VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

DIPLOMOVÁ PRÁCE

Brno, 2022 Bc. Martin Bahna

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

IMPLEMENTACE A VYHODNOCENÍ KOMUNIKAČNÍ TECHNOLOGIE LORAWAN V SIMULAČNÍM PROSTŘEDÍ NS-3

IMPLEMENTATION AND PERFORMANCE EVALUATION OF THE LORAWAN COMMUNICATION TECHNOLOGY UTILIZING THE NS-3

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE — Bc. Martin Bahna

AUTHOR

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

SUPERVISOR

BRNO 2022

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

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

Ústav telekomunikací

Student: Bc. Martin Bahna ***ID:*** 197765

Ročník: 2 ***Akademický rok:*** 2021/22

NÁZEV TÉMATU:

Implementace a vyhodnocení komunikační technologie LoRaWAN v simulačním prostředí NS-3

POKYNY PRO VYPRACOVÁNÍ:

Cílem diplomové práce bude studium technologie LoRaWAN. V teoretické části bude provedeno porovnání dostupných LPWA technologií, kdy bude důraz kladen na rozbor technologie LoRaWAN a srovnání s technologiemi Sigfox, NB-IoT a LTE Cat-M. Následně bude provedena implementace scénářů pro přenos dat v rámci inteligentních sítí. Implementace bude realizována v simulačním nástroji Network Simulator 3 (NS-3). Praktická část se bude sestávat z vytvoření scénáře s využitím dostupného LoRaWAN modulu. Bude provedeno porovnání aktuální implementace s přihlédnutím k teoretickým parametrům LoRaWAN. Na základě prvotních výsledků bude přistoupeno k modifikaci vybraného LoRaWAN modulu s cílem zlepšení komunikačních parametrů, tj. přenosová rychlost, komunikační vzdálenost, spotřeba koncového zařízení v různých operačních stavech. Dosažené výstupy z vytvořených komunikačních scénářů budou přehledně zpracovány a diskutovány.

DOPORUČENÁ LITERATURA:

[1] Network Simulator 3: Documentation, A Discrete-Event Network Simulator [online], 2019. Dostupné z: https://www.nsnam.org/doxygen/.

[2] REYNDERS, Brecht; WANG, Qing; POLLIN, Sofie. A LoRaWAN module for ns-3: implementation and evaluation. In: Proceedings of the 10th Workshop on ns-3. ACM, 2018. p. 61-68.

Termín zadání: 7.2.2022 ***Termín odevzdání:*** 24.5.2022

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

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

ABSTRAKT

Diplomová práca je venovaná implementácii bezdrôtovej siete LoRaWAN v simulačnom prostredí NS-3. V práci je všeobecne opísané IoT, využité technológie a druhy komunikácie medzi zariadeniami. Následne je opísaná technológia LPWAN, jej požiadavky a najpoužívanejšie protokoly využívajúce túto technológiu. Ďalej je detailne opísaná technológia LoRaWAN, vrstvy na ktorých pracuje, sieťová architektúra a bezpečnosť. V rámci praktickej časti je opísané simulačné prostredie NS-3 a vybraný najvhodnejší LoRaWAN modul z dostupných modulov. Vybraný modul je detailne popísaný a importovaný do simulačného prostredia NS-3. Následne sú vykonané dva simulačné scenáre, prvý so zameraním na vplyv počtu koncových zariadení v sieti a druhý zameraný na vplyv vzdialenosti koncového zariadenia od brány. Výsledky simulácií sú zapísané do tabuliek, z ktorých sú následne vytvorené grafické závislosti. V poslednej kapitole je pristúpené k modifikácii modulu implementovaním nových frekvenčných pásiem a teoretickou prípravou na obojsmernú komunikáciu a šifrovanie.

KĽÚČOVÉ SLOVÁ

IoT, LoRaWAN, LPWAN, NS-3, Simulácia siete

ABSTRACT

The diploma thesis deals with an implementation of the LoRaWAN wireless network within the NS-3 simulation environment. The thesis defines IoT in general, together with its technologies and types of communication between devices. Subsequently, the LPWAN technology is outlined, as well as its requirements and protocols that are most widely used with this technology. The thesis then describes the LoRaWAN technology in detail, its layers, network architecture and security. The practical part of this thesis sheds some light on the NS-3 simulation environment and the most suitable LoRaWAN module that was selected from the available ones. The chosen module is described in detail and imported to the NS-3 simulation environment. Two simulation scenarios are then performed. The first scenario is focused on the impact created by increasing the number of end devices in the network. The second scenario is focused on the impact created by increasing the distance between the end device and the gateway. The results of the simulations are recorded in the tables which are then used to display the given results in graphs. Last chapter deals with module modification where new frequency bands are implemented and theoretical setup of duplex and encrypted communication is described.

KEYWORDS

IoT, LoRaWAN, LPWAN, NS-3, Network simulation

BAHNA, Martin. *Implementace a vyhodnocení komunikační technologie LoRaWAN v simulačním prostředí NS-3*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2022, 76 s. Diplomová práca. Vedúci práce: Ing. Pavel Mašek, Ph.D.

Vyhlásenie autora o pôvodnosti diela

Meno a priezvisko autora:	Bc. Martin Bahna
VUT ID autora:	197765
Typ práce:	Diplomová práca
Akademický rok:	2021/22
Téma závěrečnej práce:	Implementace a vyhodnocení komunikační technologie LoRaWAN v simulačním prostředí NS-3

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

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

Brno ....

podpis autora*

*Autor podpisuje iba v tlačenej verzii.

POĎAKOVANIE

Rád by som poďakoval vedúcemu semestrálnej práce pánovi Ing.Pavlovi Maškovi, Ph.D. za odborné vedenie, konzultácie, trpezlivosť a podnetné návrhy k práci. Rovnako chcem poďakovať mojim rodičom za neustálu podporu počas štúdia.

Obsah

Zoznam obrázkov

Zoznam tabuliek

Úvod

Diplomová práca je zameraná na Low Power Wide Area Network (LPWAN) technológiu LoRaWAN a jej implementáciu v simulačnom prostredí Network Simulator 3 (NS-3). LoRaWAN patrí medzi najpoužívanejšie LPWAN technológie, ktoré majú široké využitie v Internet of Things (IoT) vďaka svôjmu vysokému bezdrôtovému komunikačnému dosahu s minimálnou energetickou náročnosťou.

Prvá kapitola je venovaná všeobecnému popisu IoT, jeho využitie v praxi, výhody a nevýhody a samotná technológia, ktorú IoT využíva. Nachádza sa tu tiež stručný popis využitej Device-to-Device (DSD), Machine-to-Machine (M2M) a Massive Machine-Type Communication (mMTC).

V druhej kapitole je popísaná technológia LPWAN, jej široké využitie v praxi a požiadavky. Vrámci toho sú popísané najpoužívanejšie protokoly využívajúce túto technológiu: LoRaWAN, Narrow Band-IoT (NB-IoT), LTE Cat-M1 a Sigfox.

Tretia kapitola je venovaná podrobnému popisu LoRaWAN protokolu a LoRa modulácie. Detailne je popísaná fyzická vrstva využívajúca LoRa moduláciu a linková vrstva, ktorá pracuje s LoRaWAN protokolom. V rámci popisu linkovej vrstvy je okrem používaného sub-GHz Industrial, Scientific and Medical (ISM) frekvenčného pásma (868 MHz pre EU) popísané aj frekvenčné pásmo 2,4 GHz. Ďalej sú uvedené dostupné triedy koncových zariadení, metódy aktivácie koncových zariadení, sieťová architektúra a bezpečnosť technológie.

Nasledujúca kapitola sa venuje implementácii technológie LoRaWAN v simulačnom prostredí NS-3. Na začiatku je v krátkosti popísaný simulačný nástroj NS-3 využitý pre simulácie. Následne je zvolený vhodný modul technológie LoRaWAN využiteľný v simulačnom prostredí. Vybraný modul od SIGNET Lab (signetlabdei) je detailne popísaný, pričom je dôraz kladený najmä na porovnanie s praktickou implementáciou technológie v reálnom svete.

Piata kapitola je venovaná samotným simuláciám siete LoRaWAN. Na začiatok je vybraný vhodný príklad sieťovej architektúry, ktorý je súčasťou modulu. Z vybraného príkladu sú odvodené dva simulačné scenáre. Prvým je vplyv počtu koncových zariadení na úspešnosť prenosu pri rôznych polomeroch komunikačnej oblasti. Druhým scenárom je vplyv vzdialenosti koncového zariadenia od brány, kedy je sledovaný maximálny komunikačný dosah medzi koncovým zariadením a bránou. Výsledky sú prehľadne spracované do tabuliek, ktoré následne slúžia na grafické zobrazenie simulovaných scenárov.

V záverečnej kapitole sa pristupuje k modifikácii použitého LoRaWAN modulu. Na základe možností pre rozšírenie modulu boli vybrané tri modifikácie. Jedná sa o rozšírenie používaných frekvenčných pásiem, implementáciu obojsmernej komunikácie a na koniec šifrovanie komunikácie. Nové frekvenčné pásma sú prakticky imple-

mentované a obojsmerná komunikácia so šifrovaním sú popísané iba teoreticky kvôli vysokej komplexnosti modulu. Pre novoimplementované frekvenčné pásma sú vytvorené simulačné scenáre na porovnanie so stávajúcim frekvenčným pásmom.

1 Internet vecí

Pojem Internet vecí, anglicky Internet of Things (IoT), sa dostáva v dnešnej dobe čoraz viac do povedomia bežných ľudí. Oblasti použitia sú veľmi široké, od inteligentných domácich spotrebičov cez inteligentné domy až po chytré mestá, viď obr. 1.1. Hlavnou úlohou Internetu vecí je zjednodušiť život bežným ľuďom, ale aj zvýšiť produktivitu v priemysle a hospodárstve. Komunikácia prebieha na jednej strane medzi človekom a inteligentným zariadením a na strane druhej medzi samotnými zariadeniami pomocou Device to Device (D2D), Machine to Machine (M2M) či masívnej Machine-type komunikácie (mMTC). Tieto zariadenia sú prepojené pomocou Internetu za použitia rôznych bezdrôtových či drôtových komunikačných technológií a protokolov. Rovnako napájanie zariadení môže fungovať pomocou rozvodnej elektrickej siete, ale zvyčajne disponujú zariadenia vstavanými batériami či akumulátormi. V praxi sú najvýhodnejšie zariadenia, ktoré majú vlastnú batériu a dokážu komunikovať bezdrôtovo. V takom prípade je možné zariadenie umiestniť prakticky kdekoľvek bez potreby ďalšej investície do elektrickej rozvodnej siete.

Obr. 1.1: Možné scenáre využitia Customer IoT (CIoT) a Industrial IoT (IIoT) [1].

Hlavnými výhodami IoT je napríklad použiteľnosť v ktoromkoľvek odvetví, šetrenie času a nákladov, jednoduchá škálovateľnosť či automatizácia úkonov bez akejkoľvek potreby zásahu ľudskej zložky. Ako každý systém, aj Internet vecí má niekoľko

nevýhod. Medzi ne môže patriť napríklad exponenciálny rast inteligentných zariadení, ktoré je nutné spravovať, spracovávanie získaných údajov či možné chyby systému. Internet vecí nedisponuje žiadnym medzinárodným štandardom kompatibility, preto je možné, že niektoré zariadenia od rôznych výrobcov nebudú schopné spolu komunikovať. Veľkú pozornosť je potrebné venovať aj zabezpečeniu systému [2].

1.1 Technológia

Štandardne každé inteligentné zariadenie disponuje vlastným procesorom, senzorom a komunikačným modulom. Procesor riadi celé zariadenie, vykonáva potrebné výpočty a spracováva údaje získané zo senzoru. Senzor slúži na spomenuté získavanie určitých informácií, napr. vlhkosť ovzdušia, koncentrácia chlóru vo vode ai. Komunikačný modul slúži na komunikáciu zariadenia s ostatnými prvkami v sieti. Takýmto spôsobom má každné zariadenie v sieti určitú úlohu a potrebné informácie predáva po sieti ďalej na server, ktorý informácie zhromažďuje, analyzuje a ďalej využíva. Všetky spomenuté úkony fungujú bez zásahu ľudskej zložky a sú automatizované. Napriek tomu má človek k daným dátam prístup a môže meniť chod systému či zadávať nové inštrukcie.

Obr. 1.2: Komunikácia jednotlivých zariadení v IoT sieti [3].

1.1.1 Komunikácia medzi zariadeniami

Rastúci počet IoT zariadení priniesol potrebu automatizácie komunikácie a spracovávania dát medzi jednotlivými zariadeniami. IoT zariadenia preto využívajú komunikáciu Device to Device (D2D), Machine to Machine (M2M) a masívnu Machine-type komunikáciu.

Device to Device (D2D)
Jedná sa o priamu komunikáciu v mobilnej sieti medzi dvoma mobilnými zariadeniami bez potreby využitia prístupového bodu (brána, smerovač ai.) resp. backbone siete. D2D komunikácia je vo všeobecnosti netrasparentná v mobilnej sieti a využíva mobilné frekvecie alebo nelicencované spektrum. V bežnej mobilnej sieti musí všetka komunikácia prebiehať cez prístupový bod aj v prípade, že sú komunikujúce zariadenia k sebe v dostatočnej blízkosti pre D2D komunikáciu. Komunikácia cez prístupový bod je vyhovujúca pre aplikácie s nízkou rýchlosťou prenosu (hlasový hovor, posielanie správ) kedy sú zariadenia len zriedkavo v dostatočnej blízkosti pre priamu komunikáciu. Dnešné mobilné zariadenia však vyuźívajú služby s vyššími dátovými prenosmi (zdieľanie videa, hry, ai.) kedy zariadenia môžu byť potencionálne v dostatočnej blízkosti pre priamu komunikáciu (D2D). V takýchto prípadoch D2D komunikácia môže zásadne zvýšiť efektivitu siete. Výhodou D2D komunikácie sú zvyšovanie spektrálnej účinnosti, potencionálne zvýšenie priepustnosti, úspora energie či zníženie oneskorenia [4].

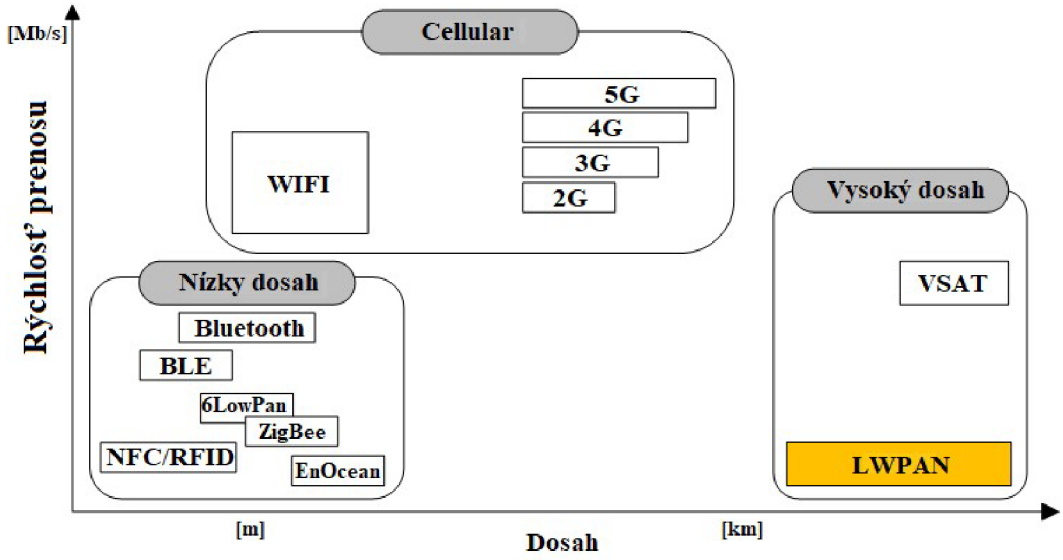
Machine to Machine (M2M)
Ide o priamu komunikáciu medzi zariadeniami využitím ktoréhokoľvek drtôvého či bezdrôtového komunikačného kanálu. M2M komunikácia môže zahŕňať priemyselné prístrojové vybavenie, ktoré umožní senzoru posielať zozbierané infromácie (teplota, vlhkosť, počet, ai.) aplikačnému zariadeniu, ktoré informácie ďalej využije (spustenie klimatizácie, závlahový systém, ai.). Takáto komunikácia pôvodne prebiehala v sieti s mnohými vzdialenými zariadeniami cez prístupový bod, ktorý zozbierané dáta najprv analyzoval a až následne presmeroval na príslušné zariadenie. Dnešná M2M komunikácia sa zmenila v systém rôznych sietí, ktoré prenášajú dáta na rôzne spotrebiče. Rozmach IP sietí spôsobil, že M2M komunikácia je omnoho rýchlejšia a jednoduchšia pričom spotrebuje podstatne menej energie [5].

Masívna Machine-type komunikácia (mMTC)
Ako už bolo spomenuté, Machine-type komunikácia je charakteristická plne automatickou generáciou, preposielaním a spracovávaním dát medzi inteligentnými zariadeniami s malým resp. žiadnym zásahom ľudského faktoru. Vzhľadom na rastúci

počet inteligentných zariadnení sa momentálne jedná o masívnu Machine-type komunikáciu. MMTC model sa líši tým, že obsahuje potencionálne veľké množstvo malých a energeticky obmedzených zariadení, kde každé zariadenie nefrekventovane posiela malé množstvo neoneskorených citlivých informácií. Okrem toho, rôzne mMTC služby obsahujú odlišnú prevádzku, ktorá v kombinácii s počtom zariadení vytvára problém alokovania potrebných prostriedkov [6].

2 LPWAN

Bežný človek sa na dennej báze stretáva s niekoľkými bezdrôtovými technológiami ako je WiFi, Bluetooth či mobilné siete 4G a po novom aj 5G. V IoT aplikáciách však každá z nich obsahuje niektorú nevýhodu. Buď sa jedná o malý dosah signálu (Bluetooth a WiFi), alebo napriek širokému pokrytiu ide o vysokú spotrebu elektrickej energie (mobilné bezdrôtové siete). Preto bolo nutné vyvynúť štandard vhodný pre IoT aplikácie, ktorým je Low Power Wide Area Network (LPWAN). Jedná sa o komunikačnú technológiu, ktorá je schopná pokryť veľkú zemepisnú oblasť a zároveň svojou nízko frekventovanou komunikáciou šetrí elektrickú energiu. Rozdelenie týchto technológií je možné vidieť na obr. 2.1.



Obr. 2.1: Porovnanie bezdrôtových technológií [7].

2.1 Požiadavky

LPWAN technológia je populárna hlavne v priemyselných a výskumných oblastiach vďaka nízkej spotrebe energie, veľkému pokrytiu a nízkym komunikačným nákladom. Medzi najzákladnejšie požiadavky patrí pokrytie veľkého územia, v praxi až do 10–40 km v neosídlených oblastiach a 1–5 km v osídlených oblastiach. Ďalšou základnou požiadavkou je vysoká energetická účinnosť, rádovo sa jedná o 10 + rokov výdrže batérie [7]. Treťou hlavnou požiadavkou je cenová dostupnosť kde rádiový chipset stojí menej ako 2 € a prevádzkové náklady sa pohybujú okolo 1 € na rok na zariadenie. Vďaka týmto aspektom je LPWAN technológia priam ideálna pre použitie v IoT aplikáciách, ktoré potrebujú posielať malé množstvo dát na veľkú vzdialenosť. Vzniklo

množstvo LPWAN technológií v licencovanej aj nelicencovanej podobe, popredné a najpoužívanejšie sa však stali LoRa, LTE Cat-M1 a NB-IoT [7], ktoré zahŕňajú mnoho technických rozdielov a preto budú popísané bližšie.

2.2 Rozdiely LPWAN technológií

Technológie LoRa, LTE Cat-M1 a NB-IoT sa líšia v mnohých technických aspektoch ako je popísané v tab. 2.1. Najhlavnejšie rozdiely spočívajú v použitej modulácii, prenosovej rýchlosti, veľkosti payloadu[1] a spôsobe overovania a šifrovania komunikácie.

Tab. 2.1: Prehľad LPWAN technológií: Sigfox LoRa a NB-IoT [7].

