–10 km	myriametrické	Mam	VLF	velmi dlouhé
5	30–300 kHz	10–1 km	kilometrické	km	LF	dlouhé
6	300–3000 kHz	1000–100 m	hektometrické	hm	MF	střední
7	3–30 MHz	100–10 m	dekametrické	dam	HF	krátké
8	30–300 MHz	10–1 m	metrické	m	VHF	velmi krátké
9	300–3000 MHz	10–1 dm	decimetrické	dm	UHF	ultra krátké
10	3–30 GHz	10–1 cm	centimetrické	cm	SHF	centimetrové
11	30–300 GHz	10–1 mm	milimetrické	mm	EHF	milimetrové
12	300–3000 GHz	1–0,1 mm	decimilimetrické	dmm	-	-

Ultra krátké vlny

Ultra krátké vlny jsou frekvence na rozsahu 300–3000 MHz podle Mezinárodní telekomunikační unie (ITU) [12]. Tyto frekvence jsou určené pro televizní vysílání, letecké systémy, družicové systémy (GPS) nebo mobilní systémy jako třeba GSM nebo LTE, dále pak standard Wi-fi. V tomto pásmu se radiové vlny šíří přímou vlnou (tedy na přímou viditelnost). Největší problém nastává, když jsou tyto vlny blokovány nějakým objektem, především ve městech s hustou zástavbou můžou tyto vlny blokovat velké budovy, oproti tomu na volném prostranství mohou být překážkou kopce, musíme tedy dbát na velkou pravděpodobnost odrazů.

2.1 Základní radiové parametry

Tato práce se zabývá bezdrátovou komunikací je nutné, zde věnovat pozornost základním výrazům a principům v rámci radiové komunikace. Frekvence neboli kmitočet, udává počet opakování periodického děje za určitý časový úsek. Tedy jednoduše

řečeno kolikrát proběhne signál během vteřiny. Symbolem této veličiny je f a jednotkou je Hertz.

Šířka pásma (bandwidth)

Představuje určitou šířku intervalu frekvencí, kterou je schopen přenosový kanál přenést, protože každý kanál je schopen přenést pouze signál z určitého omezeného intervalu. Signál s frekvencí mimo tento interval je přenášen s velkým útlumem a zkreslením. Jednotkou šířky pásma je Hertz. Rozdělení kanálů:

- **Wideband** - širokopásmové kanály, obsazení 25 kHz radiového spektra.
- **Narrowband** - úzkopásmové kanály, obsazení 12,5 kHz radiového spektra.
- **Ultra-narrow band** - ultra úzkopásmové kanály, obsazení 6,5 kHz radiového spektra.

Modulace

Modulace je určitý postup, kterým se na nosnou (harmonický signál v přeloženém pásmu) prostřednictvím změn průběhu tohoto harmonického signálu nanáší užitečná informace (data) a dále se tímto signálem přenáší. Modulace se provádí na analogovém signálu a po modulaci zůstává signál stále analogový. Příklady modulací:

- **Amplitudová modulace (AM):** Při této modulaci jsou jednotlivé logické hodnoty vyjádřeny různými hodnotami amplitudy.
- **Frekvenční modulace (FM):** Při této modulaci jsou jednotlivé logické hodnoty vyjádřeny různými frekvencemi.
- **Fázová modulace (PM):** Při této modulaci jsou jednotlivé logické hodnoty vyjádřeny změnou fáze (posunutím).

Modulační rychlost

Vyjadřuje počet změn nosného signálu za jednotku času, tedy jak rychle se mění signál. Měří se v Baudech.

Přenosová rychlost

Udává objem informace přenesený za časovou jednotku. Je závislá nejen na šířce pásma, ale i na kvalitě přeneseného signálu (odstup signálu od šumu). Měří se v bitech za sekundu [13].

Typy přenosů

Úzkopásmový přenos(narrowband) používá pouze tak široký rozsah frekvencí jaký odpovídá přenášenému signálu. Nevýhodou je, že má menší odolnost vůči různým negativním vlivům například šum, je u něj snazší rušení a odposlech. U tohoto přenosu je nutnost vysílat nad šum, z toho důvodu potřebujeme vyšší výkon. Druhý typ přenosu je **přenos v rozprostřeném spektru** (Spread spectrum), u něj je záměrně použito širšího rozsahu frekvencí, což je nezbytně nutné pro stížení odposlechu, neoprávněného příjmu či rušení. Má tedy větší odolnost vůči nepříznivým přírodním podmínkám a hlavní výhodou je možnost vysílání nižším výkonem než u úzkopásmového přenosu, protože lze vysílat i pod úrovní šumu.

2.2 Rozdělení radiových komunikací

Radiové komunikace lze rozdělit podle licencí, a to na licenční a bezlicenční, kde bezlicenční pásma jsou popsány podrobněji. Dále budou komunikace rozděleny podle vzdáleností na Short-range a Long-range a podle rozsahu sítě PAN, LAN a WAN pro porovnání. Nakonec budou popsány existující technologie a jestli jsou standardizované nebo proprietární a co to vlastně je. Popis je kvůli jasnému zařazení technologie LoRaWAN do radiových komunikací.

Rozdělení dle licence

Licencovaná pásma Jsou pásma, na kterých může vysílat pouze provozovatel oprávněný státem, je to osoba, která má pronajaté určité frekvence. Tyto pásma v České republice přiděluje Český telekomunikační úřad (ČTÚ). Zažádat o licenci může každý, kdo splňuje přesně daná kritéria podle práva telekomunikačních licencí, které nalezneme v Zákonu o telekomunikacích v dokumentu č. 151/2000 Sb., s úč. 1.7.2000 [14]. Běžné vyřízení trvá 40 dnů, ve složitých případech až 120 dnů a při výběrovém řízení až 240 dnů. Cena se odvíjí od určité licencované frekvence a podle ČTÚ. Důležitým parametrem je pásmo, šířka kanálu, vysílací výkon atd. Ceny se pohybují v řádech tisíců až desetitisíců korun, různé poplatky lze nalézt v sazebníku správních poplatků [15].

Bezlicenční pásma Pásma nesoucí název ISM (Industrial, Scientific and Medical) jsou pásma, na kterých může každý volně vysílat. V České republice jsou taktéž spravovány ČTÚ. Výhody oproti licencovaným jsou, že počet uživatelů zde není omezen, takže využívat je může kdokoli. Nevýhodou je, že u těchto sítí není nic garantováno a nastává tu problém se vzájemným rušením, například Wi-fi. Pásmo 2400–2500 MHz je volné a pracuje na něm na kmitočtu 2400 MHz Wi-fi, pásmo

využívá dále také Bluetooth, nebo mikrovlnné trouby. ISM pásmo s frekvencí 433 MHz se používá pro komunikaci na krátké vzdálenosti většinou do 300 m, toto pásmo je mimo jiné velmí vytížené.

Rozdělení dle vzdálenosti

Komunikace Short-range Je bezdrátová komunikace, která má dosah stovky metrů a až několik kilometrů. Největší výhodou je velmi malá spotřeba díky malým vysílacím výkonům v řádech mW. Slouží k propojení malých zařízení nebo periferií. Pracují v režimu ad-hoc tedy bez přístupového bodu. Technologie pracující s tímto dosahem jsou třeba Bluetooth, UWB (UltraWide-Band), jež jsou obě pracující v rozprostřeném spektru, nebo ZigBee pracující jako úzkopásmové.

Komunikace Long-range Je bezdrátová komunikace, která má dosah stovky metrů a až několik kilometrů. Většinou metropolitní sítě nebo i regionální. Pracují v režimu infrastruktury to znamená, že mají nějakou koncovou stanici a používají přístupové body (AP). Nejvíce využívané technologie v mobilních sítích jsou technologie GSM a LTE pracující na dlouhé vzdálenosti. Dále pak Wi-fi a především LPWAN technologie jako LoRa a Sigfox.

Rozsah Pro lepší orientaci jsou zde popsány rozsahy sítí. Nejmenší PAN (personal area network) je síť, která propojuje telefony, počítače a další zařízení v rámci místnosti nebo domu, mají velmi malý okruh dosahu zhruba 10 m. Dále LAN (Local Area Network) síť, která propojuje zařízení v okruhu firmy zvládá vzdálenosti až 100 m. Poslední WAN (Wide Area Network) jde síť, která komunikuje v rámci určitých oblastí na velké vzdálenosti až desítky kilometrů.

Rozdělení dle provedení

Standardizované řešení Jedná se o technologie v rámci nějaké uznávané autority pro příklad společenství IEEE nebo 3GPP. Existuje i řešením open-standard, které zastřešují různé aliance firem. Výhodou je, že do těchto řešení lze „vidět“ a přizpůsobit se jim, takže garantují dobrou komunikaci mezi různými systémy.

Proprietární řešení Je to takové řešení, které je většinou v rámci jedné firmy nebo autora, tedy pokud provozovatel má zájem, aby do tohoto řešení nikdo neviděl, nestane se tak a ani jej bez svolení nemůže nikdo převzít. Problematické propojení mezi dalšími systémy, bývá i dražší.

Zařazení radiových technologií

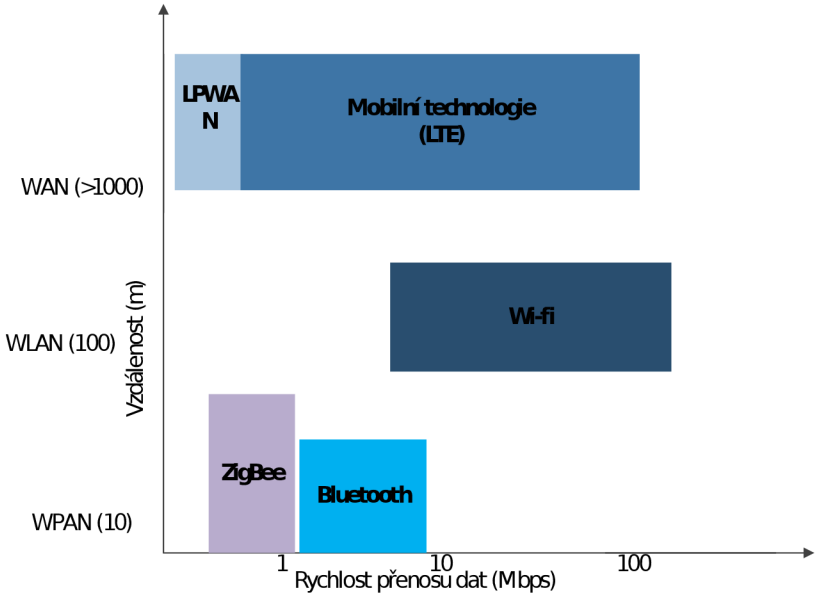
Podle předchozích parametrů byly v Tab. 2.2 zařazeny různé radiové technologie pro porovnání s Low Power WAN technologií LoRaWAN využívanou a popsanou dále v této práci.

Tab. 2.2: Parametry vybraných radiových technologií.

Technologie	**Licence**	**Frekvence**	**Vzdálenost**	**Rozsah**	**Řešení**
LoRaWAN	Bezlicenční	868 MHz	Long-range	WAN	Open-standard
SigFox	Bezlicenční	868 MHz	Long-range	WAN	Proprietární
Wi-Sun	Bezlicenční	868 MHz	Long-range	WAN	Open-standard
Ha-Low	Bezlicenční	868 MHz	Long-range	WAN	Open-standard
Nb-IoT	Licenční	800 MHz, 900 MHz	Long-range	WAN	Standard
LTE	Licenční	800 MHz, 900 MHz, 1800 MHz, 2600 MHz	Long-range	WAN	Standard
GSM	Licenční	900 MHz a 1800 MHz	Long-range	WAN	Standard
RACON	Licenční	9320 - 9500 MHz a 2920 - 3100 MHz	Long-range	WAN	Proprietární
Wi-max	Licenční	3,5 GHz a 10,5 GHz	Long-range	WAN	Standard
Wi-fi	Bezlicenční	2,4 GHz a 5 GHz	Long-range	LAN	Standard
Bluetooth	Bezlicenční	2,4 GHz	Short-range	PAN	Standard
Zigbee	Bezlicenční	868 MHz a 2,4 GHz	Short-range	PAN	Standard

3 LOW POWER WIDE AREA NETWORK

Je to technologie, která dokáže komunikovat na velmi velké vzdálenosti s co nejmenší spotřebou energie. Výdrží několik let na jednu baterii po splnění podmínek, kdy při vysílání je spotřeba co nejmenší v jednotkách až desítkách mA. Přenáší velmi malý objem dat, proto je tato technologie vhodná pro sběr dat ze senzorů v IoT. V LPWAN nazýváme přístupové body (BTSky) jako gateway na nichž záleží kvalita komunikace, čím větší hustota těchto přístupových bodů v zastavěných oblastech, tím lepší dostupnost signálu. Koncové zařízení dokáží v terénu bez překážek komunikovat s přístupovými body až v rámci desítek kilometrů. V grafu Obr. 3.1 lze vidět porovnání LPWAN s ostatními technologiemi [16]. Detailnější srovnání parametrů [17], [18], [19] je pak v grafu Obr. 3.2.

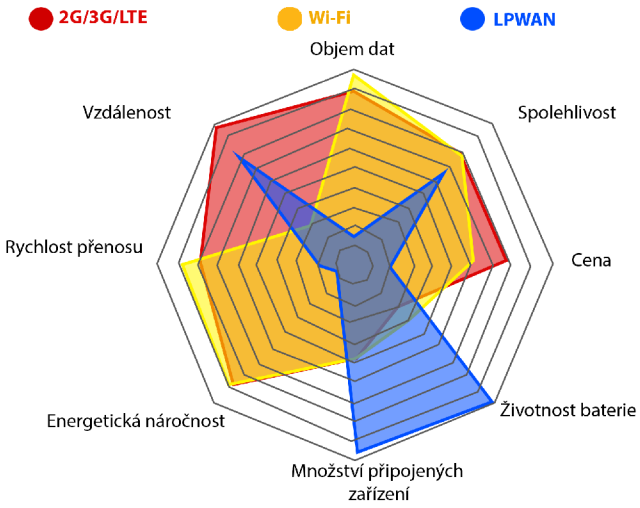


Obr. 3.1: Graf závislosti rychlosti přenosu dat na vzdálenosti.

Technologie LPWAN dokáže pracovat s útlumem celkové trasy až 160 dB, a to díky velmi velké citlivosti přijímače kolem -130 dBm. U běžných bezdrátových technologií je citlivost přijímačů zhruba od -90 dBm až -110 dBm. Technologie přijímače s citlivostí -130 dBm může detekovat až 10 000 krát slabší signály než přijímač s citlivostí -90 dBm, což je pro LPWAN klíčové. Zvětšení citlivosti přijímače docílíme snížením modulační rychlosti. Při snížení modulační rychlosti o polovinu je potřeba na každý znak (bit) dvakrát více energie, a to vede k většímu zatížení linky, ale také ke zvýšení citlivosti přijímače v poměru 2:1 tedy 3 dB [20].

LPWAN pracují jak v licenčních pásmech, tak i v bezlicenčních. Výhodou licencovaného pásma je, že pracuje lépe a je zde daleko menší rušení od ostatních

uživatelů než v bezlicenčním, v nejlepším případě by rušení nemělo nastat vůbec. Hlavní nevýhodou je hlavně zpoplatnění těchto pásem. Další nevýhoda může být velikost přiděleného pásma, které je menší než 1 MHz, oproti tomu bezlicenční mají možnost až 26 MHz [20]. Pro bezlicenční pásmo pracují LPWAN v Evropě na frekvenci 868 MHz a ve Spojených státech na frekvenci 915 MHz.



Obr. 3.2: Ukázka LPWAN v porovnání s jinými technologiemi.

3.1 Technologie

Zde jsou ve stručnosti popsány Low Power WAN technologie, parametry těchto technologií jsou porovnány v tabulce nacházející se v příloze B. Mimo technologii LoRaWAN, která je podrobně popsána dále v práci. Byly zvoleny k porovnání LPWAN technologie, které jsou v současné době nejvíce diskutovány a propagovány.

Sigfox Je technologie, která zde bude popsána podrobněji, vzhledem k tomu, že se jedná v této době o největší konkurenci LoRaWAN technologie v ČR. Technologie pochází od stejnojmenné francouzské firmy, ve Francii je také SigFox nejrozšířenější více než 1000 stanic po celé zemi. V České Republice tuto technologii propaguje společnost T-mobile se společností SimpleCell a pracuje na bezlicenčním pásmu 868 MHz. Plánované pokrytí pro ČR do konce roku 2016 je pokrýt 95 % území a 85 % vnitřních prostorů [21]. Jde o nejvíce energeticky úsporné řešení, rozbor energetické spotřeby lze nalézt na stránkách onsemi [22]. Nevýhodou je, že nejde o otevřený protokol, není moc dobře využitelná pro zpětnou vazbu vzhledem k downlinku max 4

zprávy. Jde o úzkopásmový přenos s frekvencí signálu 100 Hz. Má velmi malou rychlost přenosu a je zde použita klíčovací modulace DBPSK. Propustnost dat je velmi malá, maximálně dvanácti bajtové pakety. Rychlost přenosu je velmi malá 100 bit/s, doba přenosu a zpracování jedné zprávy je kolem 2–4 sec. Za den může poslat maximálně 140 zpráv. Pokud je možné denně poslat 140 zpráv a jedna může mít 12 bajtů tak vychází že $1440/140 = 10$, tedy jedna zpráva za 10 minut. Zpětný kanál je velmi omezen, dříve byla SigFox jen jednosměrnou komunikací, teď umožňuje na zpětném kanále 4 zprávy po 8 bajtech denně.

Symphony Link Technologie postavena na modulaci LoRa je to alternativa pro LoRaWAN běžící na licenčním pásmu 900 MHz. Jedná se o standardizovanou technologii vyvíjenou firmou Link Labs [23]. Výhody oproti LoRaWAN jsou garance příjmu zpráv, to je důležité v industriální sféře, kde je důležitá nulová chybovost, a garance vždy potvrzení přijaté zprávy. Odesílání velkých souborů do koncových zařízení, a tím je možno aktualizovat firmware na dálku. Nemá limit střídy (LoRaWAN má duty-cycle limit 1 %). Umožňuje použití opakovače a tím rozšířit dosah sítě (to není u LoRaWAN možné vzhledem k limitu střídy) a zajišťuje QoS. U symphony linku není potřeba konfigurace klíčů, u všech zařízení stejného typu je v první fázi konfigurace stejná, po připojení se automaticky pomocí PKI založeného na Diffie Helman architektuře změní. Zařízení mohou vysílat výkonem až 1W. Pracuje na licencovaném pásmu 900 MHZ. Pracuje pomocí rozprostřeného spektra a využívá modulaci LoRa. Maximální přenosová jednotka je 256 bajtů. Rychlost přenosu se dostává ke 150 bit/s. Více informací pro porovnání s technologií LoRaWAN lze nalézt zde [23].