	LoRaWAN	**LTE Cat-M1**	**NB-IoT**	**Sigfox**
Pokrytie (MCL)	157 dB	155 dB	164 dB	162 dB
Technológia	Proprietárna	Open LTE	Open LTE	Proprietárna
Spektrum	Nelicencované	Licencované (LTE)	Licencované (LTE)	Nelicencované
Limit pracovného cyklu	Áno	Nie	Nie	Áno
Reštrikcia výstupného výkonu	Áno (14 dBm = 25mW)	Nie (23 dBm = 200 mW)	Nie (23 dBm = 200 mW)	Áno (14 dBm = 25 mW)
Downlink rýchlosť	0,3 - 50 kb/s	<300 kb/s	0,5 - 27,2 kb/s	<1 kb/s
Uplink rýchlosť	0,3 - 50 kb/s	<375 kb/s	0,3 - 32,25 kb/s	<1 kb/s
Max. veľkosť správy DL	243 B	1280 B	1280 B	12 B
Max. veľkosť správy UL	243 B	1280 B	1280 B	8 B
Životnosť batérie/ prúdový odber	8+ rokov <2 uA	10+ rokov <8uA	10+ rokov <3 uA	10+ rokov <2 uA
Cena modulu	<8€	<21€	<8€	<8€
Zabezpečenie	Stredné (AES-128)	Veľmi vysoké (LTE zabezpečenie)	Veľmi vysoké (LTE zabezpečenie)	Nízke (AES-128)

2.2.1 LoRaWAN

LoRa je modulácia pracujúca na fyzickej vrstve, ktorá moduluje signál v sub-GHZ ISM pásme použitím proprietárnej techniky rozšíreného spektra. LoRa využíva nelicencované ISM frekvenčné pásma 868 MHz v Európe, 915 MHz v Severnej Amerike a 433 MHz v Ázii. Obojsmerná komunikácia funguje pomocou CSS (Chirp Spread Spectrum[2]) modulácie, ktorá šíri úzkopásmový signál cez kanály s väčšou šírkou pásma. Výsledný signál má nízku úroveň šumu, čo zabezpečuje, že má vyššiu odolnosť voči rušeniu a tým je ťažké signál detekovať a narušiť.

[1] Payload je časť prenášaného obsahu, ktorá obsahuje užitočné dáta pre používateľa.

[2] Technika rozšíreného frekvenčného spektra, ktorá používa širokopásmové lineárne modulované "cvrlikajúce" impulzy (CSS) na šifrovanie informácie [8].

LoRa využíva šesť faktorov rozprestrenia (Spreading Factors) od SF7 do SF12 na prispôsobenie rýchlosti prenosu údajov. Čím vyšší je faktor šírenia, tým väčší je dosah, avšak na úkor prenosovej rýchlosti. Prenosová rýchlosť sa pohybuje medzi 300 b/s až 50 kb/s v závislosti na faktore šírenia a šírke pásma kanálu. Správy posielané použitím rôznych faktorov šírenia môžu byť prijaté LoRaWAN stanicami súčasne. Maximálny payload pre každú správu je 243 B. Komunikačný protokol LoRaWAN, založený na modulácii LoRa, bol štandardizovaný spoločnosťou LoRa-Alliance. Použitím LoRaWAN protokolu je každá správa vyslaná koncovým zariadením prijatá každou stanicou v dosahu. Týmto spôsobom si protokol LoRaWAN zaisťuje vysoký pomer úspešne doručených správ. Je to však na úkor vyššieho počtu staníc v dosahu, čo môže spôsobiť vyššiu cenu za zavedenie siete. Výsledné duplicitné záznamy sa filtrujú v backendovom systéme (server), ktorý obsahuje potrebnú inteligenciu na zaistenie bezpečnosti, posielanie potvrdzovaní na koncové zariadenia a odosielanie správ na zodpovedný aplikačný server [7].

Keďže je táto práca venovaná práve technológii LoRaWAN, bude okrem tohto stručného zhrnutia technológii venovaná ďalšia kapitola kde bude LoRaWAN popísaná bližšie.

2.2.2 NB-IoT

NB-IoT je Narrow Band IoT technológia špecifikovaná vo Vydaní 13 3GPP v Júni 2016. NB-IoT dokáže koexistovať s GSM (global system for mobile communications) a LTE (long-term evolution) pod licencovanými frekvenčnými pásmami (napr. 700 MHz, 800 MHz a 900 MHz). NB-IoT využíva frekvenčné pásmo šírky 200 kHz, čo zodpovedá jednému bloku GSM a LTE prenosu. S touto šírkou pásma je možné pracovať s prevádzkovými režimami:

- **Samostatná operácia:** možným scenárom je využitie v súčasnosti používaných GSM frekvenčných pásiem.
- **Operácia v ochrannom pásme:** využitie nepoužitých blokov LTE chráneného frekvenčného pásma.
- **Pásmová operácia:** využitie blokov v rámci LTE frekvenčného pásma.

V skutočnosti NB-IoT redukuje funkcionality LTE protokolu na minimum a zlepšuje ich podľa potrieb IoT aplikácií. NB-IoT teda možno považovať za nový protokol, ktorý je postavený na LTE infraštruktúre. Tento protokol umožňuje pripojenie až do 100 000 koncových zariadení na bunku s potenciálom na zväčšenie kapacity pridaním viacerých NB-IoT nosičov. Používa SC-FDMA (Single-Carrier Frequency Division Multiple Access) pre uplink a OFDMA (Orthogonal Frequency-Division Multiple-Access) pre downlink a zapája aj QPSK (Quadrature Phase-Shift Keying) moduláciu. Prenosová rýchlosť je limitovaná na 200 kb/s pre downlink a 20 kb/s

pre uplink. Maximálny payload je pre každú správu 1600 B. NB-IoT technológia dokáže zabezpečiť až 10 rokov výdrže batérie pri vysielaní priemerne 200 B denne [7].

2.2.3 LTE Cat-M1

Mobilná technológia LTE (4G mobilné siete) je rozšírená o LTE-M technológiu, ktorá stávajúce LTE obohacuje o podporu pre MTC (Machine-Type Communications) a IoT. Vo vydaní 12 3GPP boli špecifikované zariadenie pre Cat-0. Vo vydaní 13 3GPP (spolu s NB-IoT) boli špecifikované zariadenia Cat-M1, ktoré obnášali vylepšenia fyzickej vrstvy LTE a pokrytia. Pre Cat-M1 boli štandardizované dva módy pre vylepšenie pokrytia. Mód A, ktorý podporoval 32 opakovaní podrámcov na dátovom kanáli a mód B, ktorý podporoval až 2048 opakovaní. Podpora šírky pásma je rovnaká ako pri LTE. Cat-M1 vo svojej podstate rozširuje fyzickú vrstvu LTE. Rovnako ako pri NB-IoT pre uplink komunikáciu používa Cat-M1 SC-FDMA moduláciu a pre downlikovú komunikáciu je použité OFDM. Pre vysielanie sú použité úzkopásmové kanály (narrowbands). Na najvyššom mieste sa nachádza jeden hyperrámcový cyklus, ktorý obsahuje 1024 hyperrámcov, kde každý hyperrámec pozostáva z 1024 rámcov. Jeden rámec ďalej obsahuje 10 podrámcov, z ktorým každý sa delí na dva sloty po 0,5 ms. Podporovaný je FDD (Frequency-Division Duplex), ale aj TDD (Time-Division Duplex). Pri FDD sa používajú dve rôzne nosné pre downlink a uplink. Pokiaľ zariadenie podporuje plne duplexnú prevádzku tak môže vysielať a prijímať v rovnakom čase, kdežto pri polovičnom duplexe musí prepínať medzi týmito dvoma operáciami. Zariadenie dosahuje rýchlosť do 300 kb/s pre downlink a do 375 kb/s pre uplink. Maximálna veľkosť jednej správy je pre downlink a uplink rovnaká 1280 B. Batéria dokáže zariadenie udržať funkčné viac ako 10 rokov.

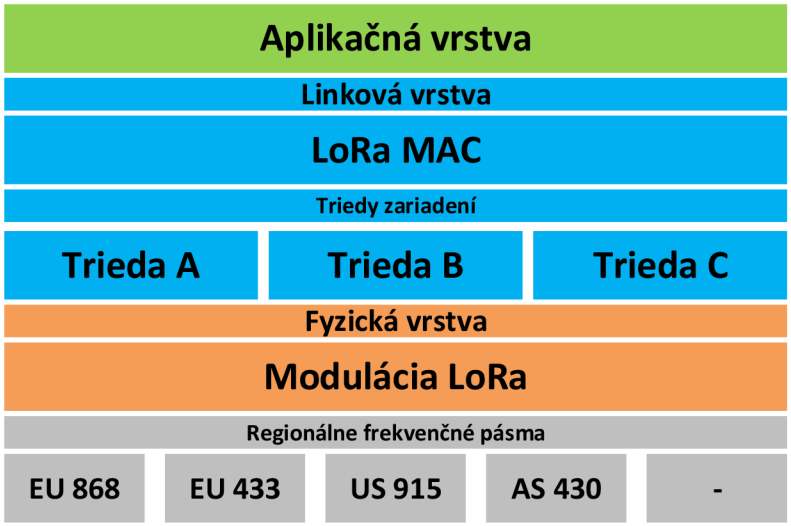
2.2.4 Sigfox

Sigfox je LPWAN sieťový operátor ktorý ponúka end-to-end IoT riešenie konektivity skrz patentované technológie. Sigfox používa vlastné stanice, pripojené k back-end serverom. Koncové zariadenia pripojené k týmto staniciam používajú moduláciu binárneho fázového posunu (BPSK) v ultra úzkopásmovom (100 Hz) sub-GHZ ISM pásmovom nosiči. Sigfox používa nelicencované ISM pásma napr. 868 MHz v Európe, 915 MHz v Severnej Amerike a 433 MHz v Ázii. Použitím ultra úzkopásmového prenosu, Sigfox dokáže efektívne využiť šírku pásma a má veľmi nízku úroveň šumu, čo spôsobuje nízky odber elektrickej energie, vysokú citlivosť prijímača a nízkorozpočtový dizajn antény na úkor maximálnej prenosovej rýchlosti iba 100 b/s. Sigfox na začiatku podporoval iba uplinkovú komunikáciu, ale neskôr začal podporovať komunikáciu obojsmernú. Downlinková komunikácia, teda dáta posielané zo stanice do koncových zariadení, môžu byť poslané iba za uplinkovou komunikáciou. Počet

správ odoslaných koncovým zariadením do stanice je limitovaný na 140 správ za deň. Maximálny payload pre každú odoslanú správu môže byť 12 B. Avšak správy prijaté koncovým zariadením zo stanice sú limitované na štyri denne, čo znamená, že potvrdzovanie správ nieje podporované. Maximálny payload pre každú prijatú správu je 8 B. Bez adekvátnej podpory potvrdzovania je spoľahlivosť uplinkovej komunikácie zabezpečená pomocou časovej a frekvenčnej diverzity ako aj duplikovaným posielaním správ. Každá správa z koncového zariadenia je posielaná niekoľko krát (štandardne 3 krát) po odlišných frekvenciách. Pre tieto účely je napríklad v Európe používané frekvenčné pásmo medzi 868,180 MHz a 868,220 MHz rozdelené na 400 ortogonálnych 100 Hz kanálov (medzi nimi je 40 kanálov vyhradených a nepoužívajú sa). Vďaka tomu, že stanica dokáže prijímať naraz správy na všetkých frekveciách, môže koncové zariadenie vyberať náhodné frekvencie na prenos dát [7].

3 LoRaWAN

Táto práca je zameraná hlavne na technológiu LoRaWAN, preto jej bude venovaná samostatná kapitola. Pozostáva z fyzickej a linkovej vrstvy, ako možno vidieť na obr. 3.1. LoRaWAN je open source štandard od orgaizácie LoRa Alliance. Jedná sa o LPWAN technológiu využívajúcu rozprestrené spektrum pre pomalý prenos nízkoobjemových dát na veľkú vzdialenosť.



Obr. 3.1: Vrstvy technológie LoRaWANí [9].

3.1 Fyzická vrstva

Na fyzickej vrstve pracuje LoRa modulácia pôvodne vyvinutá firmou Cycleo, ktorá sa neskôr stala súčasťou spoločnsti Semtech. LoRa pracuje v rozprestrenom spektre s využitím CSS modulácie. Hlavným požiadavkom bola komunikácia na veĺkú vzdialenosť bez ohľadu na nižšiu prenosovú rýchlosť. Vo výsledku sa dosahuje komunikačná vzdialenosť v jednotkách kilometrov pri osídlených oblastiach a až desiatkach kilometrov v neosídlených oblastiach. Modulácia pracuje vo frekvenčnom rozsahu od 137 MHz do 1020 MHz so zahrnutím ISM pásiem 169, 433, 868 a 915 MHz [10]. Kľúčovými parametrami modulácie sú:

- **Kódovací pomer** – Coding Rate (CR).
- **Faktor rozprestrenia** – Spreading Factor (SF),
- **Šírka pásma** – Bandwidth (BW),

Zmenou týchto parametrov sa dá ovplyvniť prenosová rýchlosť a robustnosť výsledného signálu vďaka čomu je možné udržať rádiový prenos aj pri nepriaznivých podmienkach.

3.1.1 Kódovací pomer

Kódovací pomer je pomer medzi počtom bitov užitočných dát a celkovým počtom vyslaných bitov. Najčastejšie využívaný pomer v praxi je 4/5, pri aplikáciách s vyššími nárokmi na spoľahlivosť býva pomer 4/7. Hodnota kódovacieho pomeru je určená podľa vzorca:

$$CR = \frac{4}{4+R} \tag{3.1}$$

kde parameter R určuje samostatnú identifikáciu pomeru podľa tab. 3.1.1. K zvýšeniu odolnosti voči rušeniu a na opravu chýb sa v rámci technológie LoRa využíva tzv. FEC (Forward Error Correction).

Tab. 3.1: Kódovací pomer [10].

Kódovací pomer	**Maximálny počet opravených chýb**	**Maximálny počet detekovaných chýb**	**R**
4/5	0	0	1
4/6	0	1	2
4/7	1	2	3
4/8	1	3	4

3.1.2 Technika rozprestreného spektra s využitím CSS

Táto technika prispieva k minimalizovaniu možnosti odposluchu a hlavne k zlepšieniu odolnosti proti rušiacim vplyvom. Napomáha tiež k zmenšeniu potrebného vysielacieho výkonu vďaka čomu sa znižuje spotreba elektrickej energie. Odosielaný signál tak má väčšiu šírku pásma než je šírka pásma originálnej správy.

v rámci LoRa modulácie sa využíva modulačná technika CSS (Chirp Spread Spectrum), pri ktorej je rozprestieranie vykonávané pomocou lineárnej zmeny frekvencie v čase. Maximálna zmena frekvencie definuje šírku pásma prenášaného signálu. Pre LoRa moduláciu sú definované hodnoty 125, 250 a 500 kHz (125 kHz pre EU). Každá zmena frekvencie medzi f_{low} a f_{high} sa nazýva chirp (Compressed High Intensity Radar Pulse). Podla toho, či je zmena frekvencie rastúca, alebo klesajúca je definovaný up-chirp, alebo down-chirp. Dĺžku trvania jedného chirpu ovplyvňuje hodnota SF (faktor rozprestrenia) a použitá šírka pásma. LoRa modulácia definuje celkom šesť úrovní faktoru rozprestrenia (SF7 až SF12). Čím je faktor rozprestrenia

vyšší, tým je nižšia prenosová rýchlosť. Pri zvýšení faktoru rozprestrenia o hodnotu jedna sa pomer kódovania zvýši na dvojnásobok.

Každý chirp je následne možné rozdeliť na ešte menšie jednotky, tzv. čipy. Každý čip vyjadruje jedinečnú hodnotu signálu v rámci chirp modulácie. Skupina čipov tvorí jednotku nazývanú symbol a každý symbol obsahuje 2^{SF} čipov. Pre faktor rozprestrenia SF=12 každý symbol prenáša 12 informačných bitov, takže existuje celkom 4096 jedinečných hodnôt čipov s hodnotou 0 až 4095.

Tab. 3.2: Citlivosť prijímača v závislosti od faktoru rozprestrenia [10].

Faktor rozprestrenia	**Čipy /Symbol**	**Limit SNR**	**Bitová rýchlosť**
7	128	-7,5 dB	5469 b/s
8	256	-10 dB	3125 b/s
9	512	-12,5 dB	1758 b/s
10	1024	-15 dB	977 b/s
11	2048	-17,5 dB	537 b/s
12	4096	-20 dB	293 b/s

3.1.3 Rýchlosť dátového toku

Rýchlosť prenosu dát sa líši v závislosti od faktoru rozprestrenia (SF), šírky pásma (BW) a kódovacieho pomeru (CR). Rýchlosť je v rozmedzí od 22 bit/s (pre šírku pásma 7,8 kHz a SF=12) do 27 kbis/s (pre šírku pásma 500 kHz a SF=7). Teoretickú prenosovú rýchlosť je možné vypočítať podľa vzorca:

$$R_b = SF \cdot \frac{\frac{4}{4+CR}}{\frac{2^{\mathrm{SF}}}{BW}} \qquad [bit/s]. \tag{3.2}$$

3.1.4 Doba prenosu paketu vzduchom

Pre výpočet doby prenosu paketu (Time on Air) je potrebné spočítať pomocné hodnoty. Výpočet rýchlosti symbolu za periódu:

$$T_s = \frac{2^{\mathrm{SF}}}{BW} \qquad [s], \tag{3.3}$$

kde SF je faktor rozprestrenia a BW je šírka pásma. Ďalej je nutné vypočítať preambulu, ktorá je pri LoRaWAN definovaná ako 8 symbolov ($n_{preambula}$):

$$T_{\mathrm{preambula}} = (n_{\mathrm{preambula}} + 4,25) \cdot T_s \qquad [s]. \tag{3.4}$$

Celkový počet symbolov *payloadSymbNb* (payload + hlavička protokolu LoRaWAN) je potom:

$$payloadSymbNb = 8 + max\left(\left[\frac{8PL - 4SF + 28 + 16 - 20H}{4 \cdot (SF - 2DE)}\right] \cdot (CR + 4), 0\right), \tag{3.5}$$

kde:

- **PL** – počet bajtov užívateľských dát (payload),
- **SF** – faktor rozprestrenia,
- **H** – 0 alebo 1, definuje či je použité záhlavie fyzickej vrstvy,
- **DE** – 0 alebo 1, definuje či je povolená optimalizácia pomalého prenosu,
- **CR** – 1 až 4, použitý kódovací pomer.

Výslednú dobu prenosu dátového rámca je možné spočítať podľa vzorca:

$$T_{\text{payload}} = payloadSymbNb \cdot T_s \qquad [s]. \tag{3.6}$$

Celková doba prenosu je potom tvorená vzorcom:

$$T_{\text{paket}} = T_{\text{preambula}} + T_{\text{payload}} \qquad [s]. \tag{3.7}$$

3.2 Linková vrstva

Ako už bolo spomenuté, LoRaWAN je otvorený štandard definujúci linkovú (MAC) vrstvu nad LoRa moduláciou na fyzickej vrstve. Tento protokol bol vyvinutý asociáciou LoRa Alliance. Bol navrhnutý tak, aby spĺňal požiadavky LPWA siete, medzi ktoré patrí vysoký komunikačný dosah s nízkou spotrebou elektrickej energie. Protokol vo všeobecnosti obohacuje LoRa moduláciu o optimalizovanú výdrž batérie (resp. akumulátoru) spoločne s možnosťou QoS (Quality of Service) pre koncové zariadenia.

Napriek tomu, že modulácia LoRa nepatrí medzi open standard, tak protokol LoRaWAN je plne otvorený, čo umožňuje implementáciu privátnych sietí využívajúcich túto technológiu.

3.2.1 LoRaWAN V EU

v rámci Európy sa pre LoRaWAN používa sub-GHz ISM frekvenčné pásmo. Konkrétne sú to frekvencie v oblasti 868 MHz s možnosťou využitia komunikačného kanálu s maximálnou šírkou 125 kHz. Toto rozdelenie umožňuje využitie až 56 kanálov v rámci vyhradeného pásma. Pre uplinkovú komunikáciu sa využíva osem kanálov, ktoré pracujú vo frekvenčnom rozsahu 876,1 až 868,5 MHz ako je znázornené v tab. 3.2.1.

Tab. 3.3: Frekvenčné pásmo pre LoRaWAN v rámci EU [10].

Kanál	**Frekvencia [MHz]**	**SF**	**BW [kHz]**	**DR**
0	868,100	7 -12	125	0 -5
1	868,300	7 -12 (7)	125 (250)	0 -5
2	868,500	7 -12	125	0 -5
3	867,100	7 -12	125	0 -5
4	867,300	7 -12	125	0 -5
5	867,500	7 -12	125	0 -5
6	867,700	7 -12	125	0 -5
7	867,900	7 -12	125	0 -5
8	868,800	FSK modulácia		
RX2	869,525	12	125	0 -5

Na každom z týchto kanálov je možné komunikovať s rôznymi prenosovými rýchlosťami DR0 až DR5, ktoré sú definované šírkou pásma a faktorom rozprestrenia. Druhý kanál tak môže slúžiť na rýchlejšie prenosy vďaka možnosti využitia komunikačného pásma s frekvenčnou šírkou 250 kHz. V uplinkovej komunikácii je tiež vyhradený jeden kanál s frekvenciou 868,8 MHz, ktorý pre prenos používa FSK (Frequency Shift Keying) moduláciu a podporuje maximálnu prenosovú rýchlosť až 50 kb/s. Jeho nevýhodou je však výrazne nižšia citlivosť prijímača v porovnaní s LoRa moduláciou.

Pre downlinkovú komunikáciu sú v prvom prijímacom okne (RX1) využité rovnaké frekvencie ako pri uplinkovej komunikácii. Rovnaké sú aj prenosové rýchlosti. Pre druhé prijímacie okno (RX2) je už vyhradený vlastný komunikačný kanál s frekvenciou 869,525 MHz, ktorý podporuje iba jednu prenosovú rýchlosť. Rozdiel je tiež v použitom prístupe. Uplinková komunikácia používa náhodný mnohonásobný prístup (ALOHA) a downlinková komunikácia používa prístup TDMA (Time Division Multiple Access).

LoRaWAN brána rozoznáva prichádzajúce pakety pomocou preambule so synchronizačným slovom, ktorá je zaslaná pred samotnými užívateľskými dátami (payloadom). V EU je definovaná preambula dĺžky osem symbolov, po ktorých nasleduje synchronizačné slovo kódované down-chirp sekvenciou.

3.2.2 ISM pásmo

Vzhľadom na veľký počet zariadení pracujúcich vo frekvenčnom pásme 868 MHz je nutné zavedenie pravidiel určujúcich pracovné parametre rádiových rozhraní ko-

munikačných modulov z dôvodu koexistencie s ďalšími technológiami. Správne nastavenou striedou je možné znížiť celkový šum vo frekvenčnom spektre. Preto je strieda pevne definovaná štandardmi LoRa Alliance a aj samotným európskym frekvenčným plánom. V sekcii 7.2.3 štandardu ETSI EN300.220 je definovaných päť frekvenčných rozsahov s pevne definovanou striedou. V pásme g a g1, do ktorého spadá technológia LoRaWAN, môže zariadenie vysielať iba po dobu 1% z celkového času, viď tab. 3.2.2. Najčastejšie sa strieda vzťahuje k jednej hodine, čo znamená, že je povolené max 36 sekúnd vysielania počas jednej hodiny.

Strieda (Duty Cycle) je definovaná ako pomer doby trvania $H(\tau)$ a doby trvania celej periódy T:

$$D = \frac{\tau}{T} \quad [-; s; s] \quad alebo \quad DCL = \frac{\tau}{T \cdot 100\%} \quad [\%; s; s]. \tag{3.8}$$

Tab. 3.4: Strieda v jednotlivých frekvenčných pásmach[10].

Označenie	**Pásmo [MHz]**	**Strieda [%]**
g	863,0-868,0	1
g1	868,0-868,6	1
g2	868,7-869,2	0,1
g3	869,4-869,65	10
g4	869,7-870,0	1

Okrem limitácie pracovného cyklu je vyhláškou upravený aj maximálny vysielací výkon. Pre pásmo 868 MHz je výkon obmedzený na 14 dBm.

3.2.3 2,4 GHz pásmo

Spoločnosť Semtech nedávno vydala LoRa chipset, ktorý dokáže pracovať v 2,4 GHz pásme. Presunutie zo sub-GHz pásiem na 2,4 GHz frekvenciu bolo podnietené globálne dostupným 2,4 GHz ISM frekvenčným pásmom. Táto možnosť má vyriešiť problém nutnosti výroby viacerých chipsetov, z ktorých každý pracuje len na určitej frekvencii. Týmto spôsobom by stačil jeden univerzálny chipset, ktorý by bolo možné použiť kdekoľvek na svete.

Vysielanie LoRaWAN zariadení v sub-GHz pásme je limitované striedou (Duty Cycle), preto musia byť použité pre aplikácie, ktorénevyžadujú frekventovanú prevádzku. Zariadenia pracujúce na 2,4 GHz frekvencii sú schopné posielať väčší objem dát vďaka väčšej šírke pásma. Vďaka tomu je možné implementovať aplikácie, ktoré vyžadujú posielanie väčšieho objemu dát pri zachovaní vysokého komuni-

kačného dosahu oproti iným technológiám pracujúcich v 2,4 GHz pásme ako WiFi či Bluetooth. Väčšia šírma pásma tiež zvyšuje presnosť určovania polohy zariadenia.

Tab. 3.5: Parametre prenosu [11].

Parameter	**Symbol**	**Hodnota**	**Jednotka**
Frekvencia	f	2,4	GHz
Faktor rozprestrenia	SF	7-12	-
Šírka pásma	BW	203/406/812/1625	kHz
Kódovací pomer	R_C	4/5	-
Vysielací výkon	P_{TX}	12,5	dBm
Zisk vysielacej antény	G_{TX}	2	dBi
Útlm na káblovom vedení vysielača	L_{TX}	2	dB
Zisk prijímacej antény	G_{RX}	2	dBi
Útlm na káblovom vedení prijímača	L_{RX}	2	dB

Pre získanie maximálneho možného dosahu pri frekvencii 2,4 GHz je nutné vypočítať maximálnu senzitivitu prijímača P_{RX}. Senzitivita prijímača závisí na faktore rozprestrenia (SF) a šírke pásma (BW). Použiteľné sú všetky možné faktory rozprestrenia (7-12) a možné šírky pásma pre LoRa moduláciu sú 203, 406, 812 a 1625 kHz. Rôznymi kombináciami faktoru rozprestrenia a šírky pásma dostávame rôzne hodnoty rýchlosti prenosu dát a tým pádom aj rôzne hodnoty senzitivity prijímača, viď tab. 3.2.3.

Tab. 3.6: Prijatý výkon (P_{RX}) a rýchlosť prenosu dát (R_D) v závislosti od faktoru rozprestrenia (SF) a šírky pásma (BW) [11].

BW [kHz]								
	203		**406**		**812**		**1625**	
SF [-]	P_{RX} $[dBm]$	R_D $[kbit/s]$	P_{RX} $[dBm]$	R_D $[kbit/s]$	P_{RX} $[dBm]$	R_D $[kbit/s]$	P_{RX} $[dBm]$	R_D $[kbit/s]$
7	-115	11,1	-113	22,2	-112	44,41	-106	88,87
8	-118	6,34	-116	12,69	-115	25,38	-109	50,78
9	-121	3,57	-119	7,14	-117	14,27	-111	28,56
10	-124	1,98	-122	3,96	-120	7,93	-114	15,87
11	-127	1,09	-125	2,18	-123	4,36	-117	8,73
12	-130	0,595	-128	1,19	-126	2,38	-120	4,76

Výpočet rýchlosti prenosu dát:

$$R_{\mathrm{b}} = \frac{SF \cdot BW}{2^{\mathrm{SF}}} \qquad [kbit/s]. \tag{3.9}$$

Celkový prijatý výkon bude potom:

$$P_{\mathrm{RX}} = P_{\mathrm{TX}} + G_{\mathrm{TX}} - L_{\mathrm{TX}} - L_{\mathrm{p}}(d) + G_{\mathrm{RX}} - L_{\mathrm{RX}} \quad [dBm], \tag{3.10}$$

kde P_{TX} je vysielací výkon v dBm, G_{TX} je zisk vysielacej antény v dBi, L_{TX} je útlm na káblovom vedení vysielača v dB, $L_p(d)$ je útlm v dB v závislosti na vzdialenosti, G_{RX} je zisk prijímacej antény v dBi a L_{RX} je útlm na káblovom vedení prijímača v dB.

Komunikačná vzdialenosť a rýchlosť prenosu tiež závisia od oblasti použitia. Oblasti použitia môžme rozdeliť na tri rôzne prostredia: volné prostredie s priamym dohľadom (LoS), interiér a mestská oblasť. V každom prípade maximálna rýchlosť prenosu logaritmicky klesá so zvyšujúcim sa komunikačným dosahom [11].

Volné prostredie s priamym dohľadom (LoS)

Vo volnom prostredí s priamym dohľadom (LoS) medzi vysielačom a prijímačom je možné využiť Free Space Path Loss (FSPL) model. Tento model vypočítava útlm medzi dvoma rádiovými zariadeniami vo voľnom priestore bez akýchkoľvek prekážok, odrazu či rušenia. Model sa pre výpočet útlmu opiera výlučne o frekvenciu a vzdialenosť medzi vysielačom a prijímačom:

$$L_{\mathrm{p,LoS}}(d) = 32,44 + 20log_{10}(f) + 20_{10}(d) \quad [dB], \tag{3.11}$$

kde f je frekvencia v MHz a d je vzdialenosť v km. Kombináciou rôzneho faktoru rozprestrenia (SF) a šírky pásma (BW) dostávame rôznu senzitivitu P_{RX}. Následne môžme vypočítať maximálnu komunikačnú vzdialenosť:

$$d = 10^{(\mathrm{L_{p,LoS}(d)\text{-}32,44\text{-}20log_{10}(f))/20}} \quad [km]. \tag{3.12}$$

Teoreticky je vo voľnom prostredí možné dosiahnuť komunikačnú vzdialenosť až 133 km čo je však v reálnom prostredí nedosiahnuteľné [11].

Interiér

V interíerovom nasadení je možné využiť Indoor Dominant Path (IDP) model [12]. Celkový útlm je súčtom vzdialenostného útlmu, akumulovaného útlmu na prekážkach (napr. steny, dvere a okná) a útlmom spôsobenom vzájomným pôsobením prítomných rádiových technológií využívajúcich rovnaké frekvenčné pásmo:

$$L_{\mathrm{p,in}}(d) = L_{\mathrm{p_0}}(d_0 + 10 \cdot n \cdot log_{10}(\frac{d}{d_0}) + \sum_i L_{\mathrm{P_i}} + \sum_j L_{\mathrm{V_j}} \quad [dB], \tag{3.13}$$

kde $L_{p_0}(d_0)$ je útlm vo vzdialenosti d_0 a n je exponent útlmu. Akumulovaný útlm na prekážkach je súčtom útlmov na všetkých prekážkach. Útlm spôsobený vzájomným pôsobením je súčtom všetkých útlmov L_{V_j}.

Kvôli všestrannosti modelu sú niektoré parametre predom nastavené na obvykle používané hodnoty. $L_{p_0}(d_0)$ je 40 dB vo vzdialenosti $d_0 = 1$ m. Pre akumulovaný útlm na prekážkach a útlm spôsobený vzájomným pôsobením sú určené hodnoty 6 a 3 dB [12]. Exponent útlmu je nastavený na $n = 5$ [13]. Následne je výpočet možné zvjednodušiť:

$$L_{\mathrm{p,in}}(d) = 40 + 5 \cdot 10 \cdot log_{10}(d) + 6 + 3 \quad [dB]. \tag{3.14}$$

Z toho je možné odvodiť výpočet komunikačného dosahu:

$$d = 10^{(\mathrm{L_{p,in}(d)\text{-}49})/50} \quad [m]. \tag{3.15}$$

Napríklad v prípade použitia faktoru rozprestrenia SF = 12 a najnižšej šírky pásma BW = 203 kHz bude útlm $\mathrm{L_{p,in}(d)} = 142{,}5$ dB. Následne bude maximálna komunikačná vzdialenosť d = 74 m s maximálnou prenosovou rýchlosťou $\mathrm{R_b} = 0{,}595$ kbit/s. V opačnom prípade je možné dosiahnuť maximálnu vydialenosť až d = 18 m s maximálnou prenosovou rýchlosťou $\mathrm{R_b} = 253{,}91$ kbit/s [11].

Mestská oblasť

Pre túto oblasť použitia je využitý Electronic Communication Committee (ECC-33) model [14]. Výpočet útlmu:

$$L_{\mathrm{p,mo}}(d) = A_{\mathrm{vp}} + A_{\mathrm{zm}} + G_{\mathrm{v}} + G_{\mathrm{p}} \quad [dB], \tag{3.16}$$

kde A_{vp} je útlm volného prostredia, A_{zm} je základný medián útlmu, G_v je výkonostný zisk vysielača a G_p výkonostný zisk prijímača. Výpočet daných parametrov:

$$A_{\mathrm{vp}} = 92,4 + 20log_{10}(d) + 20log_{10}(f) \quad [dB], \tag{3.17}$$

$$A_{\mathrm{zm}} = 20,41 + 9,83log_{10}(d) + 7,894log_{10}(f) + 9,56[log_{10}(f)]^2 \quad [dB], \tag{3.18}$$

$$G_{\mathrm{v}} = log_{10}\left(\frac{h_{\mathrm{b}}}{200}\right)\{13,958 + 5,8[log_{10}(d)]^2\} \quad [dBi], \tag{3.19}$$

$$G_{\mathrm{p}} = [42,57 + 13,7log_{10}(f)][log_{10}(h_{\mathrm{m}}) - 0,585] \quad [dBi]. \tag{3.20}$$

Maximálnu vzdialenosť získame iterovaním hodnoty d od 1 m do 10 km v každej rovnici, čím získame odpovedajúci útlm $L_{p,mo}(d)$.

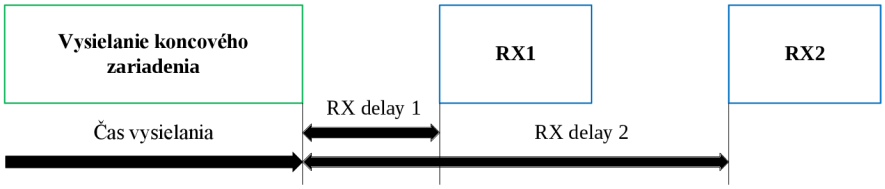
Najvyšší komunikačný dosah môže byť až d = 443 m pri prenosovej rýchlosti $\mathrm{R_b} = 0{,}595$ kbit/s, naopak pri najvyššej prenosovej rýchlosti $\mathrm{R_b} = 253{,}91$ kbit/s dosiahneme komunikačný dosah d = 3 m [11].

3.3 Triedy koncových zariadení

Špecifikácia LoRaWAN protokolu definuje tri triedy koncových zariadení. Sú to zariadenia triedy A, B a C. Trieda A je základnou implementáciou pre všetky koncové zariadenia a je vždy podporovaná. Triedy B a C rozširujú triedu A a ich implementácia nie je povinná.

3.3.1 Trieda A

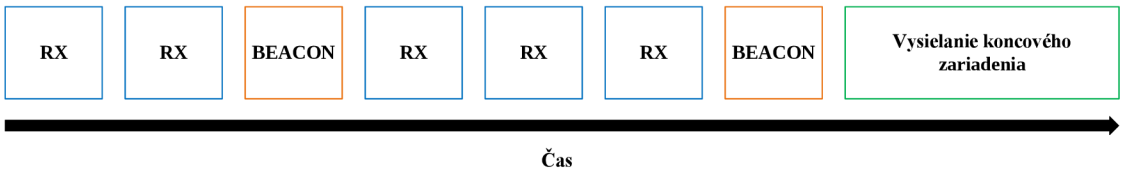
Koncové zariadenia triedy A podporujú obojsmernú komunikáciu, kde je každá uplinková komunikácia nasledovaná dvoma krátkymi downlinkovými oknami ako je znázornené na obr. 3.2. Vždy by malo byť pre downlinkovú komunikáciu využité len jedno z týchto dvoch okien. Teda ak prenos neprebehne v RX1 tak môže byť využité RX2. Ak prenos prebehne v RX1 tak v RX2 by už prenos prebehnúť nemal. Jedná sa o energeticky najúspornejšie riešenie. Downlinková komunikácia v inom čase teda musí vyčkať kým nebude prijatá uplinková správa z koncového zariadenia.



Obr. 3.2: Priebeh komunikácie zariadenia triedy A [10].

3.3.2 Trieda B

Koncové zariadenia triedy B podporujú obojsmernú komunikáciu s plánovanými prijímacími oknami. Oproti triede A, zariadenie triedy B otvára prijímacie okná v presne plánovaných intervaloch ako je možné vidieť na obr. 3.3. Koncové zariadenie otvára okná v správnych intervaloch na základe prijatého synchronizačného Beacon rámca.

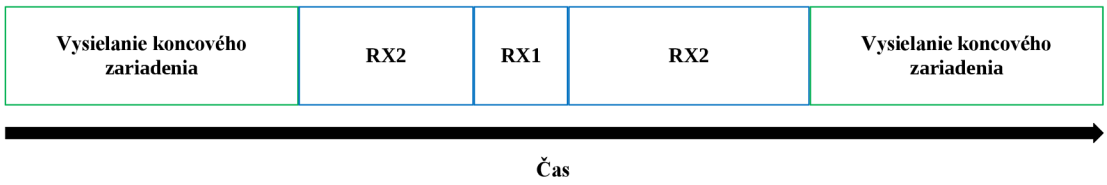


Obr. 3.3: Priebeh komunikácie zariadenia triedy B [10].

3.3.3 Trieda C

Koncové zariadenia triedy C podporujú obojsmernú komunikáciu s maximálnym využitím počtu prijímacích okien. Zariadenie teda má otvorené prijímacie okná takmer vždy, mimo času kedy samo vysiela, ako je znázornené na obr. 3.4. Výhodou je

prenos dát s nízkym opozdením za cenu vyššej spotreby elektrickej energie. Zariadenia triedy C sú teda primárne napájané z elektrickej siete a nie vstavanou batériou (resp. akumulátorom).



Obr. 3.4: Priebeh komunikácie zariadenia triedy C [10].

3.4 Metódy aktivácie koncových zariadení

Každé koncové zariadenie, ktoré sa chce pripojiť do siete a komunikovať je potrebné na začiatku aktivovať. K aktivácii je možné využiť jednu z dvojice aktivačných metód ABP (Activation By Personalization), alebo OTAA (Over The Air Activation). Pred samotnou aktiváciou je do koncového zariadenia nutné nahrať potrebné aktivačné, či k aktivácii potrebné kľúče. Pomocou týchto kľúčov je možné následne šifrovať komunikáciu.

3.4.1 Over The Air Activation (OTAA)

Pri aktivácii OTAA sa predom do koncového zariadenia nahrajú iba kľúče *DevEUI*, *AppEUI* a *AppKey*. Pomocou týchto kľúčov sú odvodené ďalšie kľúče *NwkSKey* a *AppSKey*, ktoré slúžia na šifrovanie komunikácie. Na získanie šifrovacích kľúčov je nutná výmena join správy medzi koncovým zariadením a bránou.

Pri LoRaWAN štandarde v 1.0 (vo verzii 1.1 je proces upravený a sú zavedené nové kľúče zvyšujúce bezpečnosť) join-request správa pozostáva z kľúča *DevEUI*, *AppEUIAppEUI* a dvoch náhodne spočítaných bajtov DevNonce. Správa nie je šifrovaná, no je k nej pripojený MIC (Message Integrity Code) spočítaný s využitím kľúča AppKey. Správa join-request je bránou prijatá, pokiaľ je hodnota MIC správna a náhodná hodnota DevNonce ešte nebola zariadením použitá. Následne je zariadeniu odoslaná odpoveď join-accept, ktorá obsahuje pridelenú adresu zariadenia v lokálnej sieti DevAddr, trojbajtové slovo AppNonce a identifikátor siete NetID spoločne s ďalšími komunikačnými parametrami. Koncové zariadenie si následne s využitím AppKey, AppNonce a NetID odvodí šifrovacie kľúče AppSKey a NwkSKey.

3.4.2 Activation By Personalization (ABP)

V prípade aktivácie ABP sú všetky kľúče vrátane šifrovacích predom uložené do koncového zariadenia pred aktiváciou. Vďaka tomu už následne nie je potrebná výmena správ medzi koncovým zariadením a bránou nutných pre odvodenie šifrovacích kľúčov. Táto forma aktivácie však predstavuje bezpečnostné riziko v prípade fyzického odcudzenia zariadenia. Útočník tak získa šifrovacie kľúče a identita zariadenia môže byť zneužitá.

3.5 Sieťová architektúra

Architektúra siete je založená na topológii v tvare hviezdy. Koncové zariadenia nie sú previazané so špecifickou bránou. Naopak, správa vyslaná jedným koncovým zariadením môže byť prijatá niekoľkými bránami. Každá brána následne preposiela prijaté správy z koncových uzlov na server pomocou backbone siete. Server následne filtruje redundantné správy, vykonáva bezpečnostné kontroly, plánuje potvrdenia cez optimálne brány, kontroluje adaptívnu prenosovú rýchlosť atď. Ak je koncové zariadenie mobilné, tak nie je potrebné aby si jednotlivé brány predávali dáta medzi sebou, čo je kľúčová funkcia na zaistenie sledovania koncového zariadenia [15].