Wi-SUN IEEE 802.15.4g Je standardizované řešení, které propaguje společnost Wi-SUN. Hlavními propagátory a členy jsou firmy Analog devices, CISCO systems, Toshiba, SilverSpring networks a další. Širokopásmový přenos využívá digitální modulaci FSK tedy klíčování fázovým posuvem. Dobrá detekce chyb díky rámci FCS (rámce kontrolního součtu). Pro zmírnění rušivých signálu používá „blacklist“, díky kterému probíhá minimální rušení. Využívá adresaci na protokolu IPv6 a jedná se o plně otevřený standard [24]. Výhodou je spolupráce mezi ostatními standardy IEEE. Využívá primárně topologii Mesh (lze použít i Hvězdicovou topologii). Výhodou Mesh topologie je lepší pokrytí, ve hvězdicové topologii mohou vznikat tzv. „blackspots“, což jsou místa bez pokrytí a lze tento problém vyřešit pouze přidáním další brány. U mesh topologie zařízení komunikují navzájem se sousedními sítěmi, a tím se zvyšuje pokrytí celé sítě, vzniká takto více redundantních cest k cíli. Síť se tedy stává spolehlivější. Wi-SUN poskytuje větší rychlost přenosu dat než LoRaWAN až 300 kB/s a také má daleko menší zpoždění 0.02 sekund (LoRaWAN 1–2

sekundy). Wi-SUN má také největší možné zabezpečení takzvanou vojenskou třídu zabezpečení, porovnání bezpečnosti lze nalézt na stránkách Wi-SUN [25]. Ve stavu spánku můžou mít zařízení Wi-SUN spotřebu 2μA a ve stavu naslouchání 8 mA.

HaLow IEEE 802.11ah je standardizované řešení od aliance Wi-fi. Obrovskou výhodou je schopnost komunikace se všemi zařízeními s pásmy 802.11x, z toho plyne, že přístupové body na frekvenci HaLow budou podporovat i pásma 2,4 GHz a 5 GHz. Tento standard by se měl do oběhu dostat v průběhu roku 2018. Širokopásmový přenos, pracující s přenosovou modulací OFDM, kde budou dále subnosné modulovány pomocí BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM podle MCS indexu. Nejdůležitější zatím bude pásmo 4 MHz, které začne společnost nejdříve podporovat a na kterém by měla rychlost přenosu dosahovat 150 kb/s. O proti jiným LPWAN dosahuje celkem malých vzdáleností, kolem jednoho kilometru. Jedná se o plně otevřený standard, který je propojený s dalšímy pásmy Wi-Fi 2,4 GHz a 5 GHz [26]. Nevýhodou je malá vzdálenost komunikace pouze jeden kilometr. V Evropě pracuje na pásmu 868 MHz. Oproti ostatním LPWAN technologiím zvládá přenést velký objem dat 7 991 bajtů. Má přesně vymezený počet koncových zařízení na jednu bránu, a to 8191.

NB-IoT Je standardizované řešení telekomunikačního společenství 3GPP. Běží na stejných licencovaných pásmech jako LTE tj. 800 a 900 MHz popřípadě GSM. Ve světe i v České republice tuto technologii podporuje firma Vodafone. Oproti GSM o 20 dB lepší pokrytí. Tato technologie umožní dostupnost zařízení v sítích 2G, 3G a 4G. Díky použití licenčního pásma je zamezeno rušení ostatními zařízeními.Už podle názvu NarowBand vyplývá, že se jedná o úzkopásmový přenos. Využívá modulace rozprostřeného spektra DSSS. Má tři možnosti nasazení pro co nejlepší využití GSM nebo LTE spektra, a to standalone, guard band a in-band [27]. Pracuje buď to na GSM spektru a nebo využívá nevyužité bloky v ochranném pásmu LTE. Tato technologie je založena na topologii hvězdy. Přenáší data rychlostmi 60 kb–250 kb. Využívá pro GSM šířku pásma 200 kHZ. Vysílá s výkonem 23 dBm. Oproti LoRaWAN zaručuje QoS. NB-IoT je synchronní protokol a tedy zařízení musí pravidelně kontrolovat síť, tím se snižuje výdrž baterie, ale také je tím sníženo zpoždění. NB-IoT prvky sítě (moduly a jiné) vychází dráž než u LoRaWAN podrobné srovnání lze nalézt na stránkách lora alliance [28].

LTE-Cat M Nesoucí též název eMTC (enhanced Machine Type Communication) vychází ze standardu 3GPP. Pro uplink využívá deterministickou metodu přístupu FDMA s modulací GMSK. Pro downlink využívá OFDMA. Pracuje na frekvencích LTE tedy na licencovaných pásmech. Stejně jako NB-IoT tři možnosti nasazení –

Standalone, Guard band a in-band. LTE-M využívá hvězdicové topologie a pracuje s šířkou pásma 1,4 MHz zvládá velké rychlosti datového přenosu až 10 Mb, ale pro potřebu malé spotřeby energie byla rychlost stažena na 300 kb/s. Dosah technologie je menší než u LoRaWAN maximálně kolem 5 km.

nWave Proprietární řešení Anglické firmy Nwave Technologies. Je přirovnatelná k technologii sigfox využívá ultra úzkopásmý přenos s DBPSK modulací. Topologie této sítě je hvězdicová. Oproti jiným technologiím zajišťuje obrovské množství koncových zařízení na jednu bránu údajně až milion [29] a velkou penetraci do budov. Zvládá komunikaci na 10 km s energetickým výkonem 25–100 mW. Jedná se o open standard technologii. Velkou nevýhodou je, že nemá žádný downlink. Další nevýhoda je rychlost, pouze 100 b/s. Dále tato technologie není zabezpečená.

Ingenu RPMA Dříve pod názvem On-ramp nyní pod firmou Ingenu využívající protokol RPMA (random phase, multiple access). Velkou výhodou je vyšší přenosová rychlost a velké vzdálenosti přenosu. Vstupuje na trh později než předešlé technologie, společnost se zaměřila více na vývoj než na propagaci. Pracuje na frekvenčním pásmu 2,4 GHz. Díky své architektuře má daleko lepší kapacitu pro uplink a downlink než LoRaWAN a Sigfox. Má vysoký link budget 177 dBm a tedy i lepší pokrytí než SigFox a LoRaWAN. Nevýhodou může být použití pásma 2,4 GHz větší rušení s Wi-fi nebo bluetooth, také pentrace skrz stěny budov není u vyšších frekvencí tak dobrá. Využívá více výkonu na procesor, a tak nemusí být výdrž baterie tak velká jako u konkurenční technologií [30].

Weightless-W Je jediný celkově open standard protokol pracující na bezlicenčním pásmu vytvořený Anglickou společností Weightless. Využívá modulační metody jako 16-QAM nebo BPSK. Weightless umožňuje další dva standardy -P a -N, rozdíl je ve vzdálenostech dosahu, výdrži baterie, ceně a funkcích. Mezi výhody Weightless-W patří vysoká rychlost přenosu a velký počet koncových zařízení. Je zde možnost použití v inteligentním plynárenském a ropném průmyslu díky TVWS (TV whitespace). Pracuje na TV whitespace pásmu 400–800 MHz s šířkou pásma 5 MHz. Zvládá pokrýt až 5 km v zástavbě. Posílá pouze 10 bajtů za minutu. Rychlost přenosu je až 10 Mb/s, což se projevuje na spotřebě baterie.

Srovnání parametrů LPWAN

Zde jsou popsány parametry, které jsou srovnávány v tabulce B

- **Šířka pásma**: Šířka pásma jednoho kanálu každé technologie, jednotkou je Hertz. Obecně ovlivňuje rychlost přenosu, čím větší šířka pásma přenosového kanálu, tím větší rychlosti na něm lze dosáhnout [31].
- **Rychlost přenosu dat**: Rychlost přenosu, které dosáhne vysílač (při uplinku) každé technologie za sekundu. Ovlivňuje dobu za kterou data dorazí na koncové zařízení.
- **Vzdálenost**: Vzdálenost, na kterou dokáží zařízení komunikovat, minimum značí vzdálenost v zástavbě, maximum vzdálenost mimo zástavbu. Ovlivňuje jak dlouho budou data přenášena (Time on Air) a také sílu signálu.
- **Pásmo**: Na jakých pásmech daná technologie pracuje. Jde o frekvenční pásmo pro radiové technologie. Definuje také šířku pásma, ovlivňuje penetraci signálu (čím nižší frekvenční pásmo tím lepší penetrace), dále dosah (vyšší frekvence mívají menší dosah) a také spotřebu (přenosy na vyšších frekvencích mají většinou vyšší spotřebu) [32].
- **Počet koncových zařízení**: S kolika koncovými zařízeními zvládne pracovat jeden data koncentrátor (Gateway, base station). Ovlivňuje tedy množství možných připojených koncových zařízení.
- **Standard**: Zda-li se jedná o standardizované nebo proprietární řešení.
- **Link budget**: Označuje součet všech zisků a ztrát z vysílače skrz médium až do přijímače. Čím vyšší hodnota, tím lepší pokrytí a přenos mezi vysílačem a přijímačem.
- **Vysílací výkon**: Maximální výkon koncového zařízení při vysílání dat. Ovlivňuje sílu signálu a tedy i jeho dosah a penetraci.
- **Množství dat**: Maximální množství přenesených dat v jednom paketu. Jak velké množství dat můžeme najednou odeslat.

Využití a budoucnost

V dnešní době se čím dál více hovoří o využití LPWAN v IoT a firmy se snaží propagovat každá svou vlastní technologii co nejlépe, aby se co nejdříve uplatnila v komerčním využití. V současnosti jsou právě nejvíce spelukované technologie SigFox, LoRaWAN a také NB-IoT. Sigfox začal s propagací nejdříve a také do ní vložil velké úsilí, které se zatím vyplácí, s nejlevnější cenou modulů je může testovat kdokoli i cena přístupu do backendu je od 90 Kč a celkové pokrytí republiky je již 86 % [33]. V této době je LoRaWAN dražším řešením, ale hlavní a důležitou výhodou této technologie je možnost vytvoření vlastní nezávislé sítě, a díky tomu pokrýt jakoukoliv oblast. Potenciál a budoucnost LPWAN technologií je obrovský, jde o velice důležitou součást IoT a také průmyslu 4.0 [7]. V další kapitole bude podrobně rozebrána hlavní LPWAN technologie pro tuto práci LoRaWAN.

4 TECHNOLOGIE LORAWAN

Tato práce se především zabývá samotnou technologií LoRaWAN, která ale nebyla v předchozí kapitole popsána společně s ostatními a to z důvodu nutnosti detailnějšího popisu. Ukázka vrstev této technologie na obrázku Obr. 4.1. Jedná se o open standard od neziskové organizace LoRa Alliance. LoRa je modulační technologie pro dlouhé vzdálenosti (long-range), má malou rychlost přenosu dat, nízké napájecí potřeby a je určena pro bezdrátovou komunikaci. Byla vyvinuta francouzskou firmou Cycleo, kterou později převzala společnost Semtech [34]. LoRaWAN je síťový protokol, který využívá širokopásmové modulace. Přináší konektivitu dat přenášených rychlostí nižší než 25 kbps. Umožňuje propojení tisíců uzlů připojených k jedné bráně (gateway) v rozsahu jednotek kilometrů.

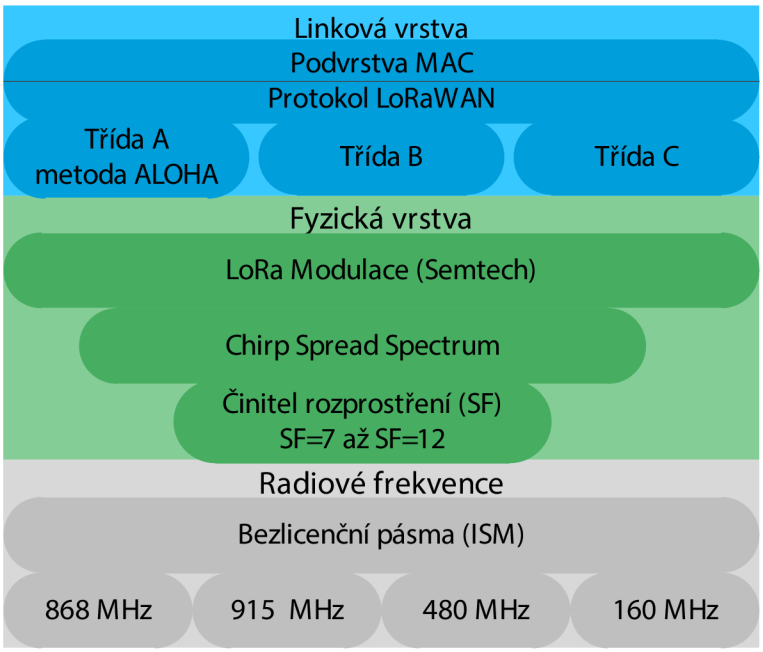
Tento protokol využívá hvězdicové topologie, ve které gateway slouží k předávání informací mezi koncovými uzly a centrálními síťovými uzly. Gateway komunikuje se síťovým serverem pomocí protokolu IP, zatímco koncové zařízení komunikuje s bránou pomocí single-hopu, což znamená, že komunikace probíhá postupně přes všechny uzly až k bráně.

Komunikace tohoto protokolu je obousměrná, ačkoli hlavní komunikace probíhá jako uplink – z koncových zařízení na síťový server, oproti tomu downlink (ze serveru na koncové zařízení) je omezen podle třídy použití. Komunikace mezi koncovými zařízeními a bránami je zprostředkována pomocí modulačního spektra CSS (Chirp Spread Spectrum), jedná se o modulační techniku rozprostřeného spektra (rozprostření mezi více kanály, širší rozsah frekvencí)[35], využívá ortogonální rozprostření, díky kterému se komunikace mezi zařízeními vzájemně neovlivňuje.

Rychlost datového přenosu LoRaWAN se pohybuje podle použité šířky pásma, v rozmezí 0,3 kbps až 27 kbps při využití šířky pásma 125 kHz a 11 kbps až 50 kbps pro 250 kHz [36]. Pro maximalizaci jak životnosti baterie koncových zařízení, tak i zvýšení celkové kapacity sítě si LoRaWAN řídí přenos pomocí schématu ADR (Adaptive Data Rate) [37].

4.1 Fyzická vrstva modulace LoRa

Fyzická vrstva využívá modulace LoRa, ta je postavena na rozprostřeném spektru, to znamená, že šířka pásma odeslaného signálu je větší než šířka pásma originální zprávy. Rozprostření probíhá pomocí CSS (Chirp Spread Spectrum). Definuje 6 činitelů rozprostření SF (Spreading Factor, který určuje poměr čipové rychlosti ku rychlosti modulační) SF=7 až SF=12, které zajišťují ortogonální vysílání s různými rychlostmi přenosu dat. Pakety zde obsahují preambuli (8 znaků, jde o rozpoznání začátku), hlavičku, užitečná data (jejichž maximální velikost se pohybuje



Obr. 4.1: Rozdělení vrstev.

od 51 bajtů po 222 bajtů odvíjející se od zvoleného činitele rozprostření) a cyklický redundantní součet CRC (hašovací funkce používaná k detekci chyb během přenosu či ukládání dat).

LoRa může pracovat na frekvencích mezi 150 MHz až 1 GHz, nicméně Semtech stanice jsou designované na práci v rozmezí 850 MHz – 1 GHz. Šířky pásma pro tuto technologii jsou 125 kHz, 250 kHz a 500 kHz v pásmu 868 MHz pro Evropu a 915 MHz pro Ameriku. Můžou být použity i nižší frekvence, a to 160 MHz a 480 MHz (mají šířku pásma od 7,5 kHz až po 62,5 kHz. Rychlost přenosu dat se liší v závislosti činitele rozprostření (SF), šířky pásma a vzdálenosti. Pohybuje se mezi rychlostmi 22 bit/s (pro šířku pásma 7,8 kHz a SF = 12) až po 27 kbit/s (pro šířku pásma 500 kHz a SF = 7) [38].

4.1.1 Rozprostřené spektrum

LoRa je modulace pracující, jak už bylo řečeno, jako rozprostřené spektrum. Je důležité zde zmínit Shannon-Hartley Theorem, tento zákon nám říká jakou maximální kapacitu dat může přenést za jednotku času po komunikačním kanálu o určité šířce pásma v přítomnosti šumu. Vztah pro výpočet kapacity kanálu je $C = B \times log_2(1+\frac{S}{N})$ [39], kde C je kapacita kanálu (objem dat který je možno na daném kanálu přenést za jednotku času), B šířka kanálu v Hz, S/N je poměr signálu k šumu (SNR).

Technika rozprostřeného spektra byla vytvořena pro minimalizaci možnosti od-

poslechu, dnes se tato technika používá hlavně pro zlepšení odolnosti proti rušícím vlivům a také kvůli potřebě menšího vysílacího výkonu, díky čemuž je menší spotřeba energie. Jednou z nejpoužívanějších technik je DSSS (Direct Sequence Spread Spectrum), zde dochází k pseudonáhodnému generování sekvence bitů a každý jednotlivý bit přenášené zprávy je nahrazen touto sekvencí a modulována na nosný signál je až tato sekvence. Tato sekvence je označovaná jako chip. Tímto dochází k rozprostření signálu do spektra. LoRa využívá modulační techniku CSS (Chirp Spread Spectrum), u které ale nedochází k pseudonáhodnému generování, zde je rozprostření prováděno pomocí lineární změny frekvence v čase. Výhodou této techniky je, že časové a frekvenční posuny jsou mezi vysílačem a přijímačem ekvivalentní, což výrazně snižuje složitost přijímače.

Teoretické výpočty technologie LoRa

Výpočet přenosové rychlosti v závislosti na Spreading Factoru [40], pro hodnoty SF=12, BW (šířka pásma) 125 kHz a Rate code = 4/5. Výsledné hodnoty pro ostatní SF jsou v Tab. 4.1 i s velikostí útlumu. Zde je vzorec výpočtu:

$$R_b = SF \times \frac{Rate\,code}{\frac{2^{SF}}{BW}}\,[bit/s],$$

$$R_b = 12 \times \frac{\frac{4}{5}}{\frac{2^{12}}{125000}} = 293\,bit/s.$$

Tab. 4.1: Rychlosti a útlum v závislosti na SF.