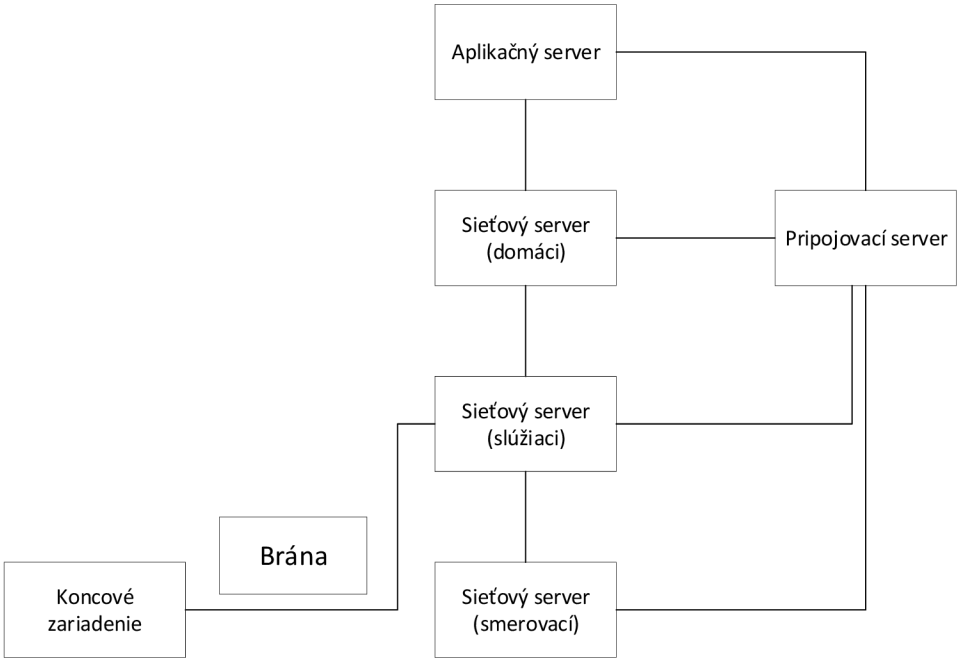
Referenčný model siete LoRaWAN je možné vidieť na obr. 3.5. Sieť sa skladá z koncových zariadení, brán, sieťových serverov, pripojovacích serverov a aplikačných serverov.

3.5.1 Koncové zariadenie

Koncové zariadenie je tvorené senzorom a je pripojené bezdrôtovo do siete pomocou brány. Aplikačná vrstva koncového zariadenia komunikuje so zodpovedajúcim aplikačným serverom, ktorý spracováva odosielané dáta.

3.5.2 Brána

Brána slúži na smerovanie všetkých prijatých paketov z koncových zariadení na sieťový server, ktorý je pripojený cez IP backbone sieť. Brána funguje iba na fyzickej vrstve a jej úlohou je dekódovať uplinkové správy zo vzduchu a posielať ich ďalej v nespracovanej podobe na sieťový server. Pri downlinkovej komunikácii brána jednoducho odošle správy zo sieťového servera na koncové zariadenie bez akéhokoľvek zásahu do payloadu.



Obr. 3.5: Referenčný model siete LoRaWAN [16].

3.5.3 Sieťový server

Sieťový server predstavuje linkovú vrstvu koncových zariadení v LoRaWAN sieti a je jadrom hviezdicovej topológie. Hlavnými úlohami sieťového servera sú:

- Kontrola adresy koncového zariadenia,
- Kontrola počítadla rámcov a overovanie rámcov,
- Potvrdzovanie,
- Prispôsobenie prenosovej rýchlosti,
- Vybavovanie všetkých požiadaviek od koncového zariadenia týkajúcich sa linkovej vrstvy,
- Smerovanie uplinkovej komunikácie na príslušný aplikačný server,
- Zaraďovanie downlinkových správ z aplikačných serverov, ktoré sa majú ďalej posielať na koncové zariadenia,
- Smerovanie správ join-request a join-accept medzi koncovým zariadením a pripojovacím serverom.

V prípade roamingu sa v sieti môže nachádzať viac sieťových serverov, pričom každý z nich plní inú úlohu. Všetko záleží či je koncové zariadenie v roamingu a aký typ roamingu používa.

Slúžiaci sieťový server riadi linkovú vrstvu koncového zariadenia. V domácom sieťovom serveri sú uložené informácie koncového zariadenia ako profil zariadenia, servisný profil, smerovací profil a DevEUI. Domáci sieťový server je priamo spojený

s pripojovacím serverom, ktorý sa používa pri aktivačnej procedúre. Je tiež pripojený na aplikačný server. V prípade, že domáci sieťový server a slúžiaci sieťový server pracujú osobitne, majú medzi sebou roamingovú dohodu. V tomto prípade sú medzi nimi smerované uplinkové a downlinkové správy.

3.5.4 Pripojovací server

Pripojovací server spracováva OTAA aktivácie koncových zariadení. Na sieťový server môže byť pripojených niekoľko pripojovacích serverov a naopak, pripojovací server môže byť pripojený na niekoľko sieťových serverov.

Koncové zariadenie sa cez join-request pomocou JoinEUI dotazuje na konkrétny prpojovací server. Každý pripojovací server má nastavenú unikátnu hodnotu JoinEUI. Vo verzii LoRaWAN protokolu 1.0 sa hodnota JoinEUI nazýva AppEUI. Pripojovací server pozná identifikátor domáceho sieťového servera koncového zariadenia a poskytuje túto informáciu ostatným sieťovým serverom na požiadavku v prípade roamingu.

Pripojovací server má potrebné informácie na spracovanie join-request správy obdržanej uplinkovou komunikáciou a následne dokáže vygenerovať join-accept správu a poslať ju downlinkovou komunikáciou. Na tomto serveri tiež prebieha odvodzovanie aplikačných a relačných šifrovacích kľúčov. Následne pošle príslušný NwkSKey koncového zariadenia na sieťový server a AppSKey na príslušný aplikačný server. Pripojovací server by mal obsahovať informácie každého koncového zariadenia pod jeho správou:

- DevEUI,
- AppKey,
- NwkKey (iba v prípade koncového zariadenia pracujúcoom s verziou LoRaWAN protokolu 1.1),
- Identifikátor domáceho sieťového servera,
- Identifikátor aplikačného servera,
- Schopnosť vybrať najlepšiu cestu na komunikáciu s koncovým zariadením,
- Verziu LoRaWAN protokolu koncového zariadenia.

Kľúče NwkKey a AppKey sú prístupné iba na pripojovacom serveri a koncovom zariadení. Nikdy sa neposielajú na sieťový či aplikačný server.

Pripojovací spolu so sieťových serverom by mali byť schopné sprevádzkovať medzi sebou zabezpečenú komunikáciu, ktorá obsahuje end-point autentifikáciu, ochranu integrity a diskrétnosť. Podobne by mal pripojovací server bezpečne doručiť AppSKey na príslušný aplikačný server. Pripojovací server môže byť pripojený na niekoľko aplikačných serverov a rovnako aplikačný server môže byť prepojený s niekoľkými pripojovacími servermi.

3.5.5 Aplikačný server

Aplikačný server sa stará o celý payload (užitočné dáta) na aplikačnej vrstve priradených koncových zariadení. Generuje tiež celý aplikačný payload pre downlinkovú komunikáciu s koncovým zariadením. Na sieťový server môže byť pripojených niekoľko aplikačných serverov. Aplikačný server môže byť rovnako pripojený na niekoľko sieťových serverov. Domáci sieťový server smeruje celú uplinkovú komunikáciu príslušnému aplikačnému serveru na základe DevEUI.

3.6 Bezpečnosť

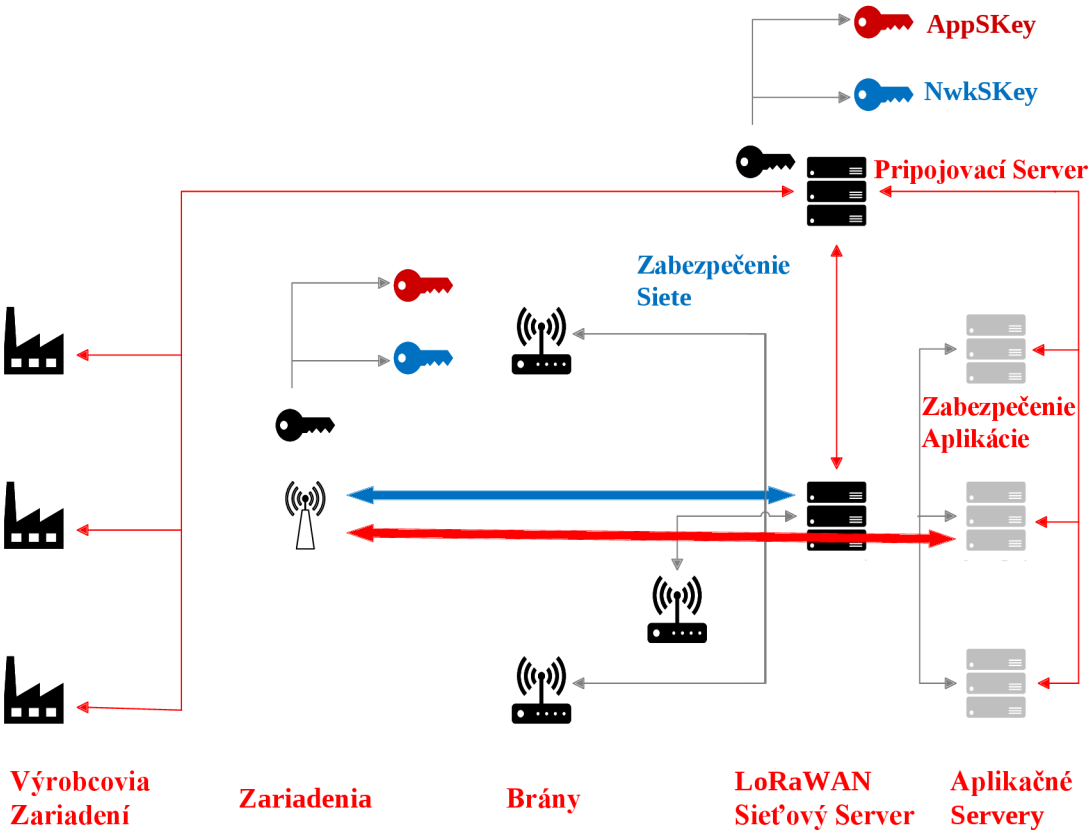
LoRaWAN pre zaistenie bezpečnosti používa dve vrstvy. Prvá je pre samotnú sieť a druhá slúži na zabezpečeniu aplikačných dát. Sieťová bezpečnostná vrstva zabezpečuje autentičnosť uzla v sieti, zatiaľ čo aplikačná bezpečnostná vrstva zabezpečuje aby sieťový operátor nemal prístup k aplikačným dátam koncového užívateľa. Používa sa šifrovanie AES s výmenným kľúčom použitím IEEE EUI64 identifikátora [15].

Bezpečnostné riešenie protokolu LoRaWAN je navrhnuté tak, aby podporovalo hlavné kritériá protokolu a to nízku spotrebu elektrickej energie, nízku náročnosť realizácie, nízku cenu zariadenia a širokú škálovateľnosť. Tým, že sa koncové zariadenia dané do prevádzky používajú dlhú dobu (niekoľko rokov), musí byť bezpečnosť zaistená aj do budúcna. Bezpečnostný dizajn protokolu dodržiava najmodernejšie princípy, medzi ktoré patrí použitý štandard, dobre preverené algoritmy a end-to-end zabezpečenie.

Počas procesu pripojenia k sieti sa medzi LoRaWAN koncovým zariadením a sieťou vytvára vzájomná autentifikácia. Vďaka tomu je zabezpečené, že iba overené zariadenia sa môžu pripojiť do siete. Aplikačné a MAC (Media Access Control) správy majú overený pôvod, chránenú integritu, sú chránené pred opakovaním a sú šifrované. Táto ochrana, spojená so vzájomnou autentifikáciou, zaisťuje aby obsah sieťového prenosu nebol zmenený a pochádzal od legitímneho zariadenia, tak isto aj to, že nie je možné zariadenie odpočúvať či komunikáciu zachytávať útočníkom. Bezpečnnosť protokolu ďalej zahŕňa aj end-to-end šifrovanie pre aplikačné dáta vymieňané medzi koncovým zariadením a aplikačným serverom. LoRaWAN je jeden z mála protokolov v IoT, ktorý používa end-to-end zabezpečenie. V niekotrých tradičných mobilných sieťach je prenos šifrovaný iba pri prenose vzduchom, inak je posielaný ako obyčajný text v backbone sieti operátora. V dôsledku toho sú používatelia zaťažený výberom, používaním a spravovaním ďalšej bezpečnostnej vrstvy (väčšinou vo forme VPN, alebo šifrovaním na aplikačnej úrovni). Takéto riešenia sa však vôbec nehodia pre použitie v LPWAN technológii, kde prídavná bezpečnostná zložka značne zvyšuje spotrebu elektrickej energie, náročnosť a cenu zariadenia [17].

3.6.1 Implementácia bezpečnosti

Bezpečnostné mechanizmy protokolu LoRaWAN sa opierajú o osvedčené a štandardizované kryptografické algoritmy AES (Advanced Encryption Standard). Tieto algoritmy boli analyzované kryptografickou komunutou po veľa rokov, sú schválené inštitútom NIST [18] (National Institute of Standards and Technology) a sú široko používané ako najlepšie šifrovacie algoritmy pre uzly a siete. LoRaWAN používa na zabezpečenie AES šifrovanie kombinované s niekoľkými režimami prevádzky: CMAC (Cipher-based Message Authentication Code[1]) pre ochranu integrity a CTR (Counter Mode Encryption[2]) na šifrovanie. Každé LoRaWAN koncové zariadenie je vyrobené s unikátnym 128 bitovým AES kľúčom (AppKey) a globálne unikátnym identifikátorom (EUI-64-based DevEUI). Obe tieto vlastnosti zariadenia sa používajú pri procese overovania zariadenia. Podobne sú aj LoRaWAN siete identifikované podľa 24 bitového, globálne unikátneho identifikátora prideleného od LoRa Alliance [17]. Implementáciu bezpečnosti je možné vidieť aj graficky znázornenú na obr. 3.6.



Obr. 3.6: Zabezpečenie siete LoRaWAN [17].

[1]CMAC je šifrovací autentifikačný kód pre správy.
[2]CTR je režim činnosti algoritmu AES, ktorý sa opiera o počítadlo na šifrovanie toku dát.

3.6.2 Zabezpečenie aplikačných dát

Aplikačné dáta sú vždy šifrované end-to-end medzi koncovým zariadením a aplikačným serverom. Ochrana integrity je zaistená dvoma krokmi. Prvým krokom je ochrana integrity počas prenosu vzduchom poskytnutá LoRaWAN protokolom. Druhým krokom je zabezpečenie medzi sieťovým a aplikačným serverom použitím zabezpečeného prenosu pomocou protokolov ako sú HTTPS a VPN.

Pri aktivácii koncového zariadenia metódou OTAA sa overuje, že koncové zariadenie aj sieť majú informáciu o AppKey. Overuje sa to na základe výpočtu AES-CMAC[3] (s použitím AppKey) pri požiadavke zariadenia o pripojenie a tiež aj backendovým prijímačom. Ďalej sú odvodené dva kľúče relácie. Jeden zabezpečuje integritu a šifrovanie LoRaWAN MAC príkazov a aplikačných dát (NwkSKey) a druhý slúži na šifrovanie end-to-end aplikačných dát (AppSKey). NwkSKey je distrubuovaný LoRaWAN sieti pre overenie autentičnosti a integrity správ. AppSKey je potom distribuovaný aplikačnému serveru na šifrovanie a dešifrovanie aplikačných dát. AppKey a AppSKey sú ukryté pre sieťového operátora aby nemohol dešifrovať aplikačné dáta [17].

Všetky LoRaWAN prenosy sú chránené použitím dvoch kľúčov v relácii. Všetky dáta sú šifrované pomocou AES-CTR a obshujú počítadlo rámcov (používa sa na zamedzenie opakovania správ) a MIC (Message Integrity Code) vypočítaný pomocou AES-CMAC (aby sa predišlo neoprávnenému zásahu do správy). Časti LoRaWAN správy sú zobrazené na obr. 3.7.

Obr. 3.7: Štruktúra LoRaWAN správy a jej zabezpečenie [17].

[3]CMAC s použitím AES algoritmu pre zabezpečenie integrity a autentičnosti správy.

4 LoRaWAN v NS-3

Súčasťou tejto práce je implementácia LoRaWAN modulu do simulačného prostredia NS-3. Táto kapitola sa preto bude venovať samotnému simulačnému prostrediu a následne bude popísaný vybraný LoRaWAN modul, ktorý bude neskôr implementovaný v simulačnom prostredí.

4.1 Network Simulator 3

NS-3 je diskrétny sieťový simulátor s hlavným zameraním na vývoj a vzdelávanie. Jedná sa o voľne stiahnuteľný program s GNU GPLv2 licenciou, ktorý je voľne dostupný verejnosti na používanie. Cieľom NS-3 projektu je vyvinúť voľne dostupné open source simulačné prostredie vhodné pre sieťový vývoj.

Projekt NS-3 je zameraný na vývoj simulačného jadra s vhodnou dokumentáciou, ktoré sa jednoducho používa a spravuje, a ktoré vyhovuje potrebám celej simuálcii od konfigurácie až po zber informácii a ich analýzu. Programová infraštruktúra NS-3 podporuje vývoj simulačných modelov, ktoré sú dostatočne realistické na to, aby umožnili použitie NS-3 ako emulátora siete v reálnom čase, prepojeného s reálnou sieťovou implementáciou. Simulačné jadro podporuje výskum sietí, ktoré sú, ale aj nie sú IP orientované. Väčšia časť sa však zameriava na bezdrôtové IP simulácie, medzi ktoré patrí WiFi, LTE, ale aj iné bezdrôtové systémy na prvej a druhej vrstve. Taktiež populárnym zameraním sú výkonostné TCP simulácie či mobilné ad–hoc smerovacie protokoly. Podporovaný je aj plánovač v reálnom čase, ktorý uľahčuje prípady ako sú in-the-loop simulácie pre interakciu s reálnym systémom. Používatelia tak môžu vysielať a prijímať pakety generované simulátorom na reálnych sieťových zariadeniach. Ďalším dôrazom simulátora je opätovné použitie reálnej aplikácie a kódu jadra. Prostredie Direct Code Execution umožňuje používateľom spúšťať C a C++ aplikácie, alebo sieťový zásobník jadra Linux [19].

4.2 Modul LoRaWAN

Pre účely simulácie v NS-3 bol vybraný LoRaWAN modul od SIGNET Lab[1], konkrétne od autorov Davide Magrin, Martina Capuzzo, Stefano Romagnolo a Michele Luvisotto. Tento modul stále v súčastnej dobe udržovaný s poslednou úpravou 26.7.2021.

Modul obsahuje dva hlavné modely: prvý pre LoRa fyzickú vrstvu, ktorý reprezentuje LoRa chirpy a správanie LoRa prenosov, a druhý pre LoRaWAN linkovú

[1]Modul je dostupný z: https://github.com/signetlabdei/lorawan

(MAC) vrstvu, ktorý zabezpečuje správanie podľa potrebných oficiálnych špecifikácií.

Na reprezentáciu týchto dvoch modelov obsahuje modul dve triedy: `LoraPhy` a `LorawanMac`. Tieto triedy sú ďalej rozšírené ďalšími triedami, ktoré modelujú charakteristické vlastnosti koncových zariadení (ED) a brány (GW). V stručnosti, fyzická vrstva môže byť modelovaná použitím `EndDeviceLoraPhy` a `GatewayLoraPhy` triedami, zatiaľ čo objekty triedy `GatewayLorawanMac`, `EndDeviceLorawanMac` a `ClassAEndDeviceLorawanMac` sú použité na reprezentáciu linkovej (MAC) vrstvy. V sieti sa ďalej nachádza zariadenie, na ktoré je možné nainštalovať `NetworkServer` aplikáciu, ktorá spravuje sieť cez brány. Na brány je následne nainštalovaná aplikácia `Forwarder`, ktorá využíva komunikačné schopnosti brány na preposielanie paketov zo sieťového serveru na koncové zariadenia [20].

4.2.1 Model fyzickej vrstvy

Model fyzickej vrstvy musí vzať do úvahy dve kľúčové vlastnosti LoRa modulácie čo je senzitivita a ortogonalita pre zisťovanie, či prenos prebehol úspešne.

Na prepojenie fyzickej vrstvy všetkých komunikujúcich zariadení v sieti slúži trieda `LoraChannel`. Trieda udržiava zoznam všetkých pripojených zariadení a informuje dané zariadenia o prichádzajúcej komunikácii podľa rovnakého vzoru ako triedy `Channel` v NS-3.

Fyzické vrstvy všetkých pripojených zariadení k prenosovému kanálu sú vystavené `StartReceive` metóde, ktorá dovoľuje kanálu započať prenos na určenom zariadení. Všetky triedy, ktoré pracujú s fyzickou vrstvou sa opierajú o objekt `LoraInterferenceHelper`, kvôli sledovaniu všetkých prichádzajúcich paketov, či už sa jedná o očakávané správy alebo iba rušenie. Akonáhle kanál oboznámi fyzickú vrstvu o prichádzajúcom pakete, fyzická vrstva následne informuje svoj `LoraInterferenceHelper` o prichádzajúcej komunikácii. V prípade, že fyzická vrstva spĺňa určité predpoklady, môže byť prichádzajúci paket prijatý. Jedná sa o nasledujúce predpoklady:

1. Prijímač musí byť nečinný (v STANDBY réžime) v momente volania funkcie `StartReceive`,
2. Výkon prijímaného paketu musí byť nad prahom citlivosti prijímača,
3. Prijímač musí naslúchať na správnej frekvencii,
4. Prijímač musí naslúchať na správnom faktore rozprestrenia (SF).

Prah citlivosti prijímača pre konkrétnu hodnotu faktoru rozprestrenia (SF) je možné vidieť v tab. 4.1.

Hneď ako sa začne samotný príjem prichádzajúceho paketu je naplánovaná funkcia `EndReceive`, ktorá sa spustí po prijatí celého paketu. Po celú dobu prenosu

je uvažovaný konštantný prijímací výkon. Po ukončení prenosu zavolá funkcia `EndReceive` metódu `IsDestroyedByInterference`, ktorá vyhodnotí či bol paket stratený kvôli rušeniu.

Tab. 4.1: Prah citlivosti prijímača v závisloti od faktoru rozprestrenia (SF) [20].

SF7	-124 [dBm]
SF8	-127 [dBm]
SF9	-130 [dBm]
SF10	-133 [dBm]
SF11	-135 [dBm]
SF12	-137 [dBm]

Funkcia `IsDestroyedByInterference` porovnáva prijímací výkon prijímaného paketu s výkonom interferujúcich paketov na báze faktoru rozrestrenia (SF). Konkrétne sa porovnáva hodnota SIR s izolačnou maticou uvedenou v tab. 4.2.1.

Tab. 4.2: Izolačná matica pre porovnanie hodnoty SIR prijímaného paketu s interferujúcimi paketmi [20].

	SF7	**SF8**	**SF9**	**SF10**	**SF11**	**SF12**
SF7	6	-16	-18	-19	-19	-20
SF8	-24	6	-20	-22	-22	-22
SF9	-27	-27	6	-23	-25	-25
SF10	-30	-30	-30	6	-26	-28
SF11	-33	-33	-33	-33	6	-29
SF12	-36	-36	-36	-36	-36	6

Čipy inštalované na LoRa bránach musia obsahovať 8 paralelných prijímacích ciest, kvôli možnosti prijímania viacerých paketov paralelne. Táto skutočnosť je v simulačnom prostredí zabezpečená objektom `ReceptionPath`, ktorý pôsobí ako `EndDeviceLoraPhy`, zameriavaním sa na príjem prichádzajúcich paketov a ich vzájomným porovnávaním. Týmto spôsobom sa kontroluje správnosť prenosu za použitia `LoraInterferenceHelper` na bráne. `GatewayLoraPhy` je tak správcom skupiny objektov `ReceptionPath`. Počas prenosu paketu brána vybraný prenosový kanál označí ako obsadený. Potom, ako je prenos ukončený funkciou `EndReceive`, je spustený `LoraInterferenceHelper`, ktorý vyhodnotí, či prenos prebehol v poriadku.

Na vytvorenie konzistentného modelu musia prijímacie cesty spĺňať niektoré ďalšie predpoklady:

- Prijímacie cesty môžu byť nastavné aby naslúchali na akejkoľvek frekvencii,
- Prijímacie cesty môžu byť voľne alokované na dostupných frekvenciách,
- Prijímacie cesty nemusia byť predom nastavené aby naslúchali na konkrétnom faktore rozprestrenia,
- V prípade, že pri prenose paketu je voľných viacero prijímacích ciest na rovnakom kanále, je vybratá len jedna cesta,
- V prípade, že sú všetky prenosové cesty obsadené, bude ďalší prichádzajúci paket označený ako stratený [20].

4.2.2 Model linkovej vrstvy

Model linkovej (MAC) vrstvy v tomto module je zameraný na implementáciu LoRaWAN štandardu. Pre tento účel sú vytvorené niektoré triedy na správu hlavičiek, MAC príkazov, logických kanálov a výpočet striedy. Rovnako je tu implementovaný sieťový server ako aplikácia, ktorú možno nainštalovať v simulačnom prostredí na zariadenie a prepojiť s bránami cez `PointToPoint` pripojenie čím sa vytvorí backbone kanál.

Štruktúra paketu definovaná LoRaWAN štandardom je implementovaná pomocou dvoch podtried, ktoré rozširujú triedu `Header`: `LorawanMacHeader` a `LoraFrameHeader`. Trieda `LoraFrameHeader` môže obsahovať MAC príkazy z tried `MacCommand` a `LoraDeviceAddress`, ktoré sú použité na serializáciu, deserializáciu a interpretáciu MAC príkazov a LoRaWAN adresného systému.

MAC príkazy sú implementované rozšírením triedy `MacCommand`. Každý potomok triedy je použitý na definíciu skupiny premenných príkazu, metód na serializáciu a deserializáciu príkazov v `LoraFrameHeader` a na spätné volanie linkovej vrstvy na vykonávanie úkonov. Trieda `LoraDeviceAddress` je použitá pre reprezentáciu adresy LoRaWAN koncového zariadenia a pre serializáciu a deserializáciu.

Vzhľadom na to, že LoRaWAN pracuje v nelicencovanom pásme, musí sa riadiť reštrikciou striedy. Na sledovanie prebiehajúcich prenosov na linkovej vrstve je vytvorených niekoľko objektov. `LogicalLoraChannelHelper` je priradený na každú inštanciu `LorawanMac` a sleduje všetky dostupné logické kanály. Naviac na posilnenie limitácie striedy, tento objekt registruje všetky prenosy na všetkých kanáloch. Môže byť tiež dotázaný od `LorawanMac` inštancie na najbližší možný čas na vysielanie podľa platných regulácií. Ak prenos dĺžky t_{air} vykonaný zariadením na kanále, kde je definovaná strieda dc, musí zariadenie následne prestať vysielať na čas:

$$t_{\text{off}} = \frac{t_{\text{air}}}{dc} - t_{\text{air}} \qquad [s]. \tag{4.1}$$

Ak sú dva kanály pod rovnakou reštrikciou, prvý kanál bude blokovať aj druhý kanál.

K bránam je v simulačnom prostredí pripojené ďalšie zariadenie s aplikáciou `NetworkServer`. Brány smerujú prichádzajúce LoRa pakety na sieťový server a čakajú od sieťového servera pakety, ktoré budú smerovať na koncové zariadenia. Pre udržanie prehľadu o všetkých zariadeniach v sieti používa sieťový server dva zoznamy objektov: `DeviceStatus` a `GatewayStatus`, ktoré reprezentujú aktuálny stav každého koncového zariadenia a brány v sieti. Tieto objekty slúžia na udržanie prehľadu o downlinkových správach, ktoré sa posielajú na koncové zariadenia triedy A počas ich prjímacích okien. Tiež udržiavajú ukazovatele na inštancie linkovej vrstvy každej brány. Vykonáva sa to z dôvodu vykonávania dotazov v súvislosti s limitáciou striedy, tak aby brány, ktoré môžu vysielať mali správy pripravené na odoslanie. Sieťový server posiela iba downlinkové správy, ktoré požadujú potvrdenie, ignorujúc obsah paketu a obsiahnutých MAC príkazov. Prenos je vykonaný primárne cez prvé prijímacie okno a druhé okno je použité len v prípade, keď dostupné prostriedky nedovolujú využitie prvého okna [20].

4.2.3 Využitie

Model podporuje typické paradigmy NS-3, ako použitie pomocníkov (helpers) na konfiguráciu komplexnejších sietí.

Modul obsahuje pomocníkov na konfiguráciu fyzickej a linkovej vrstvy s väľkým množstvom zariadení. Tieto vrstvy sú rozdelené do tried: `LorawanMacHelper` a `LoraPhyHelper`, ku ktorým je možno pristúpiť objektom `LoraHelper` pre kompletnú konfiguráciu LoRa koncových zariadní a brán. Vzhľadom na to, že pomocníci majú všeobecnú podstatu, je nutné definovať druh zariadenia pomocou metódy `SetDeviceType` pred tým ako je zavolaná funkcia `Install`. `LorawanMacHelper` tiež obsahuje metódu pre automatické nastavenie faktoru rozprestrenia (SF) použitého pre zariadenia v sieti na základe stavu kanálu a rozloženia jednotlivých koncových zariadení a brán. Táto procedúra je statická metóda `SetSpreadingFactorsUp`, a funguje na základe skúšania minimalizovania doby prenosu paketu vzduchom. Takýmto spôsobom je nastavený najmenší možný faktor rozprestrenia tak aby bol prenos možný aspoň jednou bránou. Tento spôsob je heuristický a negarantuje optimálne nastavenie faktoru rozprestrenia v závislosti od aplikácie.

Pre simuláciu je možné nastaviť atribúty `Interval` a `PacketSize` vo funkcii `PeriodicSender`, ktoré určujú interval medzi zasielaním paketov aplikácie a veľkosť paketov generovaných aplikáciou.

Na sledovanie udalostí počas simulácie sa používajú rôzne sledovače na fyzickej vrstve, ktoré závisia hlavne od doby života paketu:

- V `LoraPhy` (pre `EndDeviceLoraPhy` aj `GatewayLoraPhy`):
  - `StartSending`, spustený keď fyzická vrstva začne s prenosom paketu,

  - `PhyRxBegin`, spustený keď fyzická vrstva začne s príjmom paketu,
  - `PhyRxEnd`, spustený keď je paket prijatý fyzickou vrstvou,
  - `ReceivedPacket`, spustený keď je paket úspešne prijatý,
  - `LostPacketBecauseInterference`, spustený keď sa paket stratí v dôsledku rušenia iným prenosom,
  - `LostPacketBecauseUnderSensitivity`, spustený keď fyzická vrstva nedokáže prijať paket v dôsledku nízkeho prijímacieho výkonu,
- V `EndDeviceLoraPhy`:
  - `LoraPacketBecauseWrongFrequency`, spustený v prípade, že prichádzajúci paket je vysielaný na inej frekvencii ako naslúcha fyzická vrstva prijímača,
  - `LoraPacketBecauseWrongSpreadingFactor`, spustený v prípade, že prichádzajúci paket je vysialný s iným faktorom rozprestrenia ako naslúcha fyzická vrstva prijímača,
  - `EndDeviceState`, použitý na sledovanie stavu fyzickej vrstvy zariadenia,
- V `GatewayLoraPhy`:
  - `LostPacketBecauseNoMoreReceivers`, spustený keď je paket stratený v dôsledku toho, že žiadna prenosová cesta nie je voľná,
  - `OccupiedReceptionPaths`, použitý na sledovanie počtu obsadených prenosových ciest z 8 dostupných na bráne,
- V `LorawanMac` (pre `EndDeviceLorawanMac` aj `GatewayLorawanMac`):
  - `CannotSendBecauseDutyCycle`, použitý na sledovanie prevádzky a riadenie prevádzky na základe striedy,
- V `EndDeviceLorawanMac`:
  - `DataRate`, použitý na sledovanie rýchlosti prenosu dát na zariadení,
  - `LastKnownLinkMargin`, sleduje koniec uplinkovej komunikácie na zariadení (táto informácia sa získava cez `LinkCheck` MAC príkaz),
  - `LastKnownGatewayCount`, sleduje počet brán v dosahu zariadenia (táto informácia sa získava cez `LinkCheck` MAC príkaz),
  - `AggregatedDutyCycle`, sleduje aktuálne limitácie agregovanej striedy,
- `PacketSent` v `LoraChannel`, spustený keď je paket poslaný kanálom [20].

4.2.4 Možnosti pre rozšírenie modulu

Napriek tomu, že modul je pomerne rozsiahli a implementuje väčšinu funkcií siete LoRaWAN, existuje niekoľko možných funkcií, ktoré by bolo možné doimplementovať.

Trieda `LoraChannel` môže byť prepojená len s LoRa fyzickou vrstvou, model nedokáže zohľadniť rušenie ostatnými technológiami. Úpravou `SpectrumChannel`

triedy by bolo možné znížiť medziprotokolové rušenie LoRa signálu až o polovicu.

Rušenie medzi čiastočne prekrývajúcimi sa kanálmi nie je opatrené. Model ošetrujúci rušenie medzi signálmi, ktoré používajú rôznu šírku pásma nie je implementovaný.

Súčastná implementácia sieťového serveru poskytuje iba základnú štruktúru pre ovládanie koncových zariadení a brán v sieti. Chýbajú možné komplexnejšie funkcie ako algoritmus pre rôznu adaptívnu rýchlosť prenosu dát (ADR), odpovedanie na MAC príkazy koncovým zariadeniam a podpora pripájacej procedúry. Inou limitáciou sieťového serveru je neprítomnosť protokolu pre priamu komunikáciu s bránami, a teda nemožno informovať bránu v reálnom čase o downlinkových správach na poslanie koncovým zariadeniam. Inak povedané, prostriedky brány nie je možné vyhradiť predom, preto downlinkové správy majú vyššiu prioritu ako uplinkové správy prijímané bránou od koncových zariadení.

Modul podporuje iba koncové zariadenia triedy A. Koncové zariadenia triedy B a C nie sú doposiaľ implementované.

Parametre siete LoRaWAN ako predvolená zostava kanálov a interpretácia MAC príkazov závisia od regiónu nasadenia siete. `LorawanMacHelper` obsahuje metódy pre špecifikáciu regiónu a modul predisponuje rôznymi konfiguráciami siete v náväznosti na región. Napriek tomu je momentálne dostupný iba EU región s frekvenčným pásmom 868 MHz.

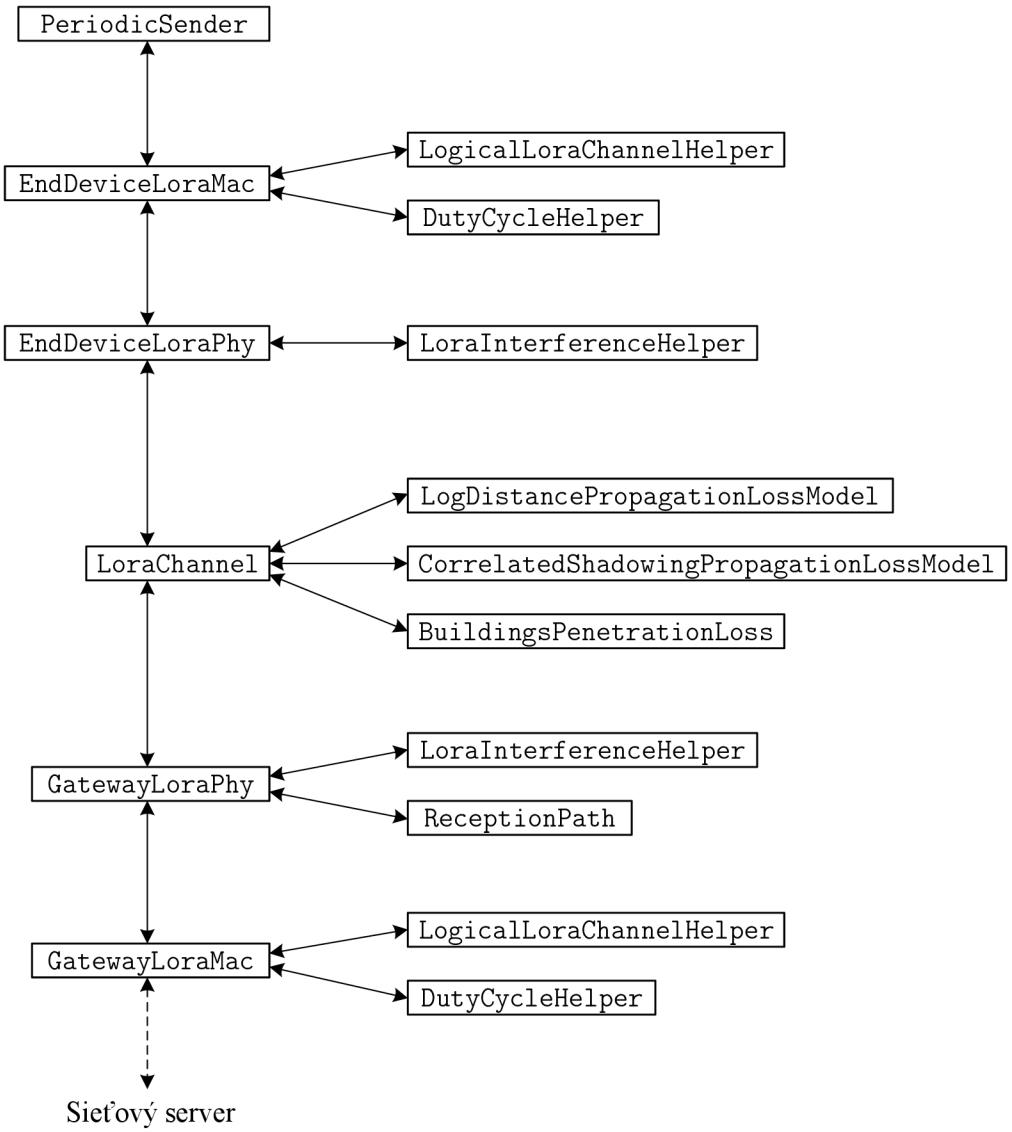
Niektoré ďalšie detaily, ktoré nie sú kľúčové pre výkon siete, ktoré nie sú implementované:

- Počítadlá rámcov na koncových zariadeniach a sieťovom serveri,
- Nastavenie ADR príznakov,
- Spravovanie pripojovacej procedúry na koncových zariadeniach a sieťovom serveri [20].

5 Simulácia siete LoRaWAN

V rámci praktickej časti tejto práce je vykonaná analýza niekoľkých simulačných scenárov siete LoRaWAN v rámci simulačného prostredia NS-3.

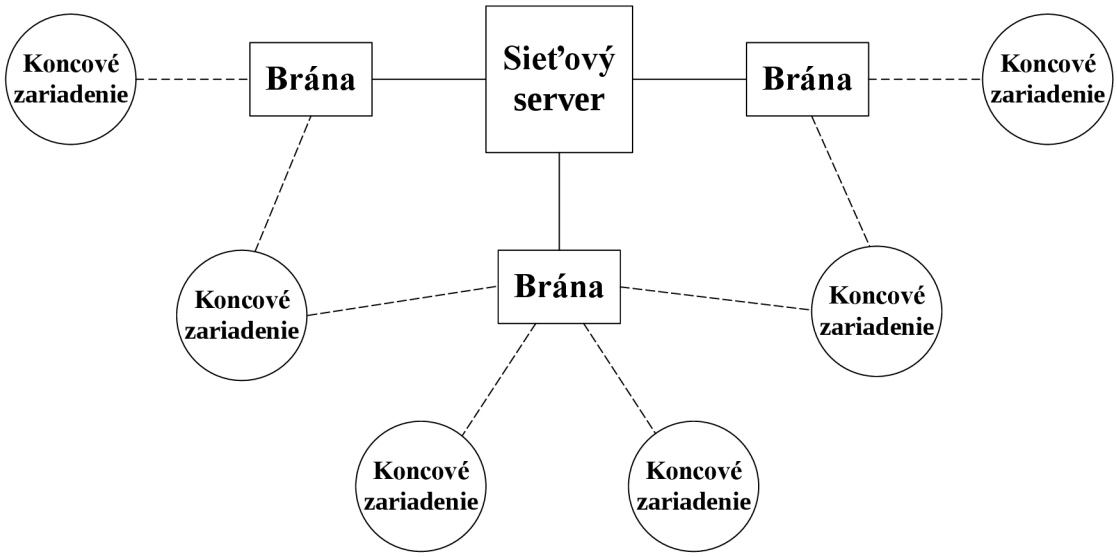
Pre korektnú simuláciu reálnej siete LoRaWAN sú použité sady tried spomenuté v predchádajúcej kapitole. Implementácia tejto sady tried do protokolového zásobníka je zobrazená na obr. 5.1.



Obr. 5.1: Sada tried reprezentujúca zásobník protokolu LoRaWAN [21].

Podobne, ako je tomu v reálnom nasadení siete LoRaWAN, aj v prípade simulácie je pre sieť využívaná hviezdicová topológia, viď. obr. 5.2. Koncové zariadenia komunikujú so sieťovým serverom cez rádiové brány, pričom vysielané pakety z koncového

zariradenia môže zachytiť hneď niekoľko brán. Koncové zariadenie teda nie je fixované na jednu konkrétnu bránu. Brána ďalej preposiela prijaté správy po backbone sieti na sieťový server, ktorý správy analyzuje. Duplikáty v prípade prijatia jednej správy viacerými bránami napomáhajú pri výbere jednej najvhodnejšej brány pri posielaní downlinkových správ zo serveru na koncové zariadenie. Rovnako tiež napomáhajú pri určovaní polohy koncového zariadenia v prípade aplikácií, ktoré túto informáciu využívajú.