Mód	**Rychlost bit/s**	**Útlum (dB)**
SF=12	293	-137
SF=11	537	-134.5
SF=10	976	-132
SF=9	1757	-129
SF=8	3125	-126
SF=7	5468	-123
SF=6	9375	-118

Teoretický výpočet pro dobu přenosu paketu. Počítáno je s těmito hodnotami: velikost payloadu je 13 bitů, Spreadin Factor má hodnotu 12, šířka pásma je 125 kHz. Nejdříve je nutno spočítat rychlost symbolu za periodu:

$$Ts = \frac{2^{SF}}{BW}\,[s],$$

$$Ts = \frac{2^{12}}{125000} = 32,768\,ms.$$

Dále je nutné spočítat preambuli což je u LoRaWAN definováno jako 8 symbolů:

$$T_{preamble} = (n_{preamble} + 4,25) \times T_s,$$

$$T_{preamble} = (8 + 4,25) \times 32,768 = 401,42\,ms.$$

Počet symbolů tvořících payload a záhlaví je dán vztahem:

$$payloadSymbNb = 8 + max(ceil(\frac{8PL - 4SF + 28 + 16 - 20H}{4(SF - 2DE)})(CR + 4), 0),$$

kde PL je hodnota payloadu, SF je Spreading Factor, H je pokud je zahrnuta i hlavička hodnota 1 pokud ne hodnota 0 zde bylo počítáno s hlavičkou. Výsledek byl dopočítán pomocí programu Microsoft Excel:

$$payloadSymbNb = 23.$$

Díky tomu můžem spočítat dobu zatížení:

$$Tpayload = payloadSymbNb \times Tsym = 753,66\,ms.$$

Nakonec lze spočíst Time on Air (tedy dobu přenosu paketu vzduchem):

$$T_{packet} = T_{preamble} + T_{payload},$$

$$T_{packet} = 1155,072\,ms.$$

Výpočet byl prováděn podle vzorců z literatury Semtech [41].

4.2 Linková vrstva

Na linkové vrstvě je LoRaWAN definován na podvrstvě MAC (tato podvrstva zajišťuje fyzické adresování a řízení přístupu k médiu). Zde LoRaWAN podporuje tři různé typy zařízení podle funkce:

- **Zařízení třídy A:** Tato zařízení využívají přístupovou metodu ALOHA. Po odesílání dat (uplinku) naslouchá po dobu určeného intervalu. Naslouchá pouze pro dva downlinky (první potvrzení a ve druhém můžou být nějaká data), a to bezprostředně po odeslání dat. Díky tomu má nejnižší spotřebu.
- **Zařízení třídy B:** Naslouchá podle přesně určených časových intervalů (downlink v určených časových intervalech).
- **Zařízení třídy C:** Tyto zařízení naslouchají nepřetržitě s výjimkou doby, kdy vysílají. Mají největší odběr energie.

Všechny tyto typy zařízení jsou definovány pro LoRaWAN [42], ale pro LPWAN jsou nejvhodnější zařízení třídy A, a to kvůli své velké výdrži baterie. Parametry LoRaWAN lze vidět v tabulce Tab. 4.2

4.3 Limity v LoRaWAN

Výkon LoRaWAN je mimo omezení v jednotlivých vrstvách také ovlivněn omezeními v ISM pásmech. Hlavním omezením je střída, která procentuálně definuje po jakou dobu může být kanál obsazen. Je zde čas potřebný pro přenos paketu, ten nazýváme jako čas ve vzduchu T_a (Time on Air), po kterém následuje vždy minimální doba vypnutí periody T_s, během této doby není kanál k dispozici pro zařízení. Maximální počet přenesených paketů za hodinu skrz jeden uzel lze spočítat pomocí vzorce dle [19]:

$$M = \frac{3600}{(T_a + T_s)}.$$

Po zvolení činitele rozprostření SF, šířky pásma a zařízení třídy A s metodou ALOHA, musíme ještě znát počet koncových zařízení N a počet kanálů n. Může nastat kolize pro určitý kanál a to v případě, že budou dvě koncová zařízení využívat stejný SF. Dále lze tedy vypočítat počet přenesených paketů za sekundu pomocí vztahu dle [19]:

$$S = \sum_{i \epsilon F} N p_i \lambda_i e^{-2 p_i N T_{a_i} \lambda_i / n},$$

kde i = 7 – 12, jedná se o výběr z rozmezí SF, p_i pravděpodobnost, že koncové zařízení používá SF_i, λ_i je množství paketů na uživatele v závislosti na SF_i, T_{a_i} Time on Air taktéž závislý na SF_i. Výkon LoRaWAN je závislý jak na střídě tak i na vnitřních kolizích ALOHA přístupu. Nejvíce vhodný činitel rozprostření je SF=12, bohužel je tedy nejpomalejší – nejvyšší hodnoty T_{a_i}.

Pokud všechny koncové zařízení odesílají maximální množství paketů ($\lambda_i = \frac{d}{T_{a_i}}$ kde d je střída), tak se počet paketů úspěšně přijatých bránou snižuje. Čím více zařízení, tím méně přijme gateway paketů. Počet přijatých paketů poklesne z důvodů ALOHA modelu (uzel se neohlíží na to jestli někdo něco odesílá). Dále vysokému množství odeslaných paketů brání střída a u nízkého množství je zase LoRaWAN limitována kolizemi (ALOHA). Zde vyplývá, že maximální propustnost klesá, čím větší množství uzlů stanice obsahuje.

4.3.1 Spolehlivost

V protokolu LoRaWAN je dosaženo spolehlivosti prostřednictvím potvrzení příjmu ACK (acknowledge), funguje tak, že strana, která přijímá data po obdržení těchto dat, potvrzením indikuje jejich bezchybnost. Vysílající strana poté může uvolnit vyrovnávací paměť, jejíž obsah musí udržovat v případě, že by došlo ke kolizi a bylo by potřeba vysílat znovu.

Pro zařízení třídy A může být rámec ACK odeslán pouze v jednom ze dvou možných downlinků, takže zbyde pouze jeden pro další data. Pro zařízení třídy B

Tab. 4.2: Charakteristika LoRaWAN.

LoRaWAN charakeristika	
Topologie	Hvězda
Frekvence	867-869 MHz (Europe and India) 902-928 MHz (North America and Brazil)
Rychlost	22 b–50 kb
Průměrné zpoždění	1 s
Max zařízení na bránu	15,000
Dosah v zástavbě	2–5 km
Dosah bez překážek	10–15 km
Uplink	Data
Downlink	Data + ACK
Payload	51–222 Bajtů
Vysílací výkon	14 dBm
Útlum	-137 dBm

je buďto jako u třídy A a nebo v přesně určených časových intervalech. U třídy C může být přenesen kdykoli. Komunikace brány se zařízením (downlink) je taktéž limitována minimálním časem, kdy je perioda vypnuta – gateway je taktéž limitována střídou). Počet ACK rámců musí být co nejvíce minimalizovaný, aby se zabránilo zbytečnému výkonu, a tedy větší spotřebě.

4.3.2 Využití

LoRaWAN technologie má mnoho oblastí , ve kterých lze tuto technologii využít. Některé oblasti využití jsou uvedeny níže.

- **Bezpečnost** – zde můžeme využít třeba pro hlídání osob (monitorování zda jsou tam, kde mají být) nebo zabezpečení domů (pokud by se někdo chtěl dostat do budovy, odešle signál).
- **Zemědělství** – Monitorování zvířat (kde se nachází a jejich stav), zavlažovací systémy.
- **Doprava** – Vytížení dopravních prostředků, monitorování parkoviště (volná místa).
- **Průmysl** – Monitorování výrobních procesů.
- **Životní prostředí** – Monitorování kvality ovzduší nebo teploty.
- **Energetika** – Monitorování spotřeby energie na dálku, lepší zapojení obnovitelných zdrojů do energetických sítí, a tím šetření energie a přírody.

Čipy technologie LoRaWAN můžeme použít téměř na cokoliv. Hlavní použití LoRaWAN je tedy **monitorování v reálném čase, měření a zaměření na aplikace ve smart city a v chytrém zemědělství**.

Monitorování v reálném čase

Je důležité třeba v průmyslu. V reálném čase se rozumí s co nejmenším zpožděním a s co nejmenším rozkolísáním (jitter). Protokol LoRaWAN není pro toto monitorování úplně vhodný, ale je pro tyto účely použitelný podle toho, co budeme od koncové aplikace požadovat. Není vhodná hlavně z důvodů, že latence by měla být opravdu malá a odezva (Time on Air) 1 ms až 100 ms. LoRaWAN i pro malé pakety o velikosti 10 bytů při použití SF = 7 má odezvu kolem 40 ms [19]. Z důvodů využívání ALOHA modelu nelze dosáhnout dostatečně rychlé odezvy, a to kvůli kolizím, které v této metodě nastávají, a tím pádem dochází ke zvyšování jitteru (rozkolísání tedy zpožďování přenosu a nepravidelnosti doručování dat). Záleží na použití aplikace, některé si vystačí s daty každou sekundu a pro toto řešení už je LoRaWAN vyhovující, ale musí být použit vhodný počet koncových zařízení (co nejmenší kvůli možnostem kolizí) a gateway se musí nacházet co nejblíže koncovým zařízením.

Měření

LoRaWAN je ideální pro odesílání dat z měřících přístrojů. Vysílání párkrát za den pro přehled spotřeby. V tomto ohledu je využitelná ve Smart Grid sítích. Pro kontrolu a regulaci spotřeby energie a implementování obnovitelných zdrojů energie.

Chytrá města

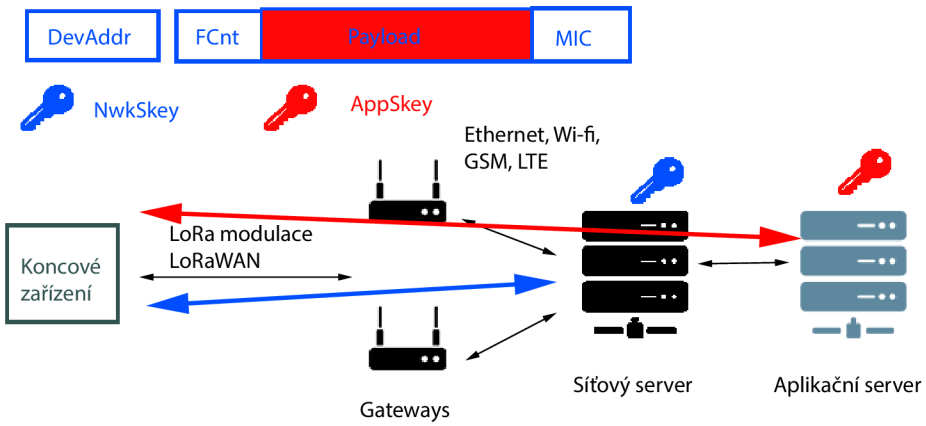
Zde se jedná o aplikace pro použití u chytrého osvětlení, chytré parkování nebo sběr odpadu. U chytrého parkování monitoruje stav volných míst na parkovišti. Problém zde je, že může být vyžadováno použití velkého množství koncových zařízení, což zpomaluje celou síť (třeba u osvětlení může zahltit bránu lavinou zpráv, když se začne rozsvěcovat v jednu dobu), nebo může dojít k úplnému zahlcení. LoRaWAN má velký potenciál využití v chytrých městech.

4.4 Bezpečnost

Zabezpečení LoRaWAN využívá kryptografický systém AES kombinovaný s několika režimy jako CMAC2 pro ochranu integrity a CTR3 pro šifrování. Každé zařízení využívá symetrického 128-bitového klíče AES. Podle organizace IEEE jsou sítě LoRaWAN identifikovány pomocí 24-bitového, globálně jedinečného identifikátoru.

4.4.1 Připojení zařízení do sítě

Pro připojení zařízení do LoRaWAN sítě jsou využívány dvě metody OTAA a ABP. LoRaWAN používá dva typy klíčů pro zabezpečení, tyto klíče jsou unikátní pro každé zařízení. Je to klíč NwkSkey, který je používán pro zprávy na síťové vrstvě od koncového zařízení k síťovému serveru a AppSkey používaný pro aplikační vrstvu využívající šifrování AES-128, používá se při komunikaci z koncového zařízení na aplikační server [43]. Ukázka klíčů na diagramu 4.2.



Obr. 4.2: Diagram použití klíčů.

OTAA(Over The Air Activation): Umožňuje připojení zařízení do sítě a jako autentizaci využívá klíč a podpis.Nejprve je zařízení a síťový server vybaven unikátním 128 bitový klíčem (AppKey), tento klíč se využívá při požadavku k připojení do sítě (join-request). Po prvním spuštění zařízení je na síťový server odeslána žádost o spojení (join-request). AppKey se používá pro vytvoření kódu integrity zpráv MIC (Message Integrity Code), server poté kontroluje MIC pomocí AppKey, pokud je klíč platný, server generuje dva nové 128-bitové klíče, klíč relace aplikace AppSkey a klíč síťové relace NwkSkey. Klíče jsou poté poslány zpět do zařízení zašifrované pomocí AppSkey. Zařízení poté klíče dešifruje a nastaví. Výhodou je, že jsou pro každou relaci generovány nové klíče. Nevýhodou je nutnost využití downlinku pro potvrzení.

ABP (Activation By Personalisation): Každé zařízení má již danou adresu (DevAddr) a dva klíče (NwkSKey - síťový a AppSKey - aplikační), které jsou pro každé zařízení jedinečné. Díky této metodě nemusí již zařízení zasílat zprávu s žádostí o připojení (join-request). Tyto klíče se zadávají většinou přímo ve výrobě, a zařízení mohou rovnou začít komunikovat se serverem. Výhodou je, že nepotřebuje

potvrzení pomocí downlinku. Nevýhodou je, že operátor zná klíče, proto se používá hlavně pro testování.

Klíče uvnitř zařízení a jejich zabezpečení: Často se stává, že je použit stejný AppKey pro všechna zařízení v rámci jedné aplikace.Vytvořen operátorem pro všechny zařízení a nebo již z výroby každé zařízení může mít stejný AppKey. Nastává zde problém, jelikož lze tento klíč přečíst, pokud je možnost fyzického přístupu k jednomu zařízení z celé aplikace. Klíč se nachází nezašifrovaný v paměti tohoto zařízení a tak jej lze lehce přečíst. Tomuto lze předejít generováním vždy jiného AppKey pro každé zařízení.

4.4.2 Ochrana dat

Po připojení do sítě pomocí jedné z metod OTAA nebo ABP budou zprávy šifrovány za pomoci kombinace NwkSKey a AppSKey. Tyto klíče zná pouze samotné zařízení a síťový server. Není připuštěno, aby tyto klíče znalo jiné zařízení, nebo aby proběhl útok man in the middle. LoRa je zabezpečena a chrání proti útokům jako man in the middle, které se týkají důvěryhodnosti a integrity dat. Zabezpečuje také nově připojená zařízení do sítě. O zbytek bezpečnosti už se musí postarat vývojáři samotných řešení LoRaWAN.

Bezpečnost klíčů: Většinou jsou klíče uloženy přímo ve flash nebo EEPROM paměti, která je nezabezpečená a při odesílání jsou posílány jako konstanty bez šifrování. Tomu lze předejít nejen zabezpečením paměti, ale také vytvořením kódu integrity zpráv (MIC) a tedy šifrováním a dešifrováním zprávy.

Šifrování dat: Je prováděno pomocí blokové šifry AES 128 (Advance Encryption Standard), využívající 128 bitový blok a Counter mode(CTR).

Podpis zpráv: Užitečná data na vrstvě MAC mají podpis, aby se zabránilo manipulaci s šifrovaným textem nebo jinými hodnotami jako DevAddr, FCntUP (Counter for sent messages), FCntDown (Counter for received messages).

4.4.3 Útoky

Fyzický útok

Když je zařízení nainstalováno na nějaké místo a někdo se k němu fyzicky dostane nastává problém. Může zařízení zničit, otevřít, vypnout, ovlivnit senzory nebo přečíst

klíče. Tyto útoky probíhají hlavně kvůli ovlivnění sbíraných dat, přerušení samotného vysílání dat a nebo odcizení zařízení. Pokud bude mít někdo přístup k zařízení, může, pokud je paměť nezabezpečena, přečíst klíče. Tento problém lze řešit nějakou bezpečnostní schránkou, dále také pohybovým senzorem, analýzou dat vysílání a použitím dalších zabezpečovacích prvků [44].

Sběr metadat

Takzvaný sběr dat, která popisují jiná data. Sběr dat o aktivitě zařízení, při odesílání vzduchem jsou veřejně přístupna metadata. Útok probíhá tak, že si kdokoliv může připojit vlastní gateway LoRaWAN a odchytávat na ni zprávy, které byly odeslány ze zařízení v jejím dosahu. Data, která lze z těchto zpráv sbírat, jsou data jako adresa zařízení, čítač odeslaných rámců (kolik rámců bylo odesláno) a také lze vidět velikost payloadu. Nebezpečí nastává hlavně v případě, kdy je zařízení používáno jen pro odesílání změny stavu, například nastane změna stavu dveří a v tuto chvíli není nutnost přečíst payload, jelikož jde pouze o odesílání stavu. Toto se dá řešit pomocí OTAA, dále fixní délkou payloadu, nebo odesláním náhodných dat a tím zamaskovat skutečný přenos [44].

Triangulace

Jde o nalezení zařízení pomocí času, než zpráva přijde na gateway, v kombinaci se sběrem metadat jde přesně lokalizovat zařízení. Využívá se gateway s dešifrováním timestampu. Využívá se pro nalezení koncového zařízení, hlavně tedy pokud je v pohybu (například senzor v autě). Dá se tomu předcházet pomocí OTAA a pravidelným znovu připojením [44].

Útok pomocí bran

Pokud je síť otevřená, což většinou bývá, lze připojit novou bránu do sítě. Tato brána se může chovat jako škodlivá brána v síti. Dále lze napadnout stávající bránu v síti pomoci spoofingu. Tyto útoky se provádí z důvodů sběru dat nebo filtrování z odeslaných a přijatých zpráv. Předejít se tomu dá pomocí autentizace bran v síti a také použitím potvrzení přijatých a odeslaných zpráv.

Dalším problém u bran bylo odesílání potvrzení nežádoucích odeslaných zpráv. Funguje to tak, že další brána filtruje potvrzení a uschová jej na později. Použití pro zmatení zařízení, že uplink byl potvrzen, ale ve skutečnosti potvrzen nebyl. Tento problém řeší update LoRaWAN 1.1 [44].

Útok opakováním

Je to útok, kdy jsou zachytávány zprávy a ukládány pro odeslání později. Tento útok probíhá tak, že je na bráně nastaven sběr zpráv a odesílání později. Využívá se třeba u stavových senzorů, odesíláním starých zpráv o změně stavu. Předejít se tomu dá díky použití serveru na kterém se počítají rámce (frame counter) [44].

Útok na klíče

Slabinou je použití symetrického šifrování (AES), jsou dvě místa, kde se nachází klíč, a to na samotném zařízení a na síťovém serveru. Klíč je pouze jeden stejný jak pro šifrování, tak i pro dešifrování. Zařízení by měla uchovávat pouze ty klíče, které potřebují. Slabinou jsou AES útoky, což jsou útoky postranním kanálem na klíče AppSKey a NwkSKey. LoRaWAN vyžaduje, aby byly pro každé zařízení klíče jedinečné a náhodné. Klíče nelze odvodit z veřejně dostupných informací. U síťových serverů se musí dbát na zamezení přístupu neoprávněným osobám.