Obr. 5.2: Hviezdicová topológia siete LoRaWAN [21].

5.1 Výsledky simulácie

Súčasťou použitého LoRaWAN modulu je niekoľko ukážkových príkladov. Pre potreby praktickej časti tejto práce bol vybratý príklad `complete-network-example`. V module je niekoľko nastaviteľných parametrov siete:

- **nDevices** - počet koncových zariadení,
- **nGateways** - počet brán,
- **radius** - polomer komunikačnej oblasti,
- **simulationTime** - dĺžka simulácie,
- **appPeriodSeconds** - perióda zasielania správ z koncových zariadení.

Zdrojový kód je rozdelený do niekoľkých častí:

- Základné nastavenie,
- Nastavenie prenosového kanálu,
- Vytvorenie pomocníkov,
- Vytvorenie koncových zariadení,

- Vytvorenie brán,
- Simulácia budov,
- Nastavenie faktoru rozprestrenia,
- Inštalácia aplikácií na koncové zariadenia,
- Vytvorenie sieťového servera,
- Simulácia,
- Výpis výsledkov simulácie.

Praktická časť práce sa zameriava na dva scenáre simulácie v NS-3. Prvým scenárom je vplyv počtu koncových zariadení v sieti na úspešnosť prenosu paketov a druhý scenár sa zameriava na vplyv vzdialenosti koncového zariadenia od brány na úspešnosť prenosu peketov. Výsledky oboch scenárov sú prehľadne spracované do tabuliek, z ktorých sú následne vytvorené grafy.

Pri prvotnom sputení simulácie bez predchádzajúcich úprav môžme vyčítať informácie uvedené v tab. 5.1.

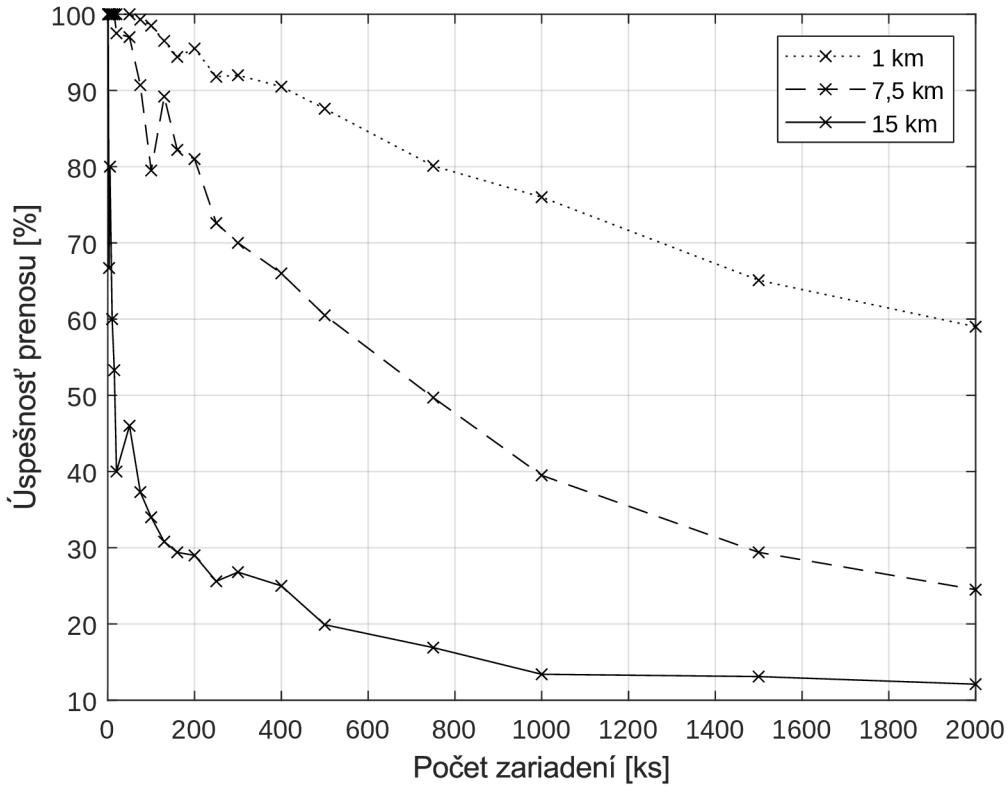
Tab. 5.1: Výstupy prvotnej simulácie.

Parameter	**Hodnota**
Počet koncových zariadení	2
Počet brán	1
Počet sieťových serverov	1
Polomer komunikačnej oblasti	100 m
Čas simulácie	300 s
Perióda zasielania správ	100 s
Veľkosť užitočných dát	23 B
Faktor rozprestrenia	7
Šírka pásma	125 kHz
Použitá frekvencia	868,3 MHz 868,5 MHz
Prenosová rýchlosť	5468 b/s
Veľkosť paketu	32 B
Doba prenosu správy	71,936 ms
Vysielací výkon	14 dBm
Prijímací výkon	KZ1: 59,50 dBm KZ2: 56,44 dBm
Vzdialenosť od brány	KZ1: 56,4 m KZ2: 46,6 m
Kódovací pomer	4/5
Počet správ odoslaných/prijatých	6/6

5.1.1 Vplyv počtu koncových zariadení v sieti

V tomto scenári je simulovaný vplyv počtu koncových zariadení na prevádzku siete a dopad na úspešnosť prenosu správ. Každé koncové zariadenie počas simulácie odošle 2 správy. Scenár obsahuje tri rôzne polomery komunikačnej oblasti: 1 km, 7,5 km a 15 km. V sieti sa okrem koncových zariadení náchádza jedna brána a jeden sieťový server. Výsledky simulácie sú zobrazené v tab. 5.1.1.

Na obr. 5.3 sú graficky znázornené výsledky z tab. 5.1.1. V grafe sú zobrazené tri priebehy v závislosti od polomeru komunikačnej oblasti. Z grafu je zrejmé, že úspešnosť prenosu klesá so zvyšujúcim sa počtom koncových zariadení v sieti, rovnako ako aj so zvyšujúcim sa polomerom komunikačnej oblasti.

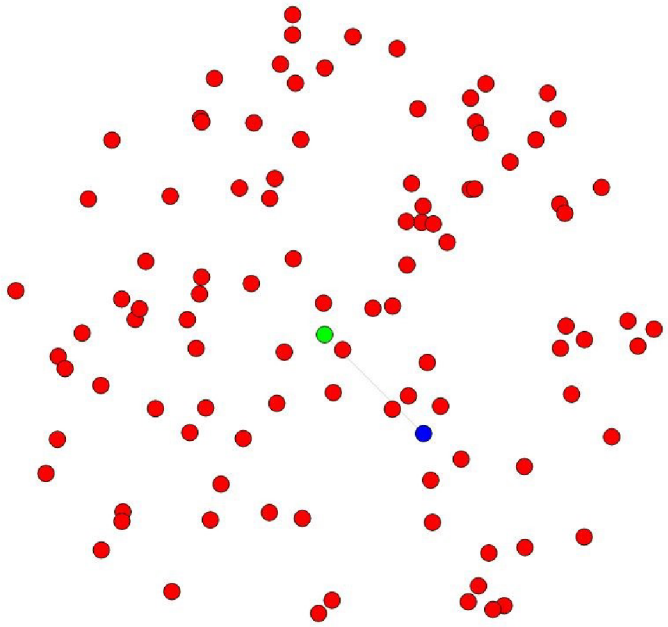


Obr. 5.3: Závislosť úspešnosti prenosu od počtu koncových zariadení.

Tab. 5.2: Vplyv počtu koncových zariadení na úspešnosť prenosu.

Počet		**Prijaté pakety pri rádiuse 1 km**		**Prijaté pakety pri rádiuse 7,5 km**		**Prijaté pakety pri rádiuse 15 km**	
Koncových zariadení [ks]	**Odoslaných paketov [ks]**	[ks]	[%]	[ks]	[%]	[ks]	[%]
1	2	2	100,0	2	100,0	2	100,0
3	6	6	100,0	6	100,0	4	66,7
5	10	10	100,0	10	100,0	8	80,0
10	20	20	100,0	20	100,0	12	60,0
15	30	30	100,0	30	100,0	16	53,3
20	40	40	100,0	39	97,5	16	40,0
50	100	100	100,0	97	97,0	46	46,0
75	150	149	99,3	136	90,7	56	37,3
100	200	197	98,5	159	79,5	68	34,0
130	260	251	96,5	232	89,2	80	30,8
160	320	302	94,4	263	82,2	94	29,4
200	400	382	95,5	324	81,0	116	29,0
250	500	459	91,8	363	72,6	128	25,6
300	600	552	92,0	420	70,0	161	26,8
400	800	724	90,5	528	66,0	200	25,0
500	1000	876	87,6	605	60,5	199	19,9
750	1500	1202	80,1	745	49,7	253	16,9
1000	2000	1520	76,0	790	39,5	267	13,4
1500	3000	1952	65,1	882	29,4	393	13,1
2000	4000	2358	59,0	981	24,5	484	12,1

Z vykonaných simulácií bol vybratý jeden príklad zobrazený na obr. 5.4. Jedná sa o 100 koncových zariadení rozložených v oblasti s polomerom 1 km. Koncové zariadenia sú označené červenou, brána zelenou a sieťový server modrou farbou. Brána je so serverom spojená pomocou P2P (point-to-point) protokolu.



Obr. 5.4: Rozmiestnenie 100 koncových zariadení v komunikačnej oblasti s polomerom 1 km.

5.1.2 Vplyv vzdialenosti koncového zariadenia od brány

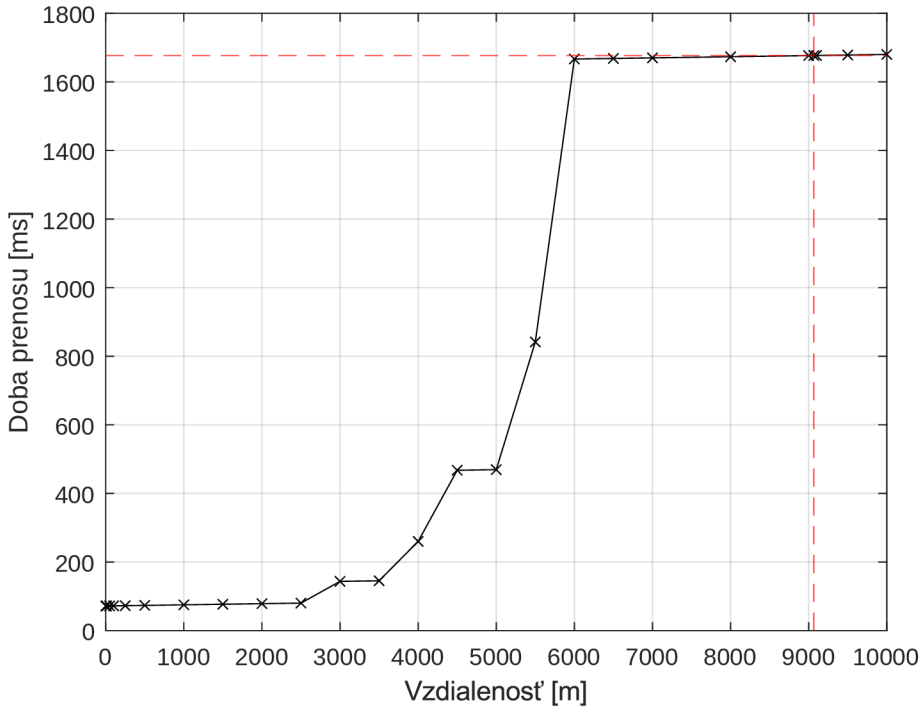
Tento scenár sa venuje vplyvu vzdialenosti koncového zariadenia od brány na úspešnosť prenosu správ. V sieti sa nachádza jedno koncové zariadenie, jedna brána a jeden sieťový server. Vysielací výkon je nastavený na 14 dBm a šírka pásma je 125 kHz. Doba prenosu odpovedá teoretickému výpočtu podľa vzorca (3.7). Faktor rozprestrenia sa automaticky zvyšuje v závislosti od zvyšujúcej sa vzdialenosti koncového zariadenia od brány. Vzhľadom na konštantnú šírku pásma sa doba prenosu zvýši vždy vtedy keď sa zvýši aj faktor rozprestrenia. K teoretickej hodnote doby prenosu je nutné pripočítať aj oneskorenie spôsobené vzdialenosťou. Výsledky simulácie sú zobrazené v tab. 5.1.2. Posledné hodnoty, ktoré sú označené červenou farbou, sú neúspešnými prenosmi kde vysoká vzdialenosť spôsobila, že výkon prenášaného paketu klesol pod hraničnú hodnotu a brána ho nedokázala prijať. Hraničná hodnota prijímacieho výkonu bola simuláciou stanovená na -142,5 dBm. Z tabulky je tiež zrejmé, že maximálny komunikačný dosah je 9066 m.

Tab. 5.3: Vplyv vzdialenosti koncového zariadenia od brány na vlastnosti prenosu.

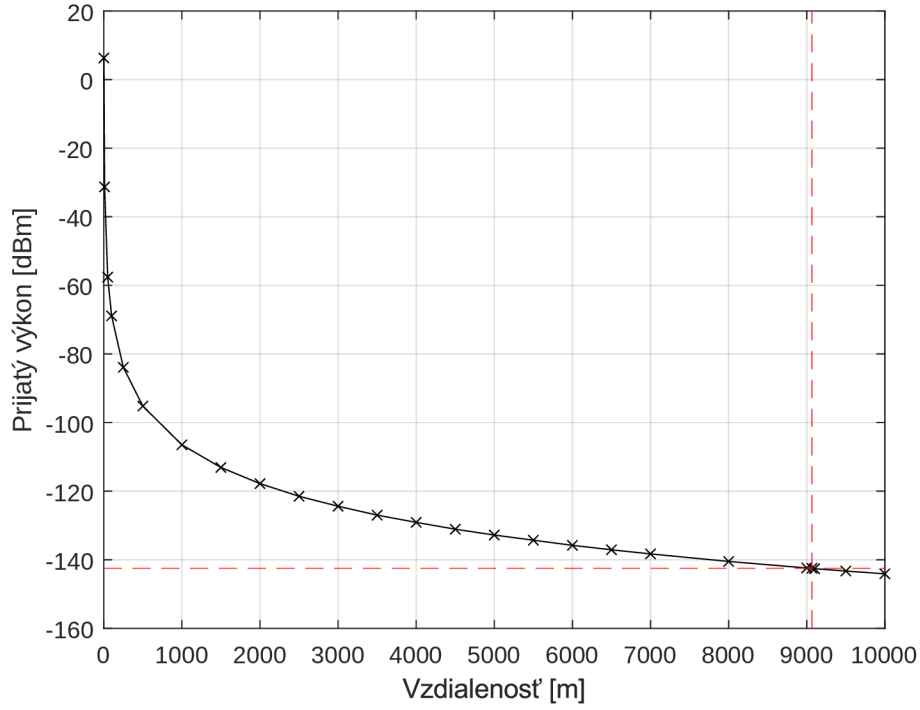
Vzdialenosť od brány [m]	**Faktor rozprestrenia**	**Doba prenosu [ms]**	**Oneskorenie [ms]**	**Celková doba prenosu [ms]**	**Prijatý výkon [dBm]**
1	7	71,936	0,003	71,939	6,3
10	7	71,936	0,033	71,969	-31,3
50	7	71,936	0,166	72,102	-57,6
100	7	71,936	0,333	72,269	-68,9
250	7	71,936	0,833	72,769	-83,9
500	7	71,936	1,667	73,603	-95,2
1000	7	71,936	3,335	75,271	-106,5
1500	7	71,936	5,003	76,939	-113,1
2000	7	71,936	6,671	78,607	-117,8
2500	7	71,936	8,339	80,275	-121,5
3000	8	133,632	10,006	143,638	-124,4
3500	8	133,632	11,674	145,306	-127,0
4000	9	246,784	13,342	260,126	-129,1
4500	10	452,608	15,010	467,618	-131,1
5000	10	452,608	16,678	469,286	-132,8
5500	11	823,296	18,346	841,642	-134,3
6000	12	1646,59	20,013	1666,603	-135,8
6500	12	1646,59	21,681	1668,271	-137,1
7000	12	1646,59	23,349	1669,939	-138,3
8000	12	1646,59	26,685	1673,275	-140,5
9000	12	1646,59	30,020	1676,610	-142,4
9066	12	1646,59	30,240	1676,830	-142,5
9100	12	1646,59	30,354	1676,944	-142,6
9500	12	1646,59	31,688	1678,278	-143,3
10000	12	1646,59	33,356	1679,946	-144,1

Na obr. 5.5 je graficky znázornená závislosť doby prenosu paketu od vzdialenosti od brány. Skokové zmeny sú spôsobené zmenou faktoru rozprestrenia, kedy sa mení aj maximálna prenosová rýchlosť, ktorá priamo ovplyvňuje dobu prenosu.

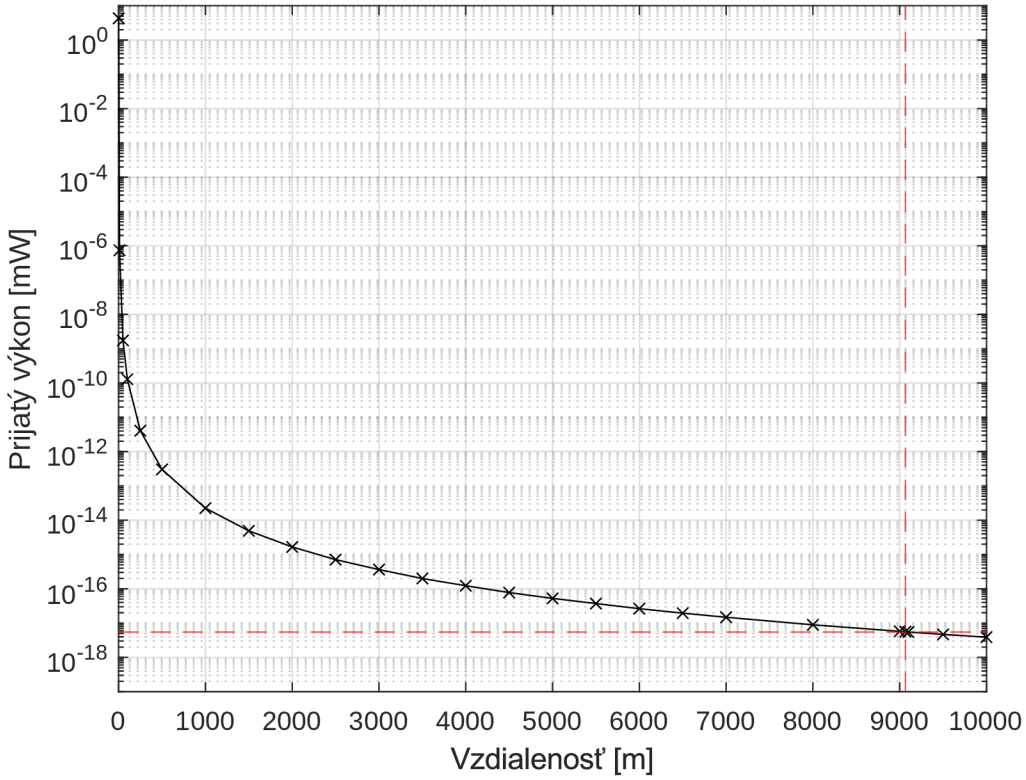
Na obr. 5.6 je znázornená závislosť prijímacieho výkonu na vzdialenosti koncového zariadenia od brány v jednotkách dBm. Obr. 5.7 obsahuje rovnakú závislosť v prepočítanej hodnote výkonu na mW.



Obr. 5.5: Závislosť doby prenosu na vzdialenosti koncového zariadenia od brány.



Obr. 5.6: Závislosť prijímacieho výkonu v dBm na vzdialenosti koncového zariadenia od brány.



Obr. 5.7: Závislosť prijímacieho výkonu v mW na vzdialenosti koncového zariadenia od brány.

6 Modifikácia LoRaWAN modulu

Poslednou súčasťou praktickej časti práce je pristúpenie k modifikácii použitého LoRaWAN modulu pre NS-3. Modifikácia bude vykonaná v troch častiach. Prvou časťou je rozšírenie komunikačných frekvencií. Ako už bolo spomenuté, v súčastnosti je dostupné iba sub-GHz pásmo pre EU región (868 MHz). Druhou a treťou časťou bude náčrt modifikácie pre obojsmernú komunikáciu a šifrovanie komunikácie. Tieto dve modifikácie budú spravené len v teoretickej hladine, z dôvodu vysokej komplexnosti použitého LoRaWAN modulu. V rámci prípravy na implementáciu obojsmernej komunikácie budú pripravené niektoré funkcie, ktoré bude možné pri prípadnom doimplementovaní použiť.