Útok na data

Útok přímo na data koncového zařízení, pomocí fyzického narušení. Koncové zařízení obsahuje mikrokontroler, který je právě slabinou, nezná šifrovací klíč, dále posílá data do LoRa modulu (např. RN2483) a ten teprve data šifruje a dále posílá do sítě. Například útočník, který má fyzický přístup k zařízení, může nahradit mikrokontroler, nebo využít piny rozhraní UART a začít posílat své vlastní zprávy jménem tohoto zařízení. Řešením může být tzv. whitelist, který zachytává pouze určitá data.

Útok na komponenty skrz internet

Útok na MIC (Message Integrity Code) - jde o útok hrubou silou (2 miliardy pokusů na 8 bajtový klíč). Dále musí být zajištěna odolnost vůči DoS (Denial of Services) útokům (přehlcení požadavků nebo využití chyby, která umožní službu rozbít). Útočník může zahltit provozní webové služby útokem, důsledkem tohoto útoku, může přestat komunikovat s bránou a nakonec i s koncovým zařízením. Tento typ útok ale není pro LoRaWAN, vzhledem k tomu, že LoRa modulace využívá rozprostřeného spektra, dobře proveditelný.

Útok na čítač

Útok pro opakování úkonu, příklad – v zabezpečené oblasti, kde je ovládán alarm, by mohl útočník stále vysílat zprávu „alarm vypnut“. Čítače jsou důležité pro šifrování LoRa. Šifrování probíhá tak, že existuje generátor keystreamu a mezi ním a šifrovaným textem proběhne logická operace XOR, a tím se vygeneruje šifrovaný text.

Problém nastává, pokud se čítače neinkrementují, tak se pro všechny zprávy používá stejný keystream. Pokud byl zašifrovaný text použit dvakrát a útočník zná tento text, může vypočítat původní text ostatních zpráv, které používají tentýž keystream [45].

Prevence

Největším problémem v bezpečnosti je stále lidský faktor, a proto je důležité dbát na prevenci, především v podnikových sítích.

- Dodržování protokolů a standardů. Využívat maximálně zabezpečení které poskytuje LoRaWAN (MIC, šifrování a dešifrování) a hlavně využívat OTAA.
- Při používání senzorů pro změnu stavu důležité volit náhodné zprávy mezi pravými zprávami a také mít fixní délku payloadu, vzhledem k tomu že z délky lze zjistit o jaký stav se jedná, například při zvýšení teploty bude delší payload.
- Náhodné klíče by neměly být umístěny na jednom místě, například uloženy na serveru, aby se k těmto klíčům nedalo dostat skrz pracoviště zaměstnance.
- Kontrola ostatních provozovaných řešení pod jedním hostitelem, aby nebylo možno zaútočit na hostitele skrz jiné řešení, a tím se dostat k informacím LoRaWAN.
- Při fyzické instalaci využívat dobré vnější zabezpečení a přidat pohybový senzor.

LoRaWAN zaručuje ochranu, která chrání společnosti a uživatele, ale hlavní bezpečnost celé sítě závisí na samotných vývojářích pro LoRaWAN řešení.

Shrnutí zabezpečení

LoRaWAN umožňuje vytvořit poměrně bezpečné řešení, které chrání jak koncové zákazníky tak poskytující firmu před kybernetickými útoky. Mělo by být ale jasné, že LoRaWAN celkově nezaručuje bezpečnost a měla by být síť navrhována s přihlédnutím na možnost útoku. Důležitým aspektem je samotné úložiště klíčů, které by mělo být co nejvíce zabezpečené. Je také těžké zabezpečit všechny koncové zařízení a u LoRaWAN se počítá s velkým množstvím, proto se na tuto věc musí brát ohled při plánování samotné sítě. Pro bezpečnost celé sítě je důležité volit náhodné generování klíčů, nejlépe nové klíče posílat pomocí druhého pásma a to jinou technologií (například Bluetooth). Při použití senzorů pro změnu stavu, používat náhodné zprávy mezi pravými zprávami a používat fixní délku payloadu. Důležité je používat všechny bezpečnostní prvky, které poskytuje LoRaWAN jako MIC, šifrování a dešifrování nebo také použít asymetrické šifrování nad samotným protokolem LoRaWAN.

5 ANALÝZA PRODUKTŮ LORAWAN

Pro vybudování sítě na technologii LoRaWAN musí být zvoleny určité prvky této sítě pro její správný chod. Jsou to prvky jako moduly, koncová zařízení, senzory, gateway a cloudy. Analýza jednotlivých prvků byla prováděna v listopadu 2016.

5.1 Komunikační moduly a koncová zařízení

Moduly

Jedná se o moduly od různých firem pracující s modulací LoRa, tyto moduly musí být v každém koncovém zařízení pro správnou komunikaci s bránou a celkově pro správnou funkčnost LoRaWAN sítě. Díky samotným modulům je možné poskládat vlastní zařízení, za použití Arduina nebo samotných AVR procesorů a přidáním požadovaného senzoru. Parametry modulů jsou porovnány v 5.1. Z této tabulky vyplývá, že nejvhodnějším modulem, díky své spotřebě energie a ceně je modul RN2483 od firmy Microchip

Tab. 5.1: Parametry modulů.

	Výrobce	Pásmo	Vzdálenost zástavba/mimo	Útlum (přijímač)	Max. spotřeba (3.3V) Tx/sleep/idle/Rx (mA)	Výkon	Cena	Tepelné podmínky	Zdroj
RN2483	Microchip	433/868 MHz	5 km/15 km	-148 dBm	40 / 0,0099 / 2,8 / 14,2	14 dBm	14.27 $	-40°C–80°C	[46]
MTDOT-868	Multitech	868 MHz	2 km/16 km	-137 dBm	41 / 0,04 / 32 / -	14 dBm	30 $	-40°C–85°C	[47]
LL-RLP-20	Link Labs	868/915 MHz	2 km/15 km	-137 dBm	122 / 0,01/ - / 10	18 dBm	102 $	-20°C–70°C	[48]
LO868-25MW	Adeunis	868 MHz	2 km/15 km	-140 dBm	80 /0,01/ - / 24	14 dBm	–	-40°C–85°C	[49]
IM880A-L LORA	IMST GmbH	868 MHz	2 km/15 km	-137 dBm	126 /0,01/ 5 / 11.2	14 dBm	–	-40°C–85°C	[50]

Vývojové kity

Jsou to již hotová řešení, vytvářená pro testování a vývoj aplikací. Do těchto vývojových kitů lze lehce připojit různé senzory, které již bývají obsahem balení tohoto kitu, usnadňuje to vytváření a připojování vlastních senzorů a dalších komponent. Tyto vývojové kity bývají často postaveny na mikropočítačích jako Arduino nebo Raspberry Pi. Pro příklad jsou zde tyto kity.

LORA™ RAPID DEVELOPMENT KIT: Vývojový kit od firmy Allthingstalk. Tento kit je postaven na Arduinu a mimo napájení baterií, využívá i solární energii. K tomuto kitu jsou poskytovány senzory pro měření teploty, tlaku, vlhkosti, světla, zvuku dále pak GPS lokátor, akcelerometr, senzor pohybu, magnetický spínač dveří a spínací tlačítko. Cena tohoto vývojového kitu je 299 eur [51].

MTUDK2-ST-MDOT: Vývojový kit od firmy Multitech. Tento kit obsahuje anténu, RSMA kabel, USB kabel. Je tedy lehce připojitelný k notebooku a vhodný k testování, cena 73 $ [52].

Hotová řešení koncových zařízení

Existuje již několik koncových zařízení, pracujících na LoRaWAN technologii. Jsou to například senzory (teplota, pohyb, tlak a další). Koncová zařízení pro kontrolu osvětlení. Různé smart měřiče v oblasti energetiky a vody. Pro vyzkoušení technologie LoRaWAN slouží demonstrátory, jsou to koncová zařízení, která v sobě mají několik senzorů a jsou připraveny pro komunikaci s LoRaWAN sítí. Díky modulům LoRa lze vytvořit i vlastní koncová zařízení přímo na míru uživatele. Zde jsou uvedeny některé tyto koncové zařízení, rozřazeny podle firem které je poskytují.

Flashnet: Poskytuje řešení pro inteligentní osvětlení inteliLIGHT. Zde je jako koncové zařízení použito LoRa RF FRE-220. Je to zařízení kompatibilní s LoRaWAN třídou A a C. Toto zařízení slouží k monitoringu a ovládání pouličního osvětlení. Lze díky němu efektivně ovládat lampy (zapínat ve vhodnou dobu na správném místě), díky tomu se ušetří spousta energie, dále díky monitoringu v reálném čase lze jednoduše detekovat poruchu, z toho plyne velké zlepšení údržby. Spotřeba tohoto zařízení je 0,5 W. Využívá stupeň krytí IP 66. Měří tyto parametry – výkon lampy, napětí, proud, činný výkon, zdánlivý výkon, jalový výkon, účiník, spotřebu energie (v aktivním i neaktivním stavu), čas běhu lampy a počet zapnutí a vypnutí lampy. Upozorňuje na přepětí, nadproud, poruchu lampy nebo poruchu samotného zařízení [53].

Abeeway: Vytváří koncové zařízení Master Tracker 38, které odesílá informace o současné pozici a je uzpůsobeno k monitoringu věcí a vozidel (velmi dobré k ochraně proti krádeži). Toto zařízení zajišťuje taktéž detekci pohybu, měření teploty, stupeň ochrany IP 67. Výdrž baterie závisí na režimu použití, při šesti vysílání po dobu patnácti minut za den vydrží 5 let a při udání GPS lokace jednou za hodinu výdrž až 8 let. Využívá baterii Li-SoCl2 s 38 Ah. Pracuje na frekvenci 868 MHz a spotřeba zařízení je maximálně 40 mA. Lze použít i druhou variantu Master Tracker 8 hlavní rozdíl je v použité baterii Li-SoCl2 s 8 Ah, výdrž baterie je tedy maximálně 2 roky [54].

Nke WATTECO: Specializuje se na výrobu několika druhů senzorů. Jsou to senzory TIC (pro detekci radiového signálu), pulzní senzory, senzory pro teplotu a vlhkost, senzory pro měření vody a další. Přiblížil bych tu zařízení Smart Plug je to zástrčka do zásuvky pro 230 V, která umožňuje zapojit do LoRa sítě i zařízení, která nejsou „smart“ jako pračky, myčky a další. Umožňuje zapínat a vypínat přívod energie pomocí LoRa technologie, dokáže i měřit spotřebu energie. Dalším zařízením je Temperature/Humidity senzor využívající solární energii (denně kolem 200 luxů), komunikuje na frekvenci 868 MHz. Měří teplotu v rozmezí -40°C – 120°C a vlhkost v rozmezí 0–100 % [55].

Adeunis RF : Firma se specializuje hlavně na testovací zařízení a demonstrátory pro LoRaWAN. Prvním zařízením je Demonstrator LoRaWAN zařízení, které je připraveno k okamžitému připojení do sítě LoRaWAN. Má v sobě zabudovány tři typy senzorů a to GPS, akcelerometr a teploměr. Parametry – dosah až 15 km, výkon 25 mW, útlum -140 dBm, frekvence 868 MHz, baterie 2000 mAh, spotřeba při vysílání 48 mA (14 dBm). Využívá modul Adeunis RF Lo868. Může pracovat jako zařízení třídy A nebo C, jeho cena se pohybuje kolem 178 eur [56].

Druhé zařízení je FIELD TEST DEVICE LoRaWAN toto zřízení má naprosto stejné parametry jako demonstrátor, ale navíc je obohaceno LCD displejem. Výdrž baterie je kolem 10 hodin [57].

SolidusTech: Česká firma, vytvářející koncové zařízení pro IoT, pracující s technologiemi LoRaWAN a SigFox. Firma má výběr z několika zařízení jako je LoRa Tester který zobrazuje hodnoty SNR a RSSI, má nastavitelný sleep mode, SF a ADR. Mají další zařízení různých senzorických typů jako je odečet pro vodoměry nebo teploměr vhodný pro potravinářský průmysl. Dále vyvíjí senzorická zařízení LoRaWAN INDOOR UNI který měří teplotu a vlhkost, sleduje stav kontaktu a má integrovaný čítač impulsů a také outdoorový LoRaWAN čítač impulsů. Tyto dvě zařízení jsou testovány i ve firmě E.ON pro zapojení do chytrých energetických sítí (smart grid) [58].

Je velký počet výrobců koncových zařízení pracující s technologií LoRaWAN, nová zařízení jsou stále vytvářena a tak je velký výběr a možnost volby. Z tohoto popisu vycházejí, jako nejvhodnější zařízení pro testování LoRaWAN sítě, zařízení od firmy Adeunis RF. Jako testovací zařízení lze použít též vývojové kity, které umožňují ještě více možností, ale demonstrátor od firmy Adeunis RF je dostatečně vyhovujícím, již hotovým a v některých případech oproti kitům i cenově dostupnější

řešením. K testování v provozu byly také zvoleny zařízení od firmy SolidusTech, testování těchto zařízení umožnila forma E.ON.

5.2 Gateway

Dalšími zařízeními pro běh LoRaWAN sítě jsou brány (gateway). Tyto brány slouží k přenosu dat na síťový server již větší rychlostí určitou technologií například Ethernet, GSM, Wi-fi, LTE a další. Je možno sestavit i vlastní gateway běžící na Raspberry PI a nebo sestavit pomocí jiných vývojových kitů. Jednotlivé brány jsou popsány a srovnány v tabulce 5.2. Z tabulky vyplývá, že díky své ceně, dobrému vysílacímu výkonu a dobrému útlumu, je LORANK 8 vhodným zařízením.

Tab. 5.2: Srovnání parametrů bran.

	Výrobce	**Propojení s páteřní sítí**	**Rozhraní**	**Spotřeba**	**Vysílací výkon**	**Útlum**	**Cena**	**Zdroj**
LL-BS-8	Link Labs	Ethernet, Wi-fi, 3G	USB	10 W	18 dBm	-133 dBm	800 $	[59]
LORANK 8	Ideetron	Ethernet, 4G	SPI	–	27 dBm	-138 dBm	412 €	[60]
Lorrier LR2	Lorrier	Ethernet	SPI	12,4 W	20 dBm	-137 dBm	575 €	[61]
Wirnet Station 868	Kerlink	Ethernet, G3	USB	15 W	28 dBm	-141 dBm	–	[62]

5.3 Cloud

Slouží ke zpracování dat přicházejících z bran a dále předávají již zpracovaná data aplikaci. Zahrnují v sobě i vlastní síťový server.

Loriot Jedná se o švýcarskou firmu. Tento síťový server pokrývá obrovské množství států. Lze si na tomto serveru vytvořit účet zdarma (je k dispozici veřejný cloud), pro připojení jedné brány a deseti koncových zařízení. Podporuje velké množství bran.

Stream technologies Jde o anglickou firmu. Jejich síťový server je kompatibilní s bránami běžícím na protokolu V1 a V2 LoRaWAN. Taktéž pokrytí téměř celého světa. Cena služeb nebyl zveřejněna.

Simfony Rumunská firma cloud je kompatibilní se všemi zařízeními standardu LoRaWAN 1.0. Měsíční poplatek za zařízení je 0.5 eur a za aktivaci každého zařízení 1 euro. Kompatibilní s hardwarem od firem Kerlin, MultiTech a LinkLabs.

5.4 Návrh sítě

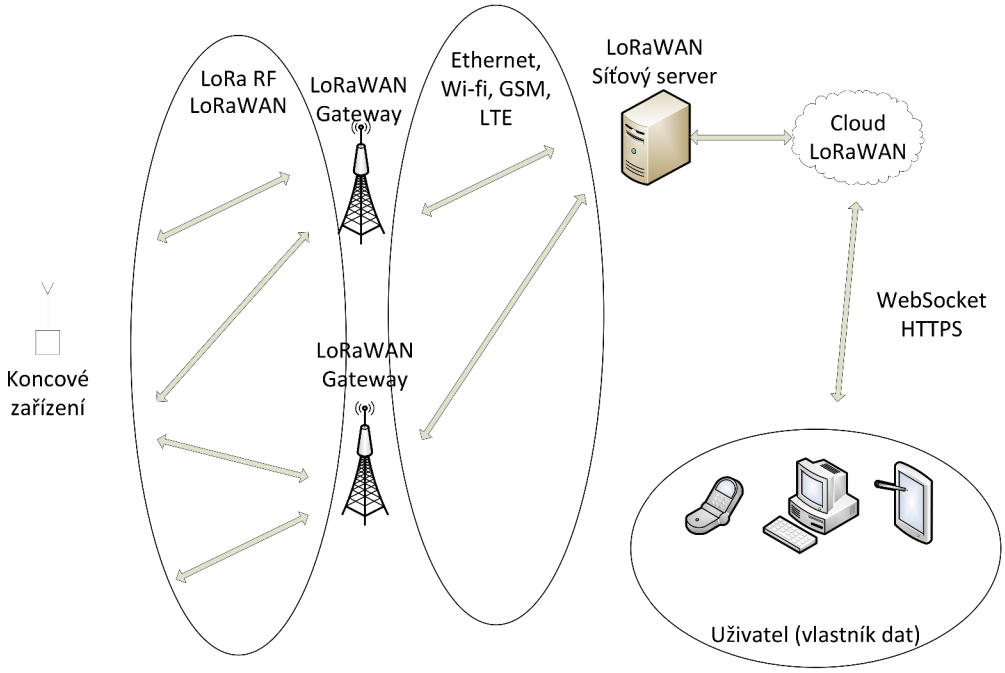
Pro realizování sítě jsou potřeba čtyři prvky a to koncová zařízení, brána, síťový server a aplikace. Je potřeba také všechny prvky aktivovat v samotném cloudu.

Po hardwarové stránce je potřeba koncové zařízení a brána. Koncová zařízení nejsou napevno připojena k jedné bráně ale ke všem branám v dosahu – všechny brány v dosahu zařízení obdrží zprávu. Brána předává dále signál do síťové služby, kde je zpracován. Pro hardwarové řešení bylo zvoleno jako koncové zařízení, zařízení Demonstrator LoRaWAN od firmy Adeunis RF, vzhledem ke svému multifunkčnímu využití je pro test velmi vhodné. Toto zařízení používá modul LO868-25MW od stejné firmy. Pro testování byly také dostupné koncové zařízení od firmy SolidusTech využívající modul od RN2483 od firmy Microchip. Jako gateway bylo zvoleno zařízení LORANK 8 z důvodu jeho nižší ceny a hlavně kvůli rozhraní SPI, které je rychlejší a potřebuje menší počet vodičů. Tato gateway byla zvolena i z důvodu podporované komunikace se síťovým serverem.

Síťový servis likviduje duplicitní pakety (které právě byli přijaty z jednoho zařízení na dvě brány). Dešifruje zprávu a zpracuje podle protokolu a předává dekódovaná data aplikaci. Díky tomu jsou přístupna koncová data uživateli v různě zvolených formátech podle samotného cloudu. Jako síťový server a cloud byl zvolen server od firmy Loriot vzhledem k jeho velké dostupnosti a možnému připojení zdarma až deseti zařízení na jednu bránu.

6 VYTVOŘENÍ SÍTĚ A OVĚŘENÍ FUNKČNOSTI

Zde je popsáno jak probíhal návrh a vytvoření sítě na technologii LoRaWAN, dále je zde popsáno ověření funkčnosti, spolehlivosti a limitů celé této sítě.



Obr. 6.1: Architektura LoRaWAN sítě.

6.1 Použitá zařízení

Pro sestavení sítě byly vzhledem k návrhu viz Obr. 6.1 potřeba zařízení typu koncové zařízení, gateway, cloud a další zařízení sloužící pro konfiguraci.

6.1.1 Senzory od firmy SolidusTech

Jako koncové zařízení byly použity dva senzory od firmy SolidusTech a to senzor LoRaWAN INDOOR UNI [63] a outdoorový LoRaWAN čítač impulsů [64]. Katalogové parametry jsou v tabulce Tab. 6.1. Tato zařízení byla použita ve dvou měřeních. U těchto senzorů byl ověřen i odběr energie a byla spočítána reálná výdrž při těchto odběrech.

Tab. 6.1: Specifické hodnoty čidel [63],[64].

	Senzor OUTDOOR	**Senzor INDOOR**
Stupeň krytí	IP 65	IP 20
Napájení	3,6 V Lithiová AA baterie 2400mA	3,6 V Lithiová AA baterie 2400mA
Odběr ve stavu sleep	20 μA	50 μA
Průměrný odběr při odesílání 2x denně	100 μA	100 μA
Provozní teplota	-20 °C až + 85 °C	-10 °C až + 85 °C
Anténí konektor	SMA	SMA
Konfigurovatelné parametry	četnost komunikace počet opakování vysílání spreading factor potvrzené/nepotvrzené vysílání uživatelské parametry přídavné krytování AES256	četnost komunikace počet opakování vysílání uživatelské parametry přídavné krytování AES256

Měření odběru energie

Vzhledem k ověření skutečného odběru energie čidel, bylo nutno změřit odběr energie u obou senzorů a porovnat s katalogovými hodnotami. Měření probíhalo dvěma způsoby Indoorové čidlo bylo proměřeno pomocí přístroje Keysight N6705B a hodnoty byly zpracovány v softwaru Keysight 14585A [65] a také na multimetru Agillent 34410A. Outdoorový senzor byl proměřen pouze na multimetru Agillent 34410A.

Měření Indoor senzoru Senzor byl měřen nejdříve pomocí přístroje Keysight N6705B a hodnoty byly zpracovány pomocí softwaru Keysight 14585A. Do tohoto programu byly načteny hodnoty z měření, které probíhalo 10 minut a každou minutu zařízení odeslalo zprávu, hodnoty lze vidět na obrázku Obr. 6.2. Pomocí kurzorů byl zjištěn průměrný odběr energie vždy v určitém režimu. Důležité režimy jsou tři a to odběr energie při startu (po připojení napájení senzoru), odběr v době sleep (senzor je ve stavu spánku a neodesílá žádná data) a v době odesílání. Hodnoty jsou v tabulce Tab. 6.2.

V tabulce jsou popsány naměřené hodnoty a výpočty doby výdrže baterie v senzoru při různém odesílání dat.

Tab. 6.2: Hodnoty Indoorového čidla.

	Hodnota	**čas**
Spotřeba při startu	13,0954 mA	37 s
Spotřeba při vysílání	17,364 mA	6 s
Odběr ve stavu sleep	36 μA	54 s (při posílání každou minutu)
Průměrný odběr při odesílání 2x denně	38,4 μA	5 let
Průměrný odběr při odesílání 1x za hodinu	64 μA	3 roky
Průměrný odběr při odesílání každých 10 minut	209 μA	0,92 roku

Pro vysílání každou hodinu denně je čidlo ve stavu sleep 3 594 s v tomto stavu je odběr 0,036 mA. Ve stavu vysílání je pouze 6 s a odebírá 17,364 mA. Průměrná hodnota za jednu hodinu je 64 μA. Zde je vzorec pro výpočet výdrže baterie, kde hodnota 0,7 je hodnota pro vnější vlivy na baterii [66].

$$Životnost\,baterie = \frac{Kapacita\,baterie\,v\,mAh}{Spotřeba\,zařízení\,v\,mA} \times 0,7$$

$$Životnost\,baterie = \frac{2400}{0,0649} \times 0,7 = 25886\,h$$

Výdrž baterie při vysílání jedné zprávy za hodinu je $25886 \div 8760 = 2,96$ roku z toho vyplývá, že senzor by měl vydržet téměř 3 roky.

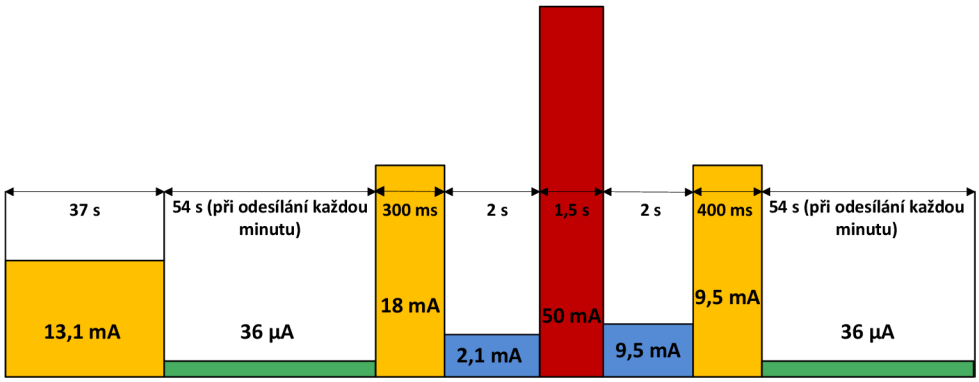
Obr. 6.2: Změřené hodnoty v programu Keysight 14585A.

Měření Outdoor senzor Senzor byl měřen pomocí multimetru Agillent 34410A, proto nejsou hodnoty tak přesné jako u měření indoorového čidla a jsou spíše jen orientační. Na obrázku Obr. 6.5 jde vidět jak měření probíhalo. Výpočet hodnot v tabulce Tab.6.3 probíhal stejně jako u indoorového čidla (vzorec 6.1.1). Hodnoty nejsou tak přesné, jelikož nebylo možno odečíst z multimetru tolik údajů. Pomocí multimetru byly naměřeny hodnoty ve stavu sleep 17,8 μA, ve stavu počátku vysílání 12 mA, při vysílání 39 mA a při ukončení vysílání 12 mA.

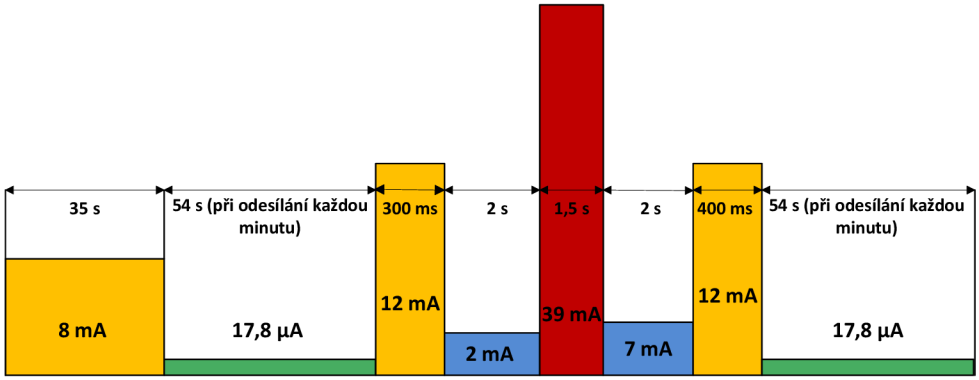
Tab. 6.3: Hodnoty Outdoorového čidla.

	Hodnota	čas
Spotřeba při startu	12 mA	35 s
Spotřeba při vysílání	13,6 mA	6 s
Odběr ve stavu sleep	17,8 μA	54 s (při posílání každou minutu)
Průměrný odběr při odesílání 2x denně	19,7 μA	9 let
Průměrný odběr při odesílání 1x za hodinu	40,4 μA	4,7 roku
Průměrný odběr při odesílání každých 10 minut	154 μA	1,2 roku

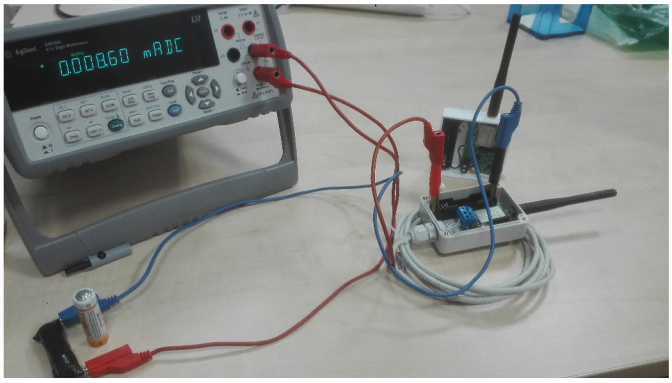
Grafy spotřeby Grafy Obr.6.3 a Obr.6.4 do nichž jsou zanesené naměřené hodnoty. První graf pro indoorový senzor je přesný. Druhý graf pro outdoorové čidlo je vzhledem k měření multimetrem jen orientační.



Obr. 6.3: Graf spotřeby Indoor senzoru.



Obr. 6.4: Graf spotřeby Outdoor senzoru.



Obr. 6.5: Měření pomocí multimetru Agillent 34410A.

6.1.2 Adeunis RF LoRaWAN demonstrator

Zařízení, které je přímo uzpůsobeno k testování sítě LoRaWAN. Zařízení obsahuje napájecí baterii, která je napájena pomocí mini USB kabelu. Nastavení zařízení probíhá pomocí terminálového programu Hercules [67] všechny příkazy pro nastavení jsou psány v ASCII. Zařízení obsahuje tři senzory a to GPS, akcelerometr a senzor teploty. Specifikace zařízení jsou v tabulce Tab. 6.4.

Tab. 6.4: Specifikace demonstratoru.

Specifikace	
Komunikace	LoRaWAN protokol a LoRa Modulace
Nastavení	přes příkazy AT
Radio data rate	Nastavitelné (SF12 - 183 bps až FSK 50 kbps)
UART konfigurace	115,2 kbps/N/8/1
UART port	USB
Frekvenční kanály	pásmo ISM 863–870MHz
RF výstupní výkon	14 dBm (25 mW)
Citlivost	až -140 dBm na SF12/CR4
Vzdálenost	až 15 km
Provozní teplota	-40°C až +85°C
Standardy	EN 300–220, EN 301–489, EN 60950

6.1.3 Lorank-8

Jako gateway bylo zvoleno zařízení Lorank-8 od firmy Ideetron. Toto zařízení zachytává rámce ze všech zařízení, které jsou v jeho dosahu, tyto rámce se filtrují dále na síťovém serveru, kde jsou zahazovány a nebo posílány dále ke zpracování. Toto zařízení je možno konfigurovat pomocí ssh nebo telnetu. Operační systém zařízení je postaven na Linuxu a je použit přímo Debian, konfigurace probíhá v bashi. Zařízení je připojeno do sítě pomocí Ethernetu (je zde možnost přidat i možnost komunikace přes 4G, ale jde o dražší variantu).

Pro přístup na Loriot cloud je potřeba nejdříve zařízení na tento cloud zaregistrovat, a to jednoduše pouze pomocí MAC adresy zařízení. Po té, co je zařízení přidáno na server, je možno přes ssh přímo na bránu z tohoto serveru stáhnout nejnovější aktualizaci softwaru Loriotu na danou bránu a pak už se jen pár příkazy připojit s bránou na Loriot, od této chvíle je možné posílat na vytvořené aplikace, ke kterým jsou registrovány koncová zařízení, data a s těmito daty můžeme dále pracovat. Dále byl na bráně nastaven frekvenční plán EU868 Semtech viz Tab. 6.5.

Zde je ukázka skriptu vytvořeného pro stažení aktualizací a přihlášení do síťového serveru. Skript byl vytvořen pro rychlejší zprovoznění brány viz Výpis 6.1.

Výpis 6.1: Skript pro přihlášení brány na server Loriot.

```
1
2  #!/bin/sh            //hlavička skriptu
3  cd /tmp              //přesunutí do složky tmp
4  wget http://www.loriot.io/home/gwsw/loriot-lorank
5  -8-ic880a-SPI-0-latest.sh   //stáhne shell script z~webu
6  //přidání práva spouštět
7  chmod +x loriot-lorank-8-ic880a-SPI-0-latest.sh
8  ./loriot-lorank-8-ic880a-SPI-0-latest.sh -n   //spustí script
9  cd /opt/lrt            //přesune se do adresáře /opt/lrt
10 ./loriot-gw -f &         //spustí script na pozadí
11 PID=$!               //uloží si pid processu
12 sleep 9              //9 vteřin počká
13 kill $PID            //zruší process
14 cd /tmp              //přesunutí do adresáře /tmp
15 ./loriot-lorank-8-ic880a-SPI-0-latest.sh    //spuštění scriptu
```

Tab. 6.5: Frekvenční plán.

Kanál	**Frekvence**	**Modulace/BW**
0	868.100 MHz	MultiSF 125 kHz
1	868,300 MHz	MultiSF 125 kHz
2	868,500 MHz	MultiSF 125 kHz
3	867,100 MHz	MultiSF 125 kHz
4	867,300 MHz	MultiSF 125 kHz
5	867,500 MHz	MultiSF 125 kHz
6	867,700 MHz	MultiSF 125 kHz
7	867,900 MHz	MultiSF 125 kHz
LoRa	868,300 MHz	SF7 250 kHz
FSK	868,800 MHz	FSK 125 kHz, 50 kbps
RX2 channel (downlink)		
RX2	869,525 MHz	SF12 125 kHz

6.1.4 Loriot

Je veřejný cloud, který zastřešuje privátní síť LoRaWAN jednotlivcům. Poskytuje software pro zpracování data přenesených v této síti a umožňuje s nimi dále pracovat. Loriot podporuje několik rozhraní pro programování aplikací a výstup dat. Jsou to

rozhraní jako WebSocket, HTTP Push, TLS Socket a MQTT. Nejvíce bylo pro přijatá data využíváno rozhraní WebSocket.

WebSocket Protokol, který umožňuje komunikaci na pozadí se serverem, náhrada HTTP vzhledem k rychlosti toku dat (nepotřebuje hlavičky HTTP, komunikace neprobíhá přes HTTP sníží se datový tok). Tento protokol aplikacím umožňuje plně duplexní obousměrnou komunikaci mezi webovým prohlížečem a serverem. Celá specifikace aplikačního protokolu TCP/IP je definována v RFC 6455 [68]. Tento protokol je kompatibilní se stávající infrastrukturou, využívá i portů HTTP (80 a 443), měl by postupně nahrazovat protokol HTTP. Využívám URI schéma ws pro nezabezpečený přenos a wss pro zabezpečený přenos.

Registrace zařízení do cloudu

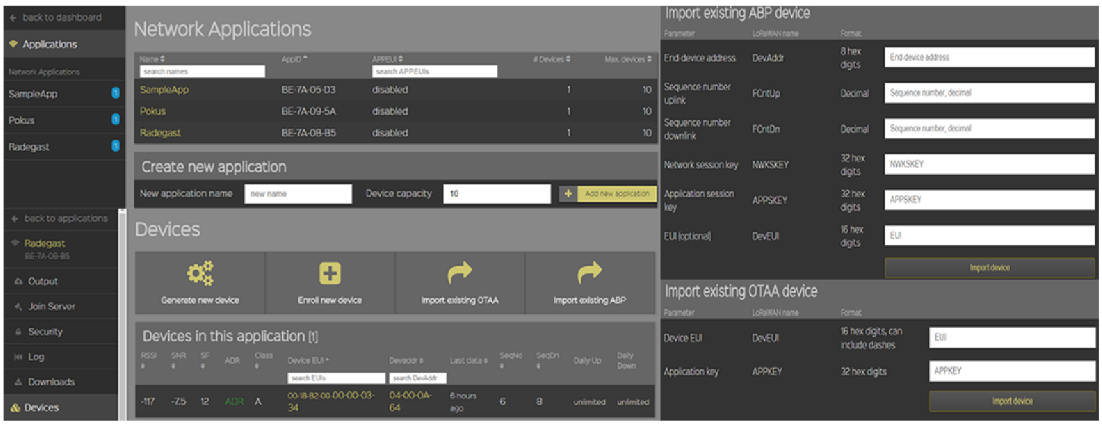
Nejprve je důležité vytvořit vlastní aplikaci, kde se také volí vhodný protokol pro výstup dat, v případě této práce je to vždy WebSocket. Po vytvoření aplikace lze přidávat zařízení, ze kterých budou loriotem zpracovávány data. Zařízení jdou přidávat dvěma způsoby buď pomocí ABP nebo OTAA. Na obrázku Obr. 6.6 lze vidět prostředí Loriot při aktivaci koncového zařízení.

Activation by personalization - (ABP) - Jde o nastavení údajů na čidlo, a poté připojení pomocí těchto údajů k serveru. Jsou to údaje jako DevAddr (8 hexa decimálních znaků), dva klíče NwkSKey a AppSKey, které jsou uloženy přímo v zařízení namísto DevEUI, AppEUI a the AppKey (oba klíče mají 32 hexa decimálních znaků). Popřípadě může být použit i DevEUI, pokud je dostupný (16 hexa decimálních znaků). Klíče by měly být unikátní pro každé zařízení.

Over-the-Air Activation - (OTAA) - Aktivace zařízení při připojení do sítě a nebo restartu zařízení. Koncová zařízení vždy při výpadku musí projít novým procesem aktivace OTAA. Aktivace touto metodou vyžaduje před aktivací zařízení, aby obsahovalo DevEUI (jedinečný celosvětový identifikátor zařízení), identifikátor aplikace (AppEUI) a klíč AES-128 (AppKey).

6.2 Zpracování dat

Všechna data z měření byla zpracována pomocí programu Microsoft Excel. U všech přenesených dat byl vždy timestamp (unixový čas) a díky němu byla data identifikována. Data lze stáhnout z cloudu Loriot jako csv nebo json. Na obrázku je ukázka jak data vypadají přímo v aplikaci cloudu Obr. 6.7. Po stažení dat ve formátu csv,



Obr. 6.6: Ukázka prostředí Loriot.

bylo nutno převést timestamp na datum a čas. Pro identifikaci při měření v terénu byla použita aplikace Geo Tracker [69], pomocí ní bylo zjištěno přesné místo měření v daných oblastech. V Excelu byly SNR (Signal-to-noise ratio), což je odstup signálu od šumu a RSSI (Received Signal Strength Indication), to je síla signálu, zprůměrovány a jejich finální podoba je vidět u každého měření v práci.