6.1 Modifikácia frekvenčných pásiem

Použitý LoRaWAN modul v aktuálnej verzii podporuje simuláciu prenosu iba v regióne EU v sub-GHz pásme (868 MHz). Modifikácia je zameraná na implementáciu prenosovej frekvencie pre región US a následne bude implementovaná aj frekvencia 2,4 GHz pre EU región. Modifikácia bude primárne riešená v `LorawanMacHelper` triede, kde je v aktuálnej verzii nadefinované frekvenčné pásmo pre EU región.

6.1.1 Regulácie pre frekvenčné pásma

Región US má naproti EU regiónu dohodnuté podstatne iné regulácie a frekvenčné rozsahy, ktoré sa delia pre uplinkovú a downlinkovú komunikáciu. Z hľadiska prenosovej frekvencie má EU nadefinovaných 16 kanálov, z ktorých najpoužívanejšie sú 3 na frekvenciách 868,1 MHz, 868,3 MHz a 868,5 MHz. Tieto 3 kanály sa nazývajú tiež "základné kanály"pre EU región. Každý z nich používa šírku pásma 125 kHz a rýchlosť dátového toku 0–5. V závislosti od použitej rýchlosti dátového toku je nadefinovaná aj maximálna veľkosť payloadu, viď. tab. 6.1.1

Pre US región sú nadefinované 3 rozdielne frekvenčné pásma, s rôznou šírkou pásma, použitou dátovou rýchlosťou a faktorom rozprestrenia. Tieto 3 pásma sa delia aj v závislosti od toho, či sa jedná o uplinkovú, alebo downlinkovú komunikáciu. Každé pásmo je rozdelené do niekoľkých kanálov, viď tab. 6.1.1. Špecifikácie podľa dátovej rýchlosti je možné vidieť v tab. 6.1.1.

Ďalší rozdiel medzi EU a US regiónmi je v maximálnom vysielacom výkone. Zatiaľ čo v EU regióne je maximálny vysielací výkon 16 dBm (40 mW), tak v US regióne je možné použiť vysielací výkon až 30 dBm (1 W). Pre väčšinu zariadení je však dostačujúci vysielací výkon 20 dBm (100 mW).

Tab. 6.1: Rýchlosť dátového toku pre EU región [22].

Data rate	**SF**	**Šírka pásma [kHz]**	**Prenosová rýchlosť [bit/s]**	**Maximálna veľkosť payloadu [B]**
0	12	125	250	51
1	11	125	440	51
2	10	125	980	51
3	9	125	1760	115
4	8	125	3125	242
5	7	125	5470	242
6	7	250	11000	242

Tab. 6.2: Frekvenčné pásma pre US región [22].

Smer	**Počet kanálov**	**Frekvenčné pásmo**	**Šírka pásma [kHz]**	**Data rate**
Uplink	64	902,3 – 914,9 MHz delené po 200 kHz	125	0 – 3
Uplink	8	903,0 – 914,2 MHz delené po 1,6 MHz	500	4
Downlink	8	923,3 – 927,5 MHz delené po 600 kHz	500	8 – 13

Tab. 6.3: Rýchlosť dátového toku pre US región [22].

Data rate	**SF**	**Šírka pásma [kHz]**	**Prenosová rýchlosť [bit/s]**	**Maximálna veľkosť payloadu [B]**
0	10	125	980	11
1	9	125	1760	53
2	8	125	3125	125
3	7	125	5470	242
4	8	500	12500	242
8	12	500	980	53
9	11	500	1760	129
10	10	500	3900	242
11	9	500	7000	242
12	8	500	12500	242
13	7	500	21900	242

V neposlednom rade je rozdiel aj v striede. V EU regióne je strieda regulovaná podľa tab. 3.2.2. V US regióne nie je definovaná strieda, ale maximálne množstvo času pre jeden prenos (dwell time) 400 ms [22].

Pre modifikáciu prenosovej frekvencie bolo okrem frekvenčného pásma pre US región vybrané aj 2,4 GHz pásmo pre EU región. V prípade tohto pásma je tiež nutné zmeniť niekoľko parametrov. Na prenos sa používajú 3 rôzne frekvencie - 2403 GHz, 2425 GHz a 2479 GHz. Ostatné parametre sú vypísané v tab. 6.1.1.

Tab. 6.4: Rýchlosť dátového toku pre EU 2,4 GHz pásmo [23].

Data rate	**SF**	**Šírka pásma [kHz]**	**Prenosová rýchlosť [bit/s]**	**Maximálna veľkosť payloadu [B]**
0	12	812	1200	59
1	11	812	2100	123
2	10	812	3900	228
3	9	812	7100	228
4	8	812	12700	228
5	7	812	22200	228

6.1.2 Implementácia frekvenčných pásiem v LoRaWAN module

Implementácia frekvenčného pásma pre US a 2,4 GHz pásma pre EU región bola vykonaná v triede `LorawanMacHelper`. V tejto triede bolo v pôvodnom stave zadefinované iba sub-GHz pásmo pre EU región. Definícia sa vykonáva pomocou troch funkcií, jedna slúži pre nastavenie koncového zariadenia, druhá na nastavenie brány a tretia pre všeobecné nastavenie komunikačného kanálu. Prvé dve funkcie vo svojom priebehu postupne pristupujú k tretej funkcii. V praxi by sa dalo povedať, že ako koncové zariadenie, tak aj brána si najprv nastavia zdieľané parametre a následne si nastavia svoje špecifické parametre.

Ukážku implementácie všeobecného nastavenia komunikačného kanálu pre novoimplementované pásmo pre US región je možné vidieť na výpise A.1 v prílohe. Následne si potrebné parametre nastaví osobitne koncové zariadenie aj brána, viď výpis A.2 v prílohe.

Ďalej je nutné implementovať možnosť výberu, ktoré frekvenčné pásmo bude použité. Ukážka výberu frekvenčného pásma použitého koncovým zariadením je vo výpise 6.1. Obdobne je nastavené frekvenčné pásmo pre bránu kedy stačí vymeniť parameter *edMac* za parameter *gwMac*.

Ako posledné je nutné zadefinovať v triede `complete-network-example` v hlavnej funkcii **Main**, ktoré frekvenčné pásmo chceme použiť, viď výpis 6.2

Výpis 6.1: Výber frekvenčného pásma.

```
switch (m_region){
  case LorawanMacHelper::EU: {
    ConfigureForEuRegion (edMac);
    break;}
  case LorawanMacHelper::EUGHz: {
    ConfigureForEuGhzRegion (edMac);
    break;}
  case LorawanMacHelper::US: {
    ConfigureForUsRegion (edMac);
    break;}
  default: {
    NS_LOG_ERROR ("This region isn't supported yet!");
    break;}
}
```

Výpis 6.2: Definícia frekvenčného pásma.

```
LorawanMacHelper macHelper = LorawanMacHelper ();
macHelper.SetRegion(LorawanMacHelper::US);
```

6.1.3 Simulácia modifikovaných frekvenčných pásiem

Po implementácii ďalších frekvenčných pásiem boli vykonané dva druhy simulačných scenárov pre porovnanie komunikácie v stávajúcom sub-GHz frekvenčnom pásme pre EU región a novo-implementovanými frekvenčnými pásmami pre US región a 2,4 GHz frekvenčného pásma pre EU región.

Prvým simulačným scenárom je porovnanie doby prenosu v jednotlivých frekvenčných pásmach v závislosti od vzdialenosti koncového zariadenia od brány. V sieti sa nachádzalo jedno koncové zariadenie, jedna brána a jeden sieťový server. Koncové zariadenie posielalo jednu správu. Výsledky simulácie sú zapísané v tab. 6.1.3.

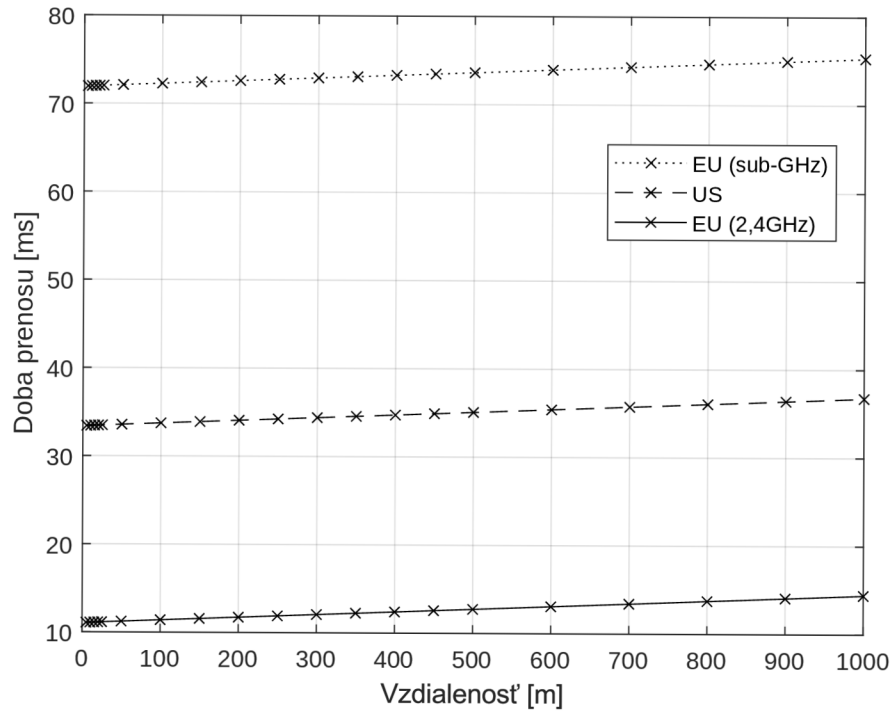
Na obr. 6.1 je graficky znázornený výsledok simulácie. Je zrejmé, že vyššia prenosová frekvencia a šírka pásma novo-implementovaných frekvenčných pásiem kladne vplýva na dobu prenosu správy z koncového zariadenia na bránu. Pre stávajúci región EU s použitou sub-GHz frekvenciou bol použitý faktor rozprestrenia 7 a šírka pásma bola 125 kHz. Toto nastavenie odpovedá použitej rýchlosti dátového toku (Data Rate) 5. Naproti tomu, frekvenčné pásmo pre US región použilo faktor rozprestrenia 8 so šírkou pásma 500 kHz, čo odpovedá použitiu rýchlosti dátového toku 4. Posledné frekvenčné pásmo 2,4 GHz pre EU región používalo faktor rozprestrenia 7 so šírkou pásma 812 kHz, čo odpovedá použitiu rýchlosti dátového toku 5.

Tab. 6.5: Rozdiel v dobe prenosu v závislosti od použitého frekvenčného pásma.

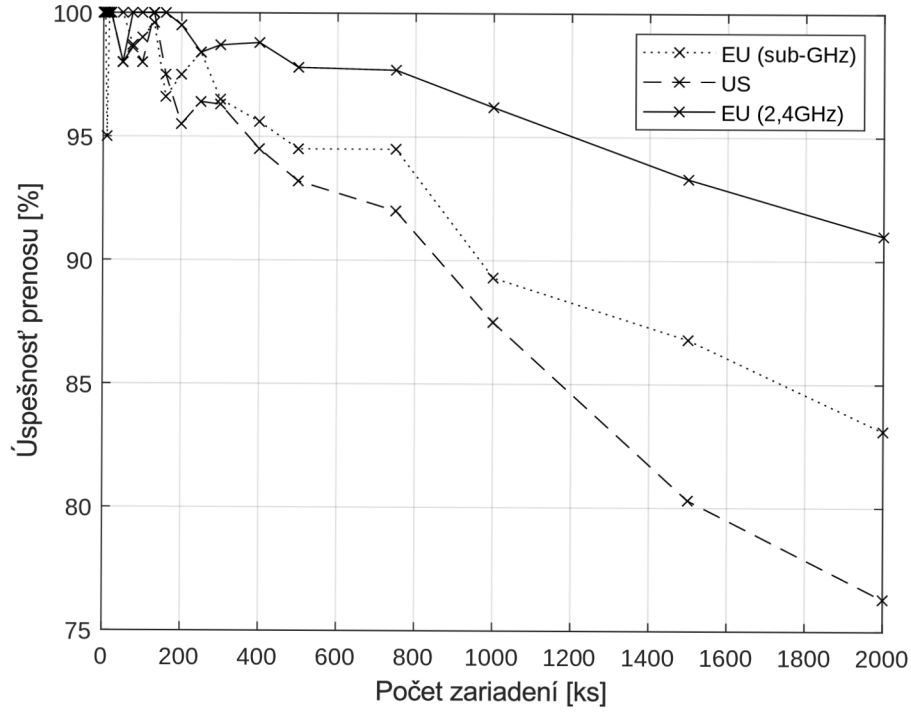
Región:	**EU sub-GHz**	**US**	**EU 2,4GHz**
Vzdialenosť [m]	**Doba prenosu [ms]**		
5	71,952	33,424	11,090
10	71,969	33,441	11,107
15	71,986	33,458	11,124
20	72,002	33,458	11,140
25	72,019	33,474	11,157
50	72,102	33,574	11,240
100	72,269	33,741	11,407
150	72,436	33,908	11,574
200	72,603	34,075	11,741
250	72,769	34,241	11,907
300	72,936	34,408	12,074
350	73,103	34,575	12,241
400	73,270	34,742	12,408
450	73,437	34,909	12,575
500	73,603	35,075	12,741
600	73,937	35,409	13,075
700	74,270	35,742	13,408
800	74,604	36,076	13,742
900	74,938	36,410	14,076
1000	75,271	36,743	14,409

Druhým simulačným scenárom je porovnanie vplyvu navyšujúceho sa počtu koncových zariadení na úspešnosť prenosu v jednotlivých frekvenčných pásmach. V sieti sa okrem koncových zariadení nachádzala jedna brána a jeden sieťový server. Scenár používal polomer komunikačnej oblasti 1 km. Každé koncové zariadenie odoslalo jednu správu. Výsledky simulácie sú uvedené v tab. 6.1.3.

Na obr. 6.2 je graficky znázornený výsledok simulácie. Z priebehu je zrejmé, že najlepšie vlastnosti má 2,4 GHz frekvenčné pásmo pre EU región vďaka vyššej prenosovej frekvencii a väčšej šírke pásma. Naopak najhoršie vlastnosti má frekvenčné pásmo pre US región, čo je spôsobené použitím nižšej rýchlosti dátového toku ako ostatné dve frekvenčné pásma.



Obr. 6.1: Závislosť doby prenosu od použitého frekvenčného pásma.



Obr. 6.2: Závislosť úspešnosti prenosu od použitého frekvenčného pásma.

Tab. 6.6: Rozdiel úspešnosti prenosu v závislosti od použitého frekvenčného pásma.

Počet		**Prijaté správy v pásme EU (sub-GHz)**		**Prijaté správy v pásme US**		**Prijaté správy v pásme EU (2,4GHz)**	
Koncových zariadení [ks]	**Odoslaných správ [ks]**	**[ks]**	**[%]**	**[ks]**	**[%]**	**[ks]**	**[%]**
1	2	2	100,0	2	100,0	2	100,0
3	6	6	100,0	6	100,0	6	100,0
5	10	10	100,0	10	100,0	10	100,0
10	20	19	95,0	20	100,0	20	100,0
15	30	30	100,0	30	100,0	30	100,0
20	40	40	100,0	40	100,0	40	100,0
50	100	100	100,0	98	98,0	98	98
75	150	148	98,7	148	98,7	150	100,0
100	200	198	99,0	196	98	200	100,0
130	260	259	99,6	260	100	260	100,0
160	320	309	96,6	312	97,5	320	100,0
200	400	390	97,5	382	95,5	398	99,5
250	500	492	98,4	482	96,4	492	98,4
300	600	579	96,5	578	96,3	592	98,7
400	800	765	95,6	756	94,5	790	98,8
500	1000	945	94,5	932	93,2	978	97,8
750	1500	1418	94,5	1380	92	1466	97,7
1000	2000	1785	89,3	1750	87,5	1924	96,2
1500	3000	2605	86,8	2410	80,3	2800	93,3
2000	4000	3325	83,1	3050	76,3	3640	91

6.2 Príprava obojsmernej komunikácie

LoRaWAN modul v aktuálnej verzii podporuje iba jednosmernú komunikáciu v smere z koncového zariadenia na bránu. V triede `LoraFrameHeader` je predpripravený parameter pre potvrdzovanie komunikácie `m_ack` 6.3. Vo východzom nastavení je tento parameter vypnutý (je mu priradená hodnota 0). Po zapnutí parametru priradením hodnoty 1 však v komunikácii zmena nenastane, práve kvôli tomu, že obojsmerná komunikácia zatiaľ nie je implementovaná.

Výpis 6.3: Voliteľné parametre v triede `LoraFrameHeader`.

```
1  LoraFrameHeader::LoraFrameHeader () :
2    m_fPort (0),
3    m_address (LoraDeviceAddress (0,0)),
4    m_adr (0),
5    m_adrAckReq (0),
6    m_ack (0),
7    m_fPending (0),
8    m_fOptsLen (0),
9    m_fCnt (0)
10 {}
```

V tejto sekcii práce bude popísané akým spôsobom je nutné použitý modul upraviť aby bolo možné implementovať obojsmernú komunikáciu. Z hľadiska vysokej komplexnosti použitého modulu nebolo možné v rámci tejto práce samotnú implementáciu uskutočniť a otestovať.

Na začiatok je nutné pripomenúť si, akým spôsobom funguje obojsmerná komunikácia LoRaWAN technológie. Downlinková komunikácia (z brány na koncové zariadenie) funguje na základe použitej triedy koncového zariadenia. Vzhľadom na to, že modul zatiaľ podporuje iba koncové zariadenie triedy A je downlinková komunikácia umožnená iba bezprostredne po uplinkovej komunikácii v dvoch časom definovaných oknách. Ako je možné vidieť vo výpise 6.4, prvé okno pre prijatie downlinkovej správy sa otvára 1 sekundu po odoslaní uplinkovej správy a druhé okno sa otvára 2 sekundy po prijatí uplinkovej správy. Tieto parametre sú nastavené v triede `classAEndDeviceLorawanMac`. Rovnako sú tam predpripravené funkcie pre prijatie správy, spracovanie neúspešného prijatia správy a otvorenie a zatvorenie prvého a druhého prijímacieho okna. Výpis týchto funkcií je zobrazený vo výpise 6.5.

Výpis 6.4: Otváranie okien pre downlinkovú komunikáciu.

```
1  ClassAEndDeviceLorawanMac::ClassAEndDeviceLorawanMac () :
2    m_receiveDelay1 (Seconds (1)),
3    m_receiveDelay2 (Seconds (2)),
```

Výpis 6.5: Funkcie v triede `classAEndDeviceLorawanMac`.

```
1 virtual void Receive (Ptr<Packet const> packet);
2 virtual void FailedReception (Ptr<Packet const> packet);
3 void OpenFirstReceiveWindow (void);
4 void OpenSecondReceiveWindow (void);
5 void CloseFirstReceiveWindow (void);
6 void CloseSecondReceiveWindow (void);
```

Frekvenčné pásmo pre US región bolo v rámci jeho implementácie pripravené aj pre obojsmernú komunikáciu. Vzhľadom na to, že toto frekvenčné pásmo využíva iné frekvencie a rýchlosti dátového toku pre uplinkovú a downlikovú komunikáciu, bolo nutné tieto parametre zadefinovať.

Vo funkcii pre nastavenie zdieľaných parametrov koncového zariadenia a brány je pripravené frekvenčné pásmo pre downlink. Následne si potrebné parametre nastaví osobitne koncové zariadenie aj brána. Koncové zariadenie potrebuje mať pripravené rýchlosti dátového toku a brána vyberá konkrétnu prenosovú frekvenciu z definovaného rozsahu. Výpis týchto parametrov v spomenutých funkciách je možné vidieť v prílohe A.3.

6.3 Príprava šifrovanej komunikácie

Po úspešnej implementácii obojsmernej komunikácie bude možné implementovať šifrovanie komunikácie. LoRaWAN koncové zariadenie šifruje prenášané dáta dvoma kľúčmi (AppSKey a NwkSKey). Na šifrovanie sa používa algoritmus AES-128. Vzhľadom na to, že AppSKey v praxi pozná iba koncové zariadenie a aplikačný server, tento kľúč implementovať, keďže použitý modul nedisponuje aplikačným serverom. Prítomný je len sieťový server, ktorý k správnemu prenášaniu dát a kontrole integrity správ potrebuje iba NwkSKey.