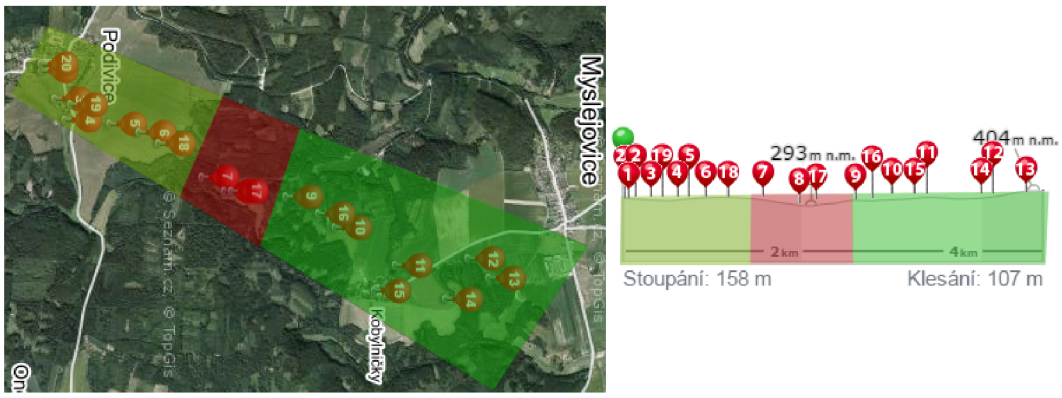
Obr. 6.7: Ukázka výpisu dat brány.

6.3 Experimentální měření a jeho ověření

Měření bylo provedeno mezi vesnicí Podivice, kde se na střeše domu nacházel přijímač gateway Lorank 8 a vesnicí Kobylničky, u které se nacházel nejvyšší a nejvzdálenější bod. K měření byl použit outdoorový senzor SolidusTech [64], na kterém byla nastavena doba odesílání dat po 10 minutách a činitel rozprostření SF=12. Data se zpracovávala na síťovém serveru Loriot. Měření probíhalo na nelicencované frek-venci 868 MHz na třech kanálech a to 868,100 MHz, 868,300 MHz a 868,500 MHz.

Měřena byla síla signálu (RSSI), která má pro tuto technologii prahovou hodnotu -120 dB a odstup signálu od šumu (SNR), jehož prahová hodnota je -10 dB.

Na obrázku Obr. 6.8 lze vidět mapu, kde je umístěna gateway na stejném místě jako poslední měření (bod 20), v tomto bodě byla brána umístěna ve výšce 358 m nad mořem. Poslední bod byl měřen ve vzdálenosti 4406 m a ve výšce 406 m nad mořem. Měření bylo rozděleno do tří oblastí.



Obr. 6.8: Ukázka ztrátovosti rámců a oblast převýšení.

V první oblasti (žlutozelené), která se nachází nejblíže, lze vidět poměrně nízkou ztrátovost (byly ztraceny 3 rámce z 9), dalším měřením bylo zjištěno že za tuto ztrátovost může odesílání vlastních dat brány Lorank-8, při odesílání brány jsou všechny ostatní data zahazována.

Ve druhé oblasti byly ztraceny všechny pakety, toto bylo zapříčiněno jak vlastním odesíláním dat, tak jak je vidět z převýšení, odesílání rámců probíhalo v nížině uprostřed lesa, zde byly hodnoty šumu největší a signál byl slabý, hodnoty k porovnání jsou vidět v ověřovacích měřeních.

Třetí oblast začínající ve vzdálenosti 2470 m od přijímače byla beze ztrát rámců i přesto, že měření neproběhlo na přímou viditelnost.

V tabulce Tab. 6.9 lze vidět všechny naměřené hodnoty a lze z ní vyčíst, v kterých oblastech byly tyto hodnoty naměřeny v závislosti na obrázku Obr. 6.8.

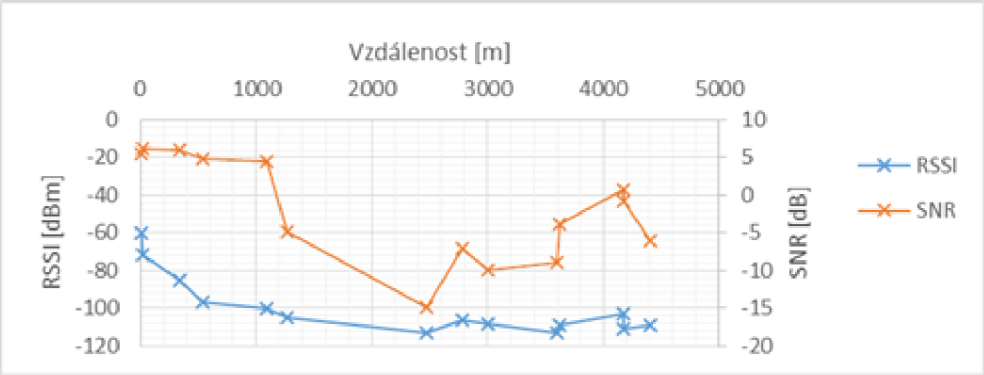
V tomto experimentálním měření se vyskytl problém s nadměrnou ztrátovostí rámců, bylo zjištěno, že za tento problém může odesílání vlastních dat brány i přesto, že bylo zakázáno. Tento problém byl vyřešen a v dalších měřeních se již nevyskytuje, proto zde bylo toto měření ještě ověřeno.

V grafu Obr. 6.10 je vidět, jak se zvětšující se vzdáleností slábne síla signálu (RSSI). Dále je vidět, jak se mění odstup signálu od šumu (SNR) podle oblasti měření, nejnižší hodnoty byly naměřeny v oblasti kolem 2500–3500 m, kde měření probíhalo v lese při stoupání z nejnižšího bodu.

#	RSSI (dBm)	SNR (dB)	Vzdálenost (m)
1	-72	6,2	23
2			62
3	-85	6	340
4	-97	4,8	536
5			810
6	-100	4,5	1096
7			1850
8			2000
9	-113	-14,8	2470
10	-108	-10	3000

#	RSSI (dBm)	SNR (dB)	Vzdálenost (m)
11	-109	-3,8	3615
12	-111	-0,8	4175
13	-109	-6	4406
14	-103	0,8	4172
15	-113	-9	3596
16	-106	-7	2784
17			2043
18	-105	-4,8	1263
19			480
20	-60	5,5	10

Obr. 6.9: Hodnoty měření rozděleny do jednotlivých oblastí.



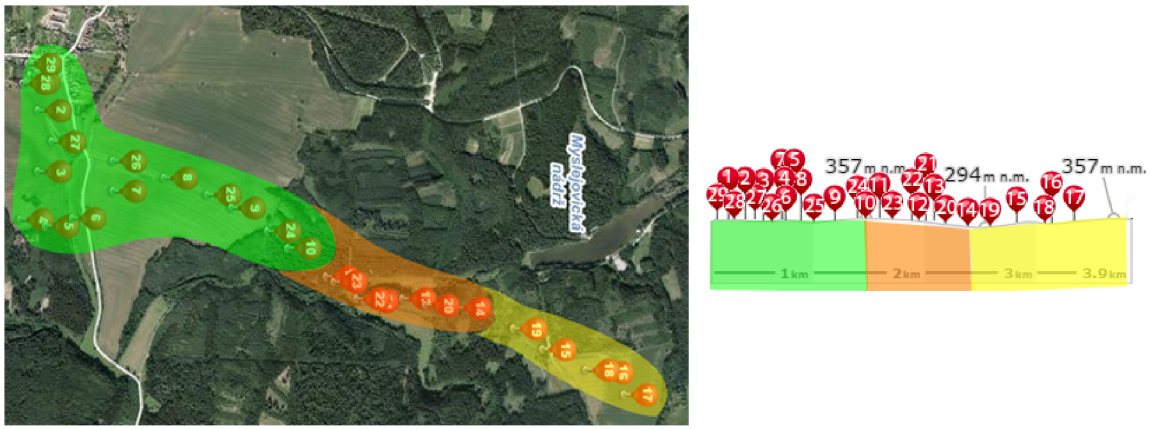
Obr. 6.10: Graf závislosti SNR a RSSI na vzdálenosti.

6.3.1 Ověření měření po opravě

Po zjištění příčiny velké ztrátovosti, byla tato anomálie opravena a bylo provedeno nové měření se stejným zařízením, ale tentokrát bylo odesílání rámců nastaveno na 5 minut. Byla zvolena stejná trasa pro ověření správnosti, ale bylo změřeno více hodnot. Tentokrát lze vidět na obrázku Obr. 6.11 barevně zvýrazněné oblasti síly signálu RSSI, kdy v nížině jak se dalo předpokládat z předchozího měření je nejměnší síla signálu (RSSI) a nízký odstup signálu od šumu.

Při měření tentokrát byla minimální ztrátovost, jak je vidět v tabulce Tab. 6.11. Byl ztracen pouze jeden paket z 28, a to právě v nejníže položeném místě uprostřed lesa.

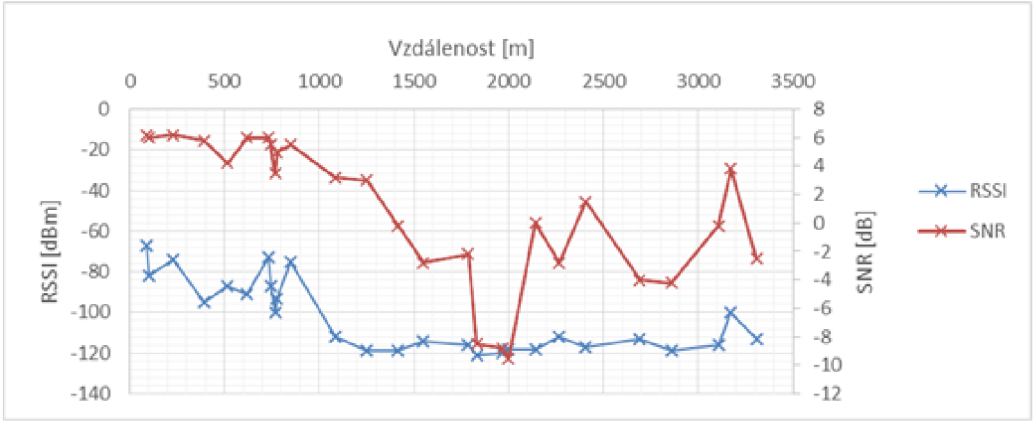
Pro porovnání je zde znovu graf závislost SNR a RSSI na vzdálenosti Obr. 6.12. Lze vidět, že hodnoty jsou podobné jako u předchozího měření.



Obr. 6.11: Hodnoty měření rozděleny podle síly RSSI.

Tab. 6.6: Hodnoty druhého měření.

#	RSSI (dBm)	SNR (dB)	Vzdálenost (m)	#	RSSI (dBm)	SNR (dB)	Vzdálenost (m)
1	-67	6,2	92	15	-119	-4.2	2858
2	-74	6.2	226	16	-100	3.8	3172
3	-87	4.2	516	17	-113	-2.5	3310
4	-87	5.5	745	18	-116	-0.2	3108
5	-93	5	776	19	-113	-4	2691
6	-100	3.5	769	20	-112	-2.8	2265
7	-73	6	734	21	-118	-9.5	2000
8	-75	5.5	851	22	-120	-8.8	1965
9	-119	3	1252	23	-121	-8.5	1831
10	-114	-2.8	1548	24	-119	-0.2	1417
11	-116	-2.2	1787	25	-112	3.2	1083
12	LOST FRAME	LOST FRAME	1996	26	-91	6	619
13	-118	0	2143	27	-95	5.8	391
14	-117	1.5	2406	28	-82	6	100

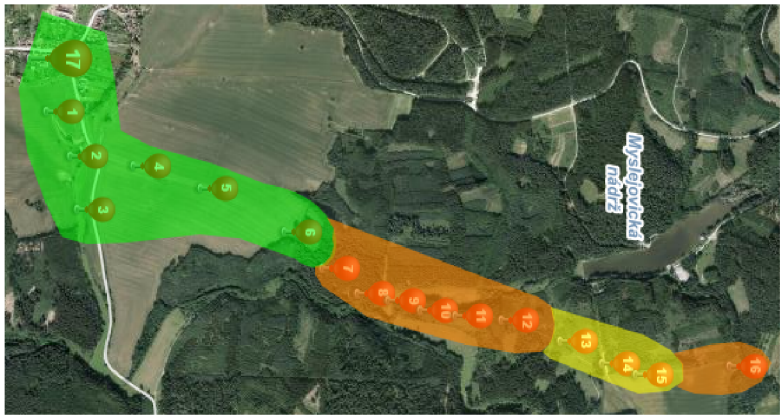


Obr. 6.12: Graf závislosti SNR a RSSI na vzdálenosti.

6.3.2 Ověření pomocí demonstrátoru Adeunis

Pro nejpřesnější proměření této oblasti bylo použito koncové zařízení přímo k testování těchto parametrů. Tentokrát bylo každé místo proměřeno pětkrát a z těchto

dat byla vypočtena průměrná hodnota jak RSSI tak SNR. Na obrázku Obr. 6.13 je tentokrát ukázán odstup signálu od šumu (SNR). V tabulce Tab. 6.7 jsou průměrné hodnoty z pěti naměřených hodnot.

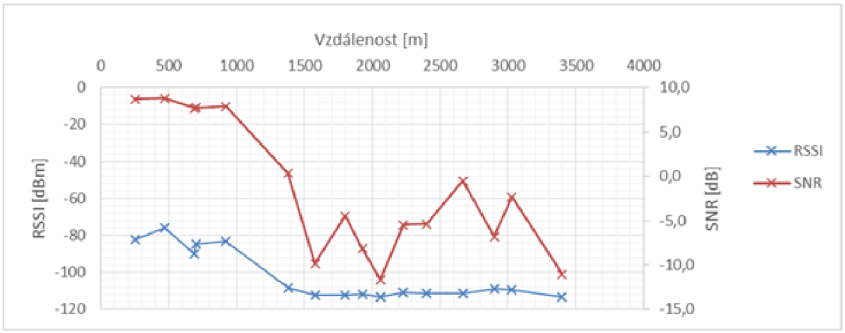


Obr. 6.13: Pokrytí v závislosti na SNR.

Tab. 6.7: Hodnoty třetího měření.

#	RSSI (dBm)	SNR (dB)	Vzdálenost (m)	#	RSSI (dBm)	SNR (dB)	Vzdálenost (m)
1	-82.4	8.68	250	9	-112	-8.16	1930
2	-76	8.7	470	10	-113	-11.64	2060
3	-90	7.68	690	11	-111	-5.46	2230
4	-85	7.74	700	12	-111	-5.4	2400
5	-83	7.88	920	13	-111	-0.54	2670
6	-109	0.3	1380	14	-109	-6.7	2900
7	-112	-9.8	1580	15	-110	-2.3	3030
8	-112	-4.4	1800	16	-113	-11	3400

Hodnoty jsou nejpřesnější ze všech tří měření, přenos byl naprosto beze ztrát rámců. Graf Obr. 6.14 je tentokrát přesnější díky více naměřeným hodnotám.



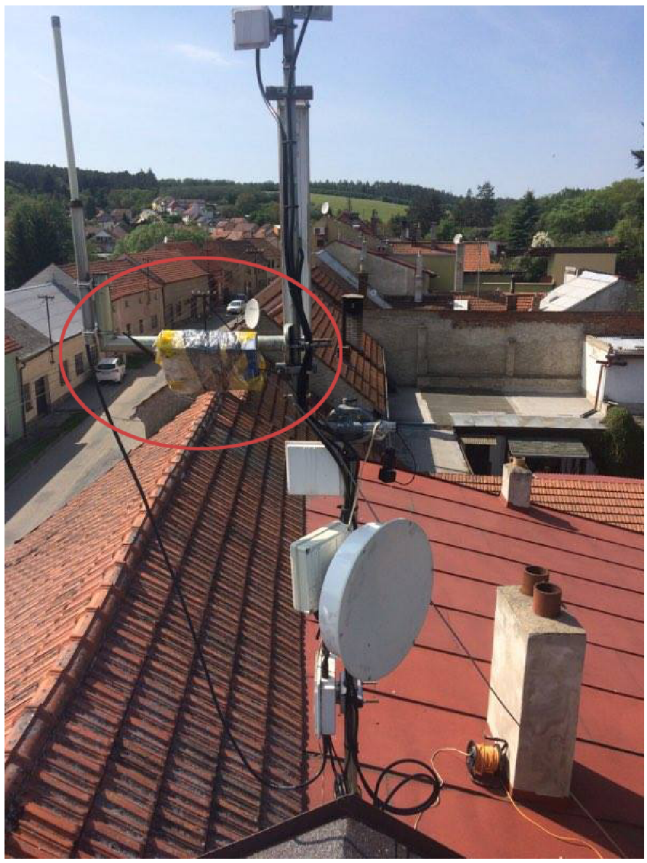
Obr. 6.14: Graf závislosti SNR a RSSI na vzdálenosti.

Tímto měřením bylo ukázáno že LPWAN technologie LoRaWAN může komunikovat i v různých terénních podmínkách velice dobře. Byla zde prokázána velmi

dobrá penetrace skrz zalesněnou oblast a to tak, že nakonec přenos probíhal beze ztrát.

6.4 Měření dosahu při umístění brány ve vesnici

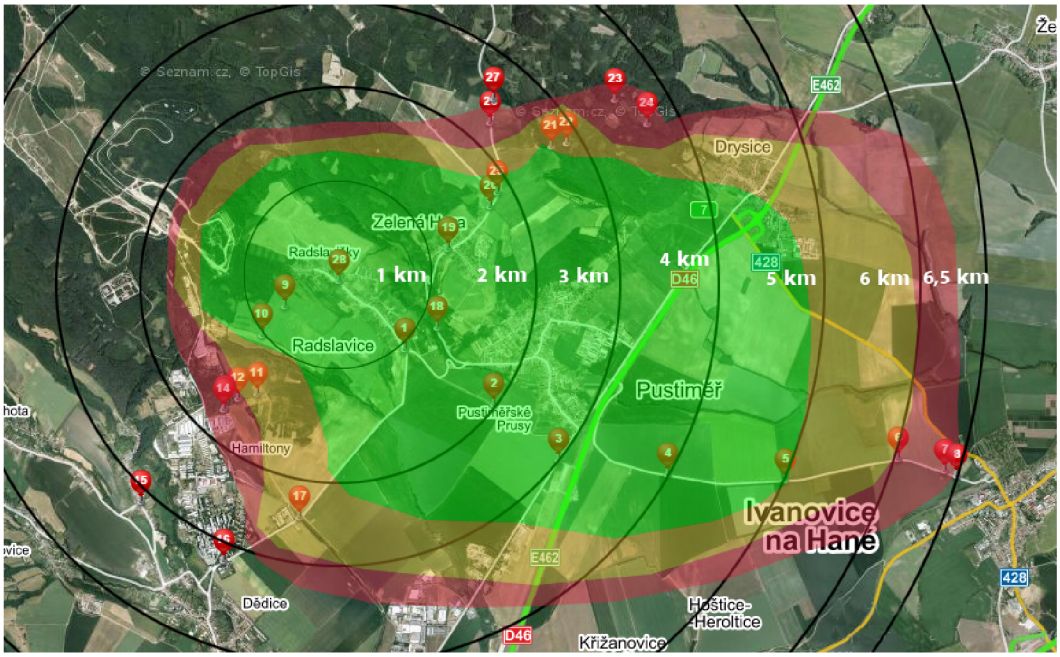
V okolí vesnice Radslavice bylo provedeno měření celkového dosahu sítě LoRaWAN. Brána byla umístěna na domě v této vesnici a to přímo na anténní stožár, umístění lze vidět na obrázku Obr. 6.15. K odesílání byl použit opět LoRaWAN demonstrátor od firmy Adeunis RF. Měření probíhalo tak, že se zvolili vzdáleností měření a po té se ověřoval dosah. Vzdálenost byla zvolena vždy po jednom km. Při začátku ztrátovosti dat se rozmezí vzdáleností snižovalo, optimálně tak, aby byla nalezena hranice, kde je ještě schopno zařízení odesílat bez ztrátovosti. Na každém místě bylo vždy proměřeno 5 hodnot a z nich byl spočten průměr.



Obr. 6.15: Umístění brány při měření.

Na obrázku Obr. 6.16 je možno vidět, že probíhalo měření na 27 bodech, z těchto bodů byla zjišťována průměrná síla signálu RSSI a průměrný odstup signálu od šumu SNR. Zelená oblast na mapě pokrývá bezproblémové odesílání, kde byly hodnoty

RSSI kolem -110 dBm a hlavně SNR -10 dB. Žlutá oblast zobrazuje již horší hodnoty RSSI do -120 dBm a SNR méně než -10 dB. Červená oblast zobrazuje již místa, kde začla ztrátovost rámců, ale stále ještě některé byly odeslány.



Obr. 6.16: Odesílání rámců v rámci oblastí.

Špatné hodnoty pokrytí levé strany obrázku jsou nejspíše zapříčiněny vojenským objektem, který začíná právě u bodu měření 14. Nejspíše je v této oblasti rušení a proto takové zhoršení odesílání a ztráta rámců. Měření bylo testováno i dále za vojenským objektem (bod měření 15), ale toto místo je navíc hodně pod úrovní přijímače a tedy vysílání probíhalo pod velkým kopcem. V tabulce Tab. 6.8 jdou vidět průměrné hodnoty z každého měřeného bodu.

Tab. 6.8: Hodnoty měření v okolí vesnice.

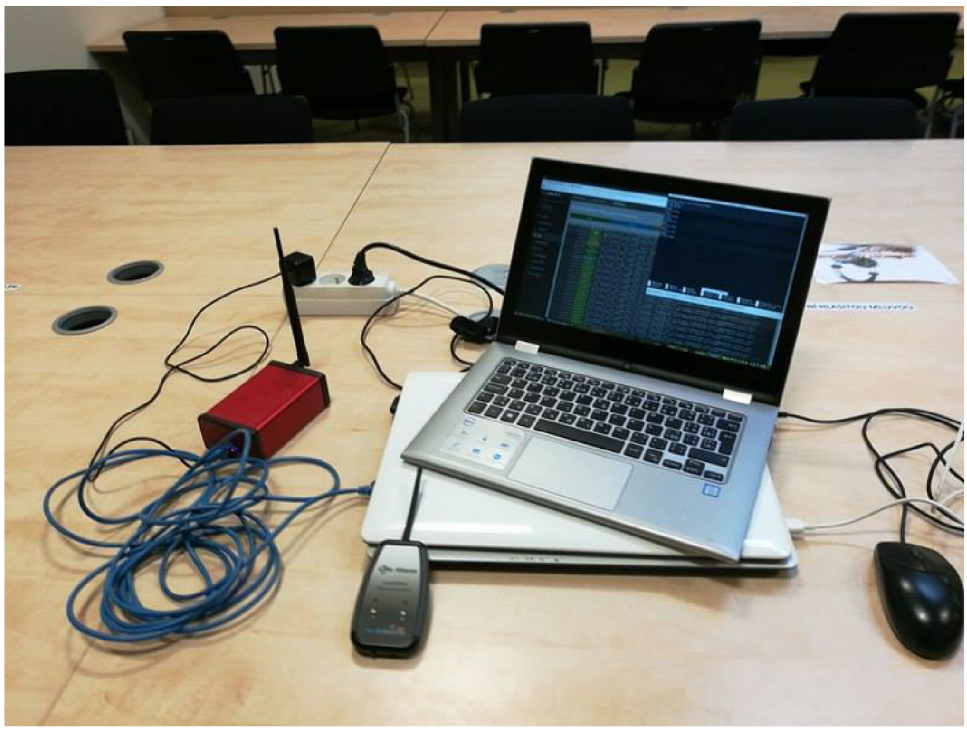
#	RSSI (dBm)	SNR (dB)	Vzdálenost (m)	#	RSSI (dBm)	SNR (dB)	Vzdálenost (m)
1	-102	4.8	1000	15	TOTAL LOST	TOTAL LOST	3100
2	-99	6.2	2000	16	TOTAL LOST	TOTAL LOST	3240
3	-95	7	3000	17	-115	-11.1	2500
4	-106	2.6	4000	18	-116	-9.6	1150
5	-110	-4.3	5000	19	-110	0.3	1200
6	-113	-12.6	6000	20	-113	-8	1750
7	-120	-20	6400	21	-114	-11.3	2580
8	TOTAL LOST	TOTAL LOST	6500	22	-114	-16.5	2730
9	-108	0.6	600	23	-120	-20	3430
10	-116	-14.8	1000	24	TOTAL LOST	TOTAL LOST	3570
11	-115	-16.8	1500	25	-114	-15.3	1900
12	-114	-15.1	1600	26	-120	-20	2290
13	-120	-20	1740	27	TOTAL LOST	TOTAL LOST	2450
14	TOTAL LOST	TOTAL LOST	1800				

Měřením bylo ověřeno, že technologie v dobrých podmínkách dokáže komunikovat až na vzdálenost 6 km. Problém při komunikaci přichází při příliš velkém množství, překážek a také v místech vysílání, které jsou příliš pod úrovní brány. Celkově má komunikace dobré výsledky, když se vezme v potaz, že měření neprobíhalo na přímou viditelnost. Při měření se v cestě nacházelo spousta překážek a i přesto byly rámce odeslány. Odesílání probíhalo na 7 kanálech (868.100, 868.300, 868.500, 867.100, 867.300, 867.500, 867.700, 867.900 MHz).

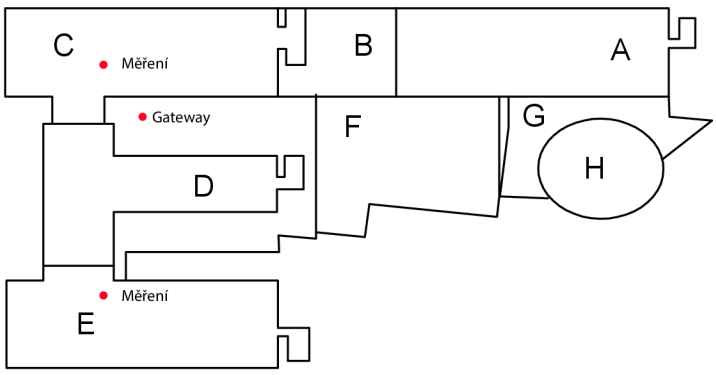
6.5 Měření penetrace skrz patra v budově T12 na FEKTU

V budově T12 FEKTu bylo provedeno měření penetrace mezi patry, aby byl zjištěn dosah signálu v této budově. Při měření byla umístěna brána v knihovně v budově T12. V budově nebylo možno se napojit na ethernet (jediný možný způsob pro připojení brány do internetu, lze za příplatek bránu ještě upravit i na připojení pomocí 4G) a bylo tedy nutno použít více zařízení ke zprovoznění tohoto vysílání, jak lze vidět na obrázku Obr. 6.17, je tedy vidět umístění brány v knihovně, dále použitý notebook pro přemostění mobilních dat na ethernet, aby bylo možné připojit bránu k internetu pomocí ethernetu. Po zprovoznění brány, bylo započato vlastní měření.

Měření probíhalo tak, že se měřilo ve dvou částech budovy a to v části E, která byla dál od knihovny a v části C, ta je blíže ke knihovně. Proměřilo se každé patro budovy a na každém patře bylo změřeno 10 hodnot. Umístění brány a také oblasti měření lze vidět na obrázku Obr. 6.18. Z měřených hodnot byl vypočten průměr a podle hodnot Tab. 6.9, kde je vidět, že síla signálu byla v celém měření velmi dobrá, byl signál zakreslen podle SNR do obrázku Obr. 6.19. Kde zelená barva reprezentuje SNR od 0 dB do 10 dB, žlutá reprezentuje signál od -10 dB až 0 dB a oranžová reprezentuje -10 dB a méně.



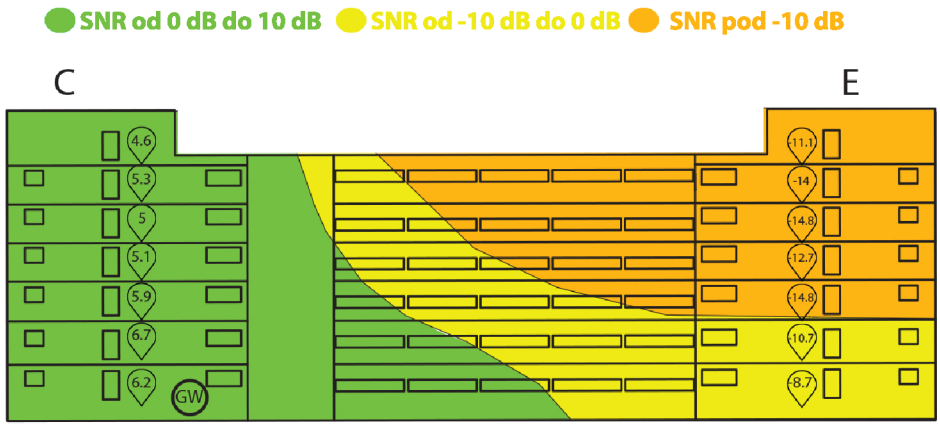
Obr. 6.17: Umístění brány v knihovně T12.



Obr. 6.18: Umístění brány a oblasti měření.

Tab. 6.9: Hodnoty měření v budově T12.

Patro	Budova	Průměr RSSI (dBm)	Průměr SNR (dB)
1	E	-107	-8.7
2	E	-107	-10.7
3	E	-106	-14.8
4	E	-107	-12.7
5	E	-107	-14.8
6	E	-106	-14
7	E	-107	-11.1
1	C	-74	6.2
2	C	-91	6.7
3	C	-91	5.9
4	C	-92	5.1
5	C	-90	5
6	C	-94	5.3
7	C	-96	4.6



Obr. 6.19: Zobrazení signálu podle SNR v budově T12.

7 ZÁVĚR

V první části bakalářské práce, byla teoreticky popsána nová radiová technologie LoRaWAN s nízkou spotřebou energie. Technologie byla parametricky srovnána s konkurenčními Low Power WAN technologiemi, které lze nalézt v příloze B. Byly zde ukázány výhody této sítě a její parametry. Tento teoretický podklad byl nutný pro samotný návrh a realizaci vlastní sítě.

Dále je zde část věnující se analýze jednotlivých prvků sítě a poté i jejich volbou. Jako koncové zařízení byl zvolen Demonstrátor LoRaWAN od firmy Adeunis RF, který je navržen právě pro testování sítě. Dále byly testovány dva senzory od firmy SolidusTech, které se uvažují pro nasazení v rámci smart grid sítí firmou E.ON. Následovala volba brány, kde byla zvolena gateway LORANK 8 od firmy Ideetron, a to díky své ceně a parametrům. Nakonec byl zvolen cloud společnosti Loriot, který je nutný pro zpracování dat LoRaWAN.

Poslední kapitola se zabývá již samotným vybudováním a ověřením funkčnosti sítě LoRaWAN v různých podmínkách. V této kapitole byly popsány jednotlivé prvky této sítě a jejich parametry, také zde byla změřena spotřeba energie koncových zařízení od firmy SolidusTech, hodnoty jsou vidět v Tab. 6.2 a Tab. 6.3. Byla tedy ověřena nízká energetická náročnost těchto zařízení. Dále probíhalo v rámci této kapitoly vlastní ověřování sítě. Nejdříve bylo měřen senzor od firmy SolidusTech v různých terénních oblastech (jako přímá viditelnost, les, nížina uprostřed lesa a také oblast za lesem nad úrovní přijímače), aby se ukázaly jeho parametry v reálném provozu. Poté byl testován venkovní dosah sítě v rámci pokrytí oblasti kolem vesnice. Dosah sítě byl také otestován v prostoru budovy školy, kde byla testována penetrace skrz patra. Síť stačila na pokrytí všech pater budovy školy.

Hlavním přínosem práce bylo seznámení se podrobně s novou rádiovou technologií LoRaWAN a její vlastní modulací LoRa. Dále návrh a vytvoření vlastní sítě na této technologii a otestování sítě v reálném provozu, při kterém bylo zjištěno, že LoRaWAN ve venkovních prostorech dokáže pokrýt poměrně velkou oblast (až 6 km) i když neprobíhá vysílání na přímou viditelnost. Ve vnitřních prostorech dopadla penetrace skrz patra poměrně dobře, technologie pokryla všech 7 pater školy s dobrou sílou signálu která neklesla pod -107 dBm (kritickou hodnotou LoRaWAN je -120 dBm), SNR v posledních patrech budovy přesáhlo i kritickou hodnotu -10 dB.

Byla vytvořena vlastní LoRaWAN síť a otestována. Nyní je připravena na aplikaci do reálného provozu. Pro reálný provoz je nutno vytvořit vlastní aplikační výstup pro koncové uživatele.

LITERATURA

[1] GUBBI, Jayavardhana, Slaven MARUSIC a Marimuthu PALANISWAMI. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems* [online]. 2013, 1(29), 1645-1660 [cit. 29. 5. 2017]. Dostupné z URL: <http://www.sciencedirect.com/science/article/pii/S0167739X13000241>.

[2] ATZORI, Luigi, Antonio IERA a Giacomo MORABITO. The Internet of Things: A survey. *Computer Networks* [online]. Elsevier B.V, 2010, 54(15), 2787-2805 [cit. 29. 5. 2017]. DOI: 10.1016/j.comnet.2010.05.010. ISSN 1389-1286. Dostupné z URL: <http://www.sciencedirect.com/science/article/pii/S1389128610001568>.

[3] BARDYN, J.-P., T. MELLY, O. SELLER a N. SORNIN. IoT: The era of LPWAN is starting now. *European Solid-State Circuits Conference* [online]. IEEE Computer Society, 2016, 2016-, s. 25-30 [cit. 29. 5. 2017]. DOI: 10.1109/ESSCIRC.2016.7598235. ISBN 9781509029723. ISSN 19308833. Dostupné z URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7598235>.

[4] BROWN Isaac A Detailed Breakdown of LPWAN Technologies and Providers *Luxresearchinc* [online]. Lux Research Inc. Client Confidential 2015 [cit. 29. 5. 2017]. Dostupné z URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7598235>.

[5] SOLUTIONS Pinacl PINACL Blog *The role of LoRaWAN in the Internet of Things* [online]. Pinacl Solutions [cit. 29. 5. 2017]. Dostupné z URL: <https://pinaclsolutions.com/blog/2017/lorawan-and-the-internet-of-things>.

[6] INVENTROM *THE "THING" IN "INTERNET OF THINGS "* [online]. Inventrom [cit. 29. 5. 2017]. Dostupné z URL: <https://inventrom.wordpress.com/2014/11/27/the-thing-in-internet-of-things/>.

[7] LASI, Heiner, Peter FETTKE, Hans-Georg KEMPER, Thomas FELD a Michael HOFFMANN. Industry 4.0. *Business & Information Systems Engineering* [online]. Wiesbaden: Springer Fachmedien Wiesbaden, 1408, 6(4), 239-242 [cit. 29. 5. 2017]. DOI: 10.1007/s12599-014-0334-4. Dostupné z URL: <http://search.proquest.com/docview/1556941973?pq-origsite=gscholar>.

[8] KABALCI, Yasin. A survey on smart metering and smart grid communication *Renewable and Sustainable Energy Reviews* [online]. Elsevier Ltd, 1605, 57,

302-318 [cit. 16. 10. 2016]. DOI: 10.1016/j.rser.2015.12.114. ISSN 1364-0321. Dostupné z URL: <http://www.sciencedirect.com.ezproxy.lib.vutbr.cz/science/article/pii/S1364032115014975>.

[9] WEI, Joseph. How Wearables Intersect with the Cloud and the Internet of Things: Considerations for the developers of wearables. *Consumer Electronics Magazine,IEEE* [online]. USA: IEEE, 1407, 3(3), 53-56 [cit. 29. 5. 2017]. DOI: 10.1109/MCE.2014.2317895. ISSN 2162-2248. Dostupné z URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6844949>.

[10] POSTSCAPES IoT Standards and Protocols *An overview of protocols involved in Internet of Things devices and applications. Help clarify with IoT layer technology stack and head-to-head comparisons.* [online]. Postscapes Navigate Your Connected World [cit. 16. 10. 2016] Dostupné z URL: <https://www.postscapes.com/internet-of-things-protocols/>.

[11] HANUS, Stanislav. *Bezdrátové a mobilní komunikace.* 1. vyd. Brno: VUT, 2001, 134 s. : il. ISBN 80-214-1833-8 [cit. 16. 10. 2016].

[12] Frequency Bands allocated to Terrestrial Broadcasting Services. *ITU Committed to connecting the world.* [online]. ©2016 [cit. 2016-10-16]. Dostupné z URL: <http://www.itu.int/en/ITU-R/terrestrial/broadcast/Pages/Bands.aspx>.

[13] PETERKA, Jiří. *Komunikace na PC* [online]. [cit. 16. 10. 2016]. Dostupné z URL: <http://www.earchiv.cz/a94/a408c502.php3>.

[14] Ústav státu a práva AV ČR. Telekomunikační zákon. *IT právo.* [online]. ©2016. [cit. 16. 10. 2016]. Dostupné z URL: <http://itpravo.cz/plne_zneni/telekomunikacni_zakon.txt>.

[15] ČTÚ. *Správní poplatky* [online]. 2016 [cit. 16. 10. 2016]. Dostupné z URL: <http://www.ctu.cz/sites/default/files/obsah/stranky/29598/soubory/spravnipoplatky.pdf>.

[16] MOERMAN, Ingrid, Jeroen HOEBEKE a Eli DE POORTER. *Converged, configurable LPWAN architecture for IoT devices (presentation)* [online]. In: . 2016 [cit. 29. 5. 2017]. Dostupné z URL: <https://biblio.ugent.be/publication/7257956>.

[17] HUANG, Junxian and Qian, et al.

A Close Examination of Performance and Power Characteristics of 4G LTE Networks [online]. In: . 2012 [cit. 29. 5. 2017]. Dostupné z URL: <http://dl.acm.org/citation.cfm?id=2307658>.

[18] CAVALCANTE, Andre M., Erika ALMEIDA, Robson D. VIEIRA, et al. Performance Evaluation of LTE and Wi-Fi Coexistence in Unlicensed Bands. In: *Vehicular Technology Conference (VTC Spring), 2013 IEEE 77th* [online]. IEEE, 1306, s. 1-6 [cit. 29. 5. 2017].DOI: 10.1109/VTCSpring.2013.6692702. ISSN 1550-2252. Dostupné z URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6692702>.

[19] ADELANTADO, Ferran, et al. *Understanding the limits of LoRaWAN.* [Online] 2015. [cit. 9. 11. 2016]. Dostupné z URL: <https://arxiv.org/pdf/1607.08011v1.pdf>.

[20] LinkLabs *A COMPREHENSIVE LOOK AT Low Power, Wide Area Networks* [online]. ©2016. Inc. 130 Holiday Court, Suite 100, Annapolis, MD 21401 [cit. 6. 11. 2016]. Dostupné z URL: <http://cdn2.hubspot.net/hubfs/427771/LPWAN-Brochure-Interactive.pdf>.

[21] SimpleCell. Technologie SIGFOX. *SimpleCell.* [online]. 2016. [cit. 9. 11. 2016]. Dostupné z URL: <https://www.simplecell.eu/technologie_sigfox/>.

[22] Semiconductor Components Industries AX-SIGFOX *Ultra-Low Power, AT Command Controlled,Sigfox Compliant Transceiver IC for Up-Link and Down-Link* [online]. 2016. [cit. 9. 11. 2016]. Dostupné z URL: <https://www.onsemi.com/pub/Collateral/AX-SIGFOX-D.PDF>.

[23] Low Power Wide Area Network (LPWA): Symphony Link vs. LoRaWAN *Link Labs* [online]. Link Labs 2016. [cit. 9. 11. 2016]. Dostupné z URL: <https://www.link-labs.com/blog/low-power-wide-area-network-lpwa>.

[24] BEECHER, Phil. Wi-SUN Alliance at European Utility Week. *Engerati.* [online]. 16. 10. 2013 [cit. 9. 11. 2016]. Dostupné z URL: <https://www.engerati.com/sites/engerati/files/Phil%20Beecher.pdf/>.

[25] How Wi-SUN® Compares with LoRaWAN® and NB-IoT *Comparing IoT Networks at a Glance*[online]. WiSun Alliance [cit. 9. 11. 2016]. Dostupné z URL: <https://www.wi-sun.org/images/assets/docs/Wi-SUN-Alliance-Comparing_IoT_Networks-r1.pdf>.

[26] SEOG, Yongho. IEEE 802.11AH (WI-FI IN 900 MHZ LICENSE-EXEMPT BAND) FOR IOT APPLICATION *IEEE Standard University* [online]. 14. 8. 2016 [cit. 9. 11. 2016]. Dostupné z URL: <http://www.standardsuniversity.org/e-magazine/august-2016-volume-6/ieee-802-11ah-wi-fi-900-mhz-license-exempt-band-iot-application/>.

[27] LANDSTRÖM, Sara, et al. NB-IoT: a sustainable technology for connecting billions of devices *Ericsson* [online]. 25. 4. 2016 [cit. 9. 11. 2016]. Dostupné z URL: <https://www.ericsson.com/thecompany/our_publications/ericsson_technology_review/archive/narrowband-iot-connecting-billions-devices>.

[28] SCHMIDBAUER Hardy, NB-IoT vs LoRa™ Technology *LoRa Alliance white paper* [online]. 2016 2400 Camino Ramon LoRa Alliance [cit. 9. 11. 2016]. Dostupné z URL: <https://www.lora-alliance.org/portals/0/documents/whitepapers/LoRa-Alliance-Whitepaper_NBIoT_vs_LoRa.pdf>.

[29] Long Range, Low power and Low cost network solutions. *nWave* [online]. nWave [cit. 9. 11. 2016]. Dostupné z URL: <http://www.nwave.io/nwave-network/>.

[30] An Educational guide how RPMA works, *A white paper of ingenu*[online]. ingenu [cit. 9. 11. 2016]. Dostupné z URL: <http://www.telecomnews.co.il/image/users/228328/ftp/my_files/General%20Files/IoT%20Ingenu%20original.pdf?id=27645739>.

[31] PETERKA Jiří, Šířka pásma a její dělení *eArchiv* [online]. Computerworld č. 43/91 v roce 1991 [cit. 29. 5. 2017]. Dostupné z URL: <http://www.earchiv.cz/a91/a143c110.php3>.

[32] PETERKA Jiří, Jak probíhají bezdrátové přenosy v sítích WLAN *eArchiv* [online]. IT-NET, v září 2002 [cit. 29. 5. 2017]. Dostupné z URL: <http://www.earchiv.cz/b02/b0900016.php3>.

[33] První celorepublikový mobilní operátor pro internet věcí *SimpleCell* [online]. SimpleCell [cit. 29. 5. 2017]. Dostupné z URL: <http://www.simplecell.eu/>.

[34] SEMTECH. *Semtech Acquires Wireless Long Range IP Provider Cycleo* [online]. [cit. 9. 11. 2016]. Dostupné z URL: <http://investors.semtech.com/releasedetail.cfm?ReleaseID=655335>.

[35] GEORGIOU, Orestis a USMAN Raza. Low Power Wide Area Network Analysis: Can LoRa Scale? *Cornell University Library* [online]. 15. 10. 2016 [cit. 9. 11. 2016]. Dostupné z URL: <https://arxiv.org/abs/1610.04793>.

[36] MOERMAN, Ingrid, Jeroen HOEBEKE a Eli DE POORTER. *Converged, configurable LPWAN architecture for IoT devices (presentation)* [online]. 31. 6. 2016 [cit. 9. 11. 2016]. Dostupné z URL: <https://biblio.ugent.be/publication/7257956>.

[37] LoRa Aliance. LoRa Alliance™ Technology *LoRa Aliance Wide Area Network* [online]. © 2016 [cit. 9. 11. 2016]. Dostupné z URL: <https://www.lora-alliance.org/what-is-lora/technology>.

[38] GOURSAUD Claire a GORCE Jean-Marie. *Dedicated networks for IoT: PHY-/MAC state of the art and challenges.* EAI endorsed transactions on Internet of Things, [online] 2015. [cit. 9. 11. 2016]. Dostupné z URL: <https://hal.archives-ouvertes.fr/hal-01231221/>.

[39] Shannon–Hartley theorem. In: *Wikipedia: the free encyclopedia*[online]. San Francisco (CA): Wikimedia Foundation, 2001. [cit. 9. 11. 2016]. Dostupné z URL: <https://en.wikipedia.org/wiki/Shannon%E2%80%93Hartley_theorem>.

[40] AN1200.22 LoRa™ Modulation Basics *Semtech application note*[online]. Semtech Corporation 2015 [cit. 9. 11. 2016]. Dostupné z URL: <http://www.semtech.com/images/datasheet/an1200.22.pdf>.

[41] SX1272/3/6/7/8: LoRa Modem *Designer's Guide*[online]. Semtech Corporation 2013 [cit. 9. 11. 2016]. Dostupné z URL: <https://www.semtech.com/images/datasheet/LoraDesignGuide_STD.pdf>.

[42] DUCROT, Nicolas, et al. *Connected Objects and Partnership.* Technical Document, [Online] 2015. [cit. 9. 11. 2016]. Dostupné z URL: <https://partner.orange.com/wp-content/uploads/2016/04/LoRa-Device-Developer-Guide-Orange.pdf>.

[43] ROSATI Tony, LoRaWAN Security Overview *Trustpoint blog* [Online]. January 17, 2017 [cit. 29. 5. 2017]. Dostupné z URL: <http://www.trustpointinnovation.com/blog/2017/01/17/lorawan-security-overview/>.

[44] STOKKING Johan LoRaWAN Security - The Things Network Webinar *The things network webinar session* [Online]. February 15th Amsterdam 2017 [cit. 29. 5. 2017]. Dostupné z URL: <https://www.thethingsnetwork.org/forum/t/webinar-session-lorawan-security-by-johan-stokking-feb-15th/5295>.

[45] MILLER, Robert. *LoRa Security Building a Secure LoRa Solution* [Online]. 22. 3. 2016 [cit. 20. 11. 2016]. Dostupné z URL: <https://labs.mwrinfosecurity.com/assets/BlogFiles/mwri-LoRa-security-guide-1.2-2016-03-22.pdf>.

[46] Microchip *RN2483* [Online]. 2016 [cit. 20. 11. 2016]. Dostupné z URL: <http://www.microchip.com/wwwproducts/en/RN2483>.

[47] Multitech *MultiConnect® mDot™* [Online]. 2016 [cit. 20. 11. 2016]. Dostupné z URL: <http://www.multitech.com/documents/publications/data-sheets/86002171.pdf>.

[48] LinkLabs *LL-RLP-20* [Online]. 2016 [cit. 20. 11. 2016]. Dostupné z URL: <https://cdn2.hubspot.net/hub/427771/file-2643325153-pdf/LL-RLP-20Datasheet.pdf>.

[49] Adeunis RF *Lo868-25mW Module* [Online]. 2016 [cit. 20. 11. 2016]. Dostupné z URL: <http://www.adeunis-rf.com/media/downloads/162/trad_file/eng/arf_lo868_25mw_lora_module_data_sheet_v1-4-gb.pdf>.

[50] *WiMOD iM880A* [Online]. IMST GmbH Carl-Friedrich 47475 KAMP GERMANY 2016 [cit. 20. 11. 2016]. Dostupné z URL: <http://www.tekmodul.de/fileadmin/Redakteure/pdf/IMST/iM880A_Datasheet.pdf>.

[51] *LORA™ RAPID DEVELOPMENT KIT* [Online]. Ajuinlei 1 Gent 9000, Belgium: AllThingsTalk, 2016 [cit. 20. 11. 2016]. Dostupné z URL: <http://www.allthingstalk.com/lora-rapid-development-kit>.

[52] *MultiConnect® mDot™* [Online].2205 Woodale Drive Mounds View, Minnesota 55112 U.S.A, 2016 [cit. 20. 11. 2016]. Dostupné z URL: <https://developer.mbed.org/media/uploads/sclark/mdotqsgrev.1.pdf>.

[53] FLASHNET *inteliLIGHT® LoRa RF FRE-220 LUMINAIRE CONTROLLER* [Online]. 2016 [cit. 20. 11. 2016]. Dostupné z URL: <http://www.flashnet.ro/download/lora_press_release_materials/inteliLIGHT%C2%AE%20LoRa%20data%20sheet%20-%20FRE-220%20controller.pdf>.

[54] ABEEWAY *Low Power Industrial GPS Tracker* [Online]. 2016 [cit. 20. 11. 2016]. Dostupné z URL: <http://www.objenious.com/wp-content/uploads/2016/05/Master-Tracker_Datasheet_V1_5.pdf>.

[55] NKE WATTECO *LoRaWAN end nodes* [Online]. 2016 [cit. 20. 11. 2016]. Dostupné z URL: <http://www.nke-watteco.com/gamme/lora-range/>.

[56] ADENUIS *Demonstrator LoRaWAN 868 EUR* [Online]. 2016 [cit. 20. 11. 2016]. Dostupné z URL: <http://www.adeunis-rf.com/media/downloads/172/trad_file/eng/arf_lorawan_demonstrator_868_data_sheet_v1-2_gb.pdf>.

[57] ADENUIS *FIELD TEST DEVICE LoRaWAN 868 EUR* [Online]. 2016 [cit. 20. 11. 2016]. Dostupné z URL: <http://www.adeunis-rf.com/media/downloads/188/trad_file/eng/arf_lorawan_field_test_device_868_data_sheet_v1.0_fr_gb.pdf>.

[58] SolidusTech *SolidusTech* [Online]. [cit. 29. 5. 2017]. Dostupné z URL: <http://www.solidustech.cz/>.

[59] LINKLABS *Spec Sheet.* [Online]. ©2015 Link Labs, LLC 130 Holiday Court, Suite 100, Annapolis, MD 21401 info@link-labs.com [cit. 20. 11. 2016]. Dostupné z URL: <http://www1.futureelectronics.com/doc/LINK%20LABS/LL-BST-8.pdf>.

[60] IDEETRON *LORANK 8* [Online] . 2016 [cit. 20. 11. 2016]. Dostupné z URL: <http://webshop.ideetron.nl/LORANK-8>.

[61] LORRIER *LR Series LoRaWAN LR2 datasheet* [Online]. 2016 [cit. 20. 11. 2016]. Dostupné z URL: <https://drive.google.com/file/d/0B2d6XCsqk9PSRkJic25yUUFnemc/view>.

[62] KERLINK *Wirnet Station 868* [Online]. 2016 [cit. 20. 11. 2016]. Dostupné z URL: <http://www.kerlink.fr/en/products/lora-iot-station-2/lora-iot-station-868-mhz>.

[63] Senzor LoRaWAN INDOOR UNI *Solidus tech datesheet* [Online]. Solidus Tech s.r.o [cit. 29. 5. 2017]. Dostupné z URL: <http://www.solidustech.cz/files/lora_indooruni_datasheet.pdf>.

[64] LoRaWAN čítač impulsů *Solidus tech datesheet* [Online]. Solidus Tech s.r.o [cit. 29. 5. 2017]. Dostupné z URL: <http://www.solidustech.cz/files/lora_%C4%8D%C3%ADta%C4%8D_impuls%C5%AF.pdf>.

[65] 14585A Control and Analysis Software for Advanced Power Supplies *Keysight technologies* [Online]. [cit. 29. 5. 2017]. Dostupné z URL: <http://www.keysight.com/main/software.jspx?cc=CZ&lc=eng&ckey=1785860&nid=-536902299.656338.02&id=1785860&cmpid=zzfind14585>.

[66] Battery Life Calculator *Digi-key electronics* [Online]. [cit. 29. 5. 2017]. Dostupné z URL: <https://www.digikey.com/en/resources/conversion-calculators/conversion-calculator-battery-life>.

[67] Aplikace Hercules *HWGroup* [Online]. [cit. 29. 5. 2017]. Dostupné z URL: <http://www.hw-group.com/products/hercules/index_cz.html>.

[68] FETTE, Ian. The websocket protocol. [Online]. 2011. [cit. 29. 5. 2017]. Dostupné z URL: <https://tools.ietf.org/html/rfc6455>.

[69] Geo Tracker *Geo Tracker Application* [Online]. [cit. 29. 5. 2017]. Dostupné z URL: <https://geo-tracker.org/>.

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

ABP	Activation By Personalization
ADR	adaptivní rychlost přenosu dat – Adaptive Data Rate
AM	amplitudová modulace – Amplitude Modulation
AMI	Advanced Metering Infrastructure
AMR	Automatic Meter Reading
AP	přístupový bod – Accesss Point
b	bit
BPSK	Binary Phase Shift Keying
CRC	cyklický redundantní součet – Cyclic Redundancy Check
CSS	Chirp Spread Spectrum
ČTÚ	Český Telekomunikační Ústav
dB	Decibel
DR	Demand Response
ETSI	European Telecommunications Standards Institute
FCS	rámec kontrolního součtu – Frame Check Sequence
FM	frekvenční modulace – Frequency Modulation
GMSK	Gaussian Minimum Shift Keying
GSM	Global System for Mobile Communications
Hz	Hertz
HTTP	Hypertext Transfer Protocol
IoT	internet věcí – Internet of Things
ISM	Industrial, Scientific and Medical
ITU	International Telecommunication Union
LPWAN	Low Power Wide Area Network

LTE	Long Term Evolution
M2M	Machine to Machine
MAC	Media Access Control
MIC	Message Integrity Code
MQTT	MQ Telemetry Transport
OFDMA	Orthogonal Frequency Division Multiple Access
OTAA	Over The Air Activation
PAN	Personal Area Network
PLC	Power Line Communication
PM	fázová modulace – Phase Modulation
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
RPMA	Random Phase, Multiple Access
RSSI	Received Signal Strength Indication
SF	činitel rozprostření – Spreading Factor
SM	Smart Metering
SNR	Signal-to-noise ratio
T_{a}	čas ve vzduchu – Time on Air
UWB	ultra-širokopásmové – Ultra-Wideband
WAN	Widde Area Band

SEZNAM PŘÍLOH

A OBSAH PŘILOŽENÉHO CD

- `/` ..... Kořenový adresář přiloženého CD
  - `Měření oblastí.` ..... Tabulky měřených hodnot v jednotlivých oblastech.
    - `Mereni budova skoly.xlsx`
    - `Mereni okoli vesnice.xlsx`
    - `Overeni pomoci demonstratoru Adeunis.xlsx`
  - `Spotřeba energie.` ..... Měření spotřeby na přístroji Keysight N6705B.
    - `eon 20170428 064734.dlog`
  - `Bakalářská práce.pdf` ..... Bakalářská práce v elektronické podobě

B TABULKA K LPWAN

Tab. A.1: Porovnání parametrů LPWAN.

	Šířka pásma	**Rychlost přenosu dat za sekundu**	**Vzdálenost**	**Pásmo**	**Počet koncových zařízení**	**Standard**	**Link budget**	**Vysílací výkon koncového zařízení**	**Množství dat (paket)**
LoRaWAN	125/250/500 kHz	22 b–50 kb	2–15 km	868 MHz, 915 MHz, 430 MHz	15 000	LoRa proprietární LoRaWAN open standard	151 dBm	14 dBm	51–222 Bajtů
SigFox	100 Hz	100 b (140 zpráv denně)	3–50 km	868 MHz, 915 MHz	50 000	Proprietární	156 dBm	14 dBm	12 Bajtů
Wi-SUN	200 kHz–1,2 MHz	50 kb–400 kb	až 20 km	868 MHz	desítky tisíc	Standard	–	13 dBm	2047 Bajtů
nWave	200 Hz	100 b	10–30 km	868 MHz	až milion	Proprietární	177 dBm	25–100 mW	32 Bajtů
Wi-f hallow	1/2/4/8/16 MHz	až 150 kb	kolem 1 km	2,4 GHz, 5 GHz	8191	Standard	–	1 mW–1 W	7 991 Bajtů
Ingenu RPMA	1 MHz	624 kb	4,6–500 km	2,4 GHz	384 000	Proprietární	163 dBm	20 dBm	až 10 kB
Weightless-W	5 MHz	1 kb–10 Mb	5 km	470 MHz–790 MHz	není limitováno	open standard	–	17 dBm	10 Bajtů/min
NB-IoT	200 kHz	60–250 kb	až 35 km	Licencované LTE	50 000	Standard	164 dBm	23 dBm	200 Bajtů
LTE-Cat M	1,4 MHz	až 10 Mb	100 km	Licencované LTE	20 000	Standard	144 dBm	100 mW (20dBm)	100–1000 Bajtů
Symphony Link	125 kHz	150 b	10 km	900 MHz	250 000	Standard Link Labs	170 dBm	až 1 W	256 Bajtů