Modul v aktuálnej verzii nepodporuje ani aktivačné procedúry (OTAA a ABP). V praxi sa šifrovacie kľúče odvodia a distribuujú práve počas aktivačnej procedúry. Vzhľadom k tejto skutočnosti je potrebné aby si koncové zariadenia a sieťový server vymenili šifrovací kľúč. Keďže sa jedná o blokovú symetrickú šifru tak najvhodnejším riešením bude použitie Diffie-Hellmanovho protokolu. Potom ako si zariadenia vymenia šifrovací kľúč bude potrebné implementovať šifrovanie každej správy dohodnutým kľúčom. Vzhľadom na komplexnosť modulu, by bolo vhodné pre zachovanie čo najlepšej prehľadnosti, implementáciu šifrovania vytvoriť v novej osobitnej triede.

Záver

Diplomová práca je venovaná Low Power Wide Area Network (LPWAN) technológii LoRaWAN. Prvá kapitola je venovaná všeobecnému popisu Internet of Things (IoT), použitej technológii, štruktúra a použité druhy komunikácie Device-to-Device (D2D), Machine-to-Machine (M2M) a Massive Machine-Type Communication (mMTC).

Následne je popísaná technológia LPWAN so zameraním na štruktúru a požiadavky tejto technológie. LPWAN siete sú zamerané na vysoký komunikačný dosah s nízkou energetickou náročnosťou a vysokou životnosťou. V rámci kapitole o LPWAN sú spomenuté najpoužívanejšie technológie v praxi: LoRaWAN, Narrow Band-IoT (NB-IoT), LTE Cat-M1 a Sigfox.

Vzhľadom na zameranie práce je nasledujúca kapitola detailne zameraná na popis technológie LoRaWAN. Technológia pracuje na dvoch vrstvách. Na fyzickej vrstve funguje LoRa modulácia, ktorá je uzavretým štandardom spoločnosti Semtech. Na linkovej vrstve následne pracuje protokol LoRaWAN, ktorý je otvoreným štandardom spoločnosti LoRa-Alliance. LoRaWAN pracuje prevažne v sub-GHz Industrial, Scientific and Medical (ISM) frekvenčnom pásme (868 MHz pre EU), no v rámci niektorých aplikácií sa využíva aj frekvenčné pásmo 2,4 GHz. Na linkovej vrstve sú koncové zariadenia rozdelené do troch tried (A, B a C) v závislosti od využitia. Následne sú popísané dve dostupné metódy pripojenia koncového zariadenia do siete: aktivácia personalizáciou (ABP) a aktivácia vzduchom (OTAA). Po popise tried koncových zariadení a pripájacích procedúr je priblížená sieťová architektúra. Sieť LoRaWAN sa skladá z koncových zariadení, ktoré bezdrôtovo komunikujú s rádiovou bránou. Brána, resp. brány sú spojené pomocou transportnej siete so sieťovým serverom, ktorý riadi tok dát. Okrem sieťového servera sa v sieti nachádza aj pripájací server, ktorý obsluhuje pripájacie procedúry koncových zariadení a aplikačný server, ktorý obsluhuje konkrétnu aplikáciu. Serverov každého druhu sa môže v sieti nachádzať aj viac, vždy v závislosti od využitia v praxi. Na záver je popísaná bezpečnosť technológie založená na použití dvojice šifrovacích kľúčov pre sieť a pre aplikačné dáta. Na šifrovanie sa používa Advanced Encryption Standard (AES) algoritmus.

V rámci praktickej časti je sieť LoRaWAN implementovaná v simulačnom prostredí Network Simulator (NS-3) pomocou dostupného modulu od SIGNET Lab (signetlabdei). Na začiatku je popísané samotné simulačné prostredie NS-3, ktoré je následne obohatené vybraným LoRaWAN modulom. Modul bol vybraný porovnávaním dostupných modulov na základe komplexnosti, kedy bol dôraz kladený na maximálnu podobnosť s reálnym modelom siete LoRaWAN. Modul obsahuje modely oboch vrstiev technológie LoRaWAN využitím skupín tried, ktoré reprezentujú zá-

sobník protokolu. Napriek detailnému spracovaniu modulu sú na konci kapitoly vypísané možnosti pre rozšírenie modulu, ktoré zatiaľ nie sú implementované.

Následne sú vykonané simulácie dvoch scenárov komunikácie. Prvým je vpliv počtu koncových zariadení v sieti na úspešnosť prenosu v rôznych polomeroch komunikačnej oblasti. Zo simulácie bolo vyvodené, že navyšujúci sa počet koncových zariadení negatívne vplíva na úspešnosť prenosu, rovnako ako zvyšujúci sa polomer komunikačnej oblasti. V prípade komunikačnej oblasti s polomerom 1 km klesla úspešnosť prenosu pod 90% pri počte 500 koncových zariadeniach. V komunikačnej oblasti s polomerom 7,5 km klesla úspešnosť pod 90% pri 100 zariadeniach a v prípade oblasti s polomerom 15 km bola úspešnosť prenosu menej ako 50% už pri 20 koncových zariadeniach v sieti. Druhým scenárom je vpliv vzdialenosti koncového zariadenia od brány na úspešnosť prenosu. Simuláciou bolo znázornené, že zvyšujúca sa vzdialenosť medzi koncovým zariadením a bránou spôsobuje vyššie oneskorenie v prenose. Samotná doba prenosu sa tiež zvyšuje navyšujúcim sa faktorom rozprestrenia, čím sa znižuje aj prenosová rýchlosť. Najvyššia možná komunikačná vzdialenosť bola stanovená na 9066 m kde je celková doba prenosu 1676,83 ms a prijímací výkon správy je -142,5 dBm. Výsledky oboch simulácií sú prehľadne spracované do tabuliek, z ktorých sú následne zostrojené grafické závislosti.

Práca je nakoniec venovaná modifikácii použitého LoRaWAN modulu pre NS-3. Modifikácia sa zameriava na rozšírenie frekvenčného pásma, kde modul podporoval iba sub-GHz frekvenčné pásmo pre EU (868 MHz). Implementované boli frekvenčné pásma pre US región (915 MHz) a 2,4 GHz pásmo pre EU región. Následne boli na novoimplementovaných frekvenčných pásmach vykonané simulácie na porovnanie so stávajúcim sub-GHz pásmom pre EU. Zo simulácií je zrejmé, že nové, vyššie frekvenčné pásma a dátové rýchlosti pozitívne vplývajú na dobu prenosu správ. Zatiaľ čo doba prenosu pre stávajúce sub-GHz pásmo pre EU sa pohybovala v rozmedzí od 71 do 75 ms, frekvenčné pásmo pre US malo dobu prenosu v rozmedzí od 33 do 37 ms a 2,4 GHz pásmo pre EU iba od 11 do 14 ms. Naproti tomu, percentuálna úspešnosť nového frekvenčného pásma pre US s rastúcim počtom koncových zariadení klesla pod 80% pri počte 2000 zariadení, zatiaľ čo stávajúce sub-GHz pásmo pre EU malo pri počte 2000 zariadení úspešnosť prenosu 83%. Frekvenčné pásmo 2,4 GHz pre EU si zachovalo úspešnosť prenosu nad 90% aj pri počte zariadení 2000 vďaka veľkej šírke pásma. Výsledky simulácií sú prehľadne spracované do tabuliek, z ktorých sú následne zostrojené grafické závislosti.

V rámci modifikácie modulu bolo pristúpené aj k teoretickej príprave pre ďalšie rozšírenie o obojsmernú komunikáciu a šifrovaný prenos. Modul v aktuálnej verzii podporuje iba jednosmernú komunikáciu z koncových zariadení na bránu a šifrovaný prenos nie je podporovaný vôbec. Modifikácie nebolo v rámci tejto práce z hľadiska vysokej komplexnosti modulu možné vykonať. Napriek tomu, bolo implementované

frekvenčné pásmo pre US región pripravené pre obojsmernú komunikáciu z hľadiska odlišnosti prenosových frekvencií pre uplinkovú a downlinkovú komunikáciu. Následne boli časti modulu, ktoré vyžadujú modifikáciu rozpísané pre zjednodušenie následnej praktickej implementácie. Rovnako boli popísané nároky na šifrovaný prenos. Modul v aktuálnej verzii nepodporuje pripojovacie procedúry pre koncové zariadenia pri ktorých sa v praxi zjednávajú a odvodzujú šifrovacie kľúče. Preto je popísaná možnosť implementácie šifrovania pomocou Diffie-Hellmanovho protokolu ako alternatíva k dohodnutiu šifrovacích kľúčov medzi jednotlivými zariadeniami.

Bibliografia

[1] GIPSON, Mel. Sensors - The Lifeblood of the Internet of Things. 2017.

[2] GILLIS, Alexander S. What is internet of things (IoT). 2020.

[3] FUJDIAK, Radek; MIKHAYLOV, Konstantin; STUSEK, Martin; MASEK, Pavel; AHMED, Ijaz; MALINA, Lukas; PARAMBAGE, Pawani; VOZNAK, Miroslav; POUTTU, Ari; MLYNEK, Petr. Security in Low Power Wide Area Networks: state-of-art and development towards the 5G. 2019.

[4] ZHOU, Liang. Mobile Device-to-Device Video Distribution: Theory and Aplication. 2016.

[5] Machine-to-Machine (M2M) Communication Challenges Established (U)SIM Card Technology. 2018.

[6] Massive Machine Type Communications 2017: IEEE Network Magazine Special Issue - Massive Machine Type Communications for 5G. 2017.

[7] MEKKI, Kais; BAJIC, Eddy; CHAXEL, Frederic; MEYER, Fernand. A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT express*. 2019, roč. 5, č. 1, s. 1–7.

[8] Chirp spread spectrum. 2020.

[9] KAHVECI, Salim; ATASOY, Tuğba. From Wireless Personal Area Network (WPAN) to Long Range (LoRa) Technology. In: *2019 11th International Conference on Electrical and Electronics Engineering (ELECO)*. 2019, s. 679–681.

[10] MASEK, Pavel; STUSEK, Martin; FUJDIAK, Radek; MLYNEK, Petr; HOSEK, Jiri. Komunikační systémy pro IoT. 2019.

[11] JANSSEN, Thomas; BNILAM, Noori; AERNOUTS, Michiel; BERKVENS, Raf; WEYN, Maarten. LoRa 2.4 GHz Communication Link and Range. *Sensors*. 2020, roč. 20, s. 4366. Dostupné z DOI: 10.3390/s20164366.

[12] PLETS, D.; JOSEPH, W.; VANHECKE, K.; TANGHE, E.; MARTENS, L. Simple Indoor Path Loss Prediction Algorithm and Validation in Living Lab Setting. 2013, roč. 68, s. 535–552. Dostupné z DOI: 10.1007/s11277-011-0467-4.

[13] RAZALI, N.A.M.; HABAEBI, M.H.; ZULKURNAIN, N.F.; ISLAM, M.R.; ZYOUD, A. The distribution of path loss exponent in 3D indoor enviroment. 2017, roč. 12, s. 7154–7161.

[14] ISKANDER, M.F. Channel Characterization and Propagation Models for LTE Path Loss Prediction in Urban and Suburban Ghana. 2019, roč. 11, s. 23–32.

[15] ALLIANCE, LoRa. What is LoRaWAN. 2020.

[16] N., Sornin; A., Yegin. LoRaWAN Backend Interfaces 1.0 Specification. 2017.

[17] GEMALTO; ACTILITY; SEMTECH. LoRaWAN Security. 2017.

[18] *National Institute of Standards and technology*. [B.r.].

[19] HENDERSON, Tom. What is NS-3. [B.r.].

[20] MAGRIN, Davide. LoRaWAN Module Documentation. *A Discrete-Event Network Simulator*. 2016.

[21] MAGRIN, Davide. Network Level Performances of a LoRa System. 2016.

[22] NETWORK, The Things. Regional Parameters. [B.r.].

[23] SEMTECH. The 2.4GHz Regional Parameters: ISM2400. [B.r.].

[24] Network Simulator 3: Documentation, A Discrete-Event Network Simulator. 2019.

[25] REYNDERS, Brecht; WANG, Qing; POLLIN, Sofie. A LoRaWAN module for ns-3: implementation and evaluation. 2018, s. 61–68.

[26] SEMTECH. Semtech SX128x Long Range Datasheet. 2019.

[27] MAGRIN, D.; CENTENARO, M.; VANGELISTA, L. Performance Evaluation of LoRa Networks in a Smart City Scenario. *in Proc. of the IEEE International Conference on Communications*. 2017.

Zoznam symbolov a skratiek

3GPP	3rd Generation Partnership Project - 3. generácia partnerského projektu
ABP	Activation By Personalization - Aktivácia personalizáciou
ADR	Adaptive Data Rate - Adaptívna prenosová rýchlosť
AES	Advanced Encryption Standard - Pokročilý šifrovací štandard
AppEUI	Application Extended Unique Identifier - Rozšírený unikátny identifikátor aplikácie
AppKey	Application Key - Aplikačný kľúč
AppNonce	Application Nonce - Jednorázový identifikátor zariadenia
AppSKey	Application Session Key - Aplikačný relačný kľúč
B	Byte - Bajt
b	bit
BPSK	Binnary Phase Shift Keying - Binárne kľúčovanie s fázovým posunom
BW	Bandwidth - Šírka pásma
CMAC	Cipher-based Message Authentification Code - Autentifikácia správ na základe šifrovania
CR	Coding Rate - Kódovací pomer
CSS	Chirp Spread Spectrum - Rozšírené spektrum chirp impulzov
CTR	Counter Mode Encryption - Šifrovanie režimom počítadla
d	Vzdialenosť
D2D	Device to Device - Zariadenie so zaraidením
dB	Decibell
DC	Duty Cycle - Strieda
DevAddr	Device Address - Adresa zariadenia
DevEUI	Device Extended Unique Identifier - Rozšírený unikátny identifikátor zariadenia

DevNonce	Device Nonce - Jednorázový identifikátor zariadenia
ECC	Electronic Communication Committee - Výber elektronickej komunikácie
EU	Európska Únia
FDD	Frequency Division Duplex - Duplex s frekvenčným delením
FEC	Forward Error Correction - Dopredná oprava chýb
FSK	Frequency Shift Keying - Kľúčovanie s frekvenčným posunom
FSPL	Free Space Path Loss - Útlm volného prostredia
GNU	GNU's Not Unix - GNU nie je Unix
GSM	Global System for Mobile communications - Globálny systém pre mobilné komunikácie
HTTPS	Hypertext Trasport Protocol Secure - Zabezpečený hypertextový prenosový protokol
Hz	Hertz
Chirp	Compressed High Intensity Radar Pulse - Stlačený vysoko intenzívny radarový impulz
IDP	Indoor Dominant Path - Dominantná cesta v interiéri
IoT	Internet of Things - Internet vecí
IP	Internet Protocol - Internetový protokol
ISM	Industrial, Scientific and Medical - Priemyselný, Vedecký a Zdravotnícky
JoinEUI	Join Extended Unique Identifier - Pripojovací rozšírený unikátny identifikátor
LAN	Local Area Network - Miesta sieť
LoRa	Long Range - Vysoký dosah
LoRaWAN	Long Range Wide Area Network - Rozľahlá sieť s vysokým dosahom
LoS	Line of Sight - Priama viditeľnosť

LPWAN	Low Power Wide Area Network - Rozľahlá sieť s nízkou energetickou náročnosťou
LTE	Long Term Evolution - Dlhotrvajúca evolúcia
M2M	Machine to Machine - Stroj so strojom
MAC	Media Access Control - Kontrola prístupu k médiu
MIC	Message Integrity Code - Kód integrity správy
mMTC	Massive Machine Type Communication - Masívna strojovo orientovaná komunikácia
MTC	Machine Type Communications - Strojovo orientovaná komunikácia
NB-IoT	Narrow Band Internet of Things - Úzkopásmový internet vecí
NetID	Network Identification - Identifikácia siete
NIST	National Institute of Standards and Technology - Národný inštitút pre štandardy a technológie
NS-3	Network Simulator 3 - Sieťový simulátor 3
NwkKey	Network Key - Sieťový kľúč
NwkSKey	Network Session Key - Sieťový relačný kľúč
OFDMA	Orthogonal Frequency Division Multiple Access - Ortogonálny viacnásobný prístup s frekvenčným delením
OTAA	Over The Air Activation - Aktivácia vzduchom
QoS	Quality of Service - Kvalita služby
QPSK	Quadrature Phase Shift Keying - Kvadratúrne kľúčovanie s fázovým posunom
s	Sekunda
SC-FDMA	Single Carrier Frequency Division Multiple Access - Viacnásobný prístup s frekvenčným delením jednej nosnej
SF	Spreading Factor - Faktor rozprestrenia
SIR	Signal to Interference Ratio - Pomer medzi signálom a rušením

TCP	Transmission Control Protocol - Protokol riadenia prenosu
TDD	Time Division Duplex - Duplex s časovým delením
TDMA	Time Division Multiple Access - Viacnásobný prístup s časovým delením
US	United States - Spojené Štáty
VPN	Virtual Private Network - Virtuálna privátna sieť
WAN	Wide Area Network - Rozľahlá sieť
WiFi	Wireless Fidelity - Bezdrôtová vernosť

A Výpisy kódu

Výpis A.1: Funkcia pre všeobecné nastavenie komunikačného kanálu.

```
1  void
2  LorawanMacHelper::ApplyCommonUsConfigurations (Ptr<LorawanMac>
       lorawanMac) const
3  {
4    NS_LOG_FUNCTION_NOARGS ();
5
6    LogicalLoraChannelHelper channelHelper;
7    channelHelper.AddSubBand (902, 928, 0.015, 30); //(firstFrequency,
         lastFrequency, DutyCycle, maxTxPower)
8
9    Ptr<LogicalLoraChannel> lc1 = CreateObject<LogicalLoraChannel> (903.1,
         0, 4); //(frequency, minDataRate, maxDataRate)
10   channelHelper.AddChannel (lc1);
11
12   lorawanMac->SetLogicalLoraChannelHelper (channelHelper);
13
14   lorawanMac->SetSfForDataRate (std::vector<uint8_t>{10, 9, 8, 7, 8});
15   lorawanMac->SetBandwidthForDataRate (
16       std::vector<double>{125000, 125000, 125000, 125000, 500000});
17   lorawanMac->SetMaxAppPayloadForDataRate (
18       std::vector<uint32_t>{30, 61, 133, 230, 230});
19 }
```

Výpis A.2: Funkcia pre nastavenie koncového zariadenia.

```
1  void LorawanMacHelper::ConfigureForUsRegion
       (Ptr<ClassAEndDeviceLorawanMac> edMac) const
2  {
3    NS_LOG_FUNCTION_NOARGS ();
4    ApplyCommonUsConfigurations (edMac);
5    edMac->SetTxDbmForTxPower (std::vector<double>{30, 20});
6
7    // Matrix to know which DataRate the GW will respond with
8    LorawanMac::ReplyDataRateMatrix matrixUL = {{{{0, 0, 0, 0}},
9                                                 {{1, 0, 0, 0}},
10                                                {{2, 1, 0, 0}},
11                                                {{3, 2, 1, 0}},
12                                                {{4, 3, 2, 1}},
13                                                {{5, 4, 3, 2}}}};
```

```
14    edMac->SetReplyDataRateMatrix (matrixUL);
15    edMac->SetNPreambleSymbols (8);
16    edMac->SetSecondReceiveWindowDataRate (0);
17    edMac->SetSecondReceiveWindowFrequency (923.3);
18  }
19
20  void LorawanMacHelper::ConfigureForUsRegion (Ptr<GatewayLorawanMac>
        gwMac) const
21  {
22    NS_LOG_FUNCTION_NOARGS ();
23    Ptr<GatewayLoraPhy> gwPhy =
24        gwMac->GetDevice ()->GetObject<LoraNetDevice> ()->GetPhy
            ()->GetObject<GatewayLoraPhy> ();
25    ApplyCommonUsConfigurations (gwMac);
26    if (gwPhy)
27      {
28        NS_LOG_DEBUG ("Resetting reception paths");
29        gwPhy->ResetReceptionPaths ();
30        std::vector<double> frequenciesUL;
31  // For Data Rate 0-3
32        for (int i=0; i<64; i++){
33          frequenciesUL.push_back (i*0.2+902.3);
34        }
35  // For Data Rate 4
36        for (int i=0; i<8; i++){
37          frequenciesUL.push_back (i*1.6+903.0);
38        }
39        for (auto &fUL : frequenciesUL)
40          {
41            gwPhy->AddFrequency (fUL);
42          }
43        int receptionPaths = 0;
44        int maxReceptionPaths = 8;
45        while (receptionPaths < maxReceptionPaths)
46          {
47            gwPhy->GetObject<GatewayLoraPhy> ()->AddReceptionPath ();
48            receptionPaths++;
49          }
50      }
51  }
```

Výpis A.3: Funkcia pre všeobecné nastavenie komunikačného kanálu.

```
1  void
2  LorawanMacHelper::ConfigureForUsRegion (Ptr<ClassAEndDeviceLorawanMac>
       edMac) const {
3    LorawanMac::ReplyDataRateMatrix matrixDL = {{{{8, 8, 8, 8, 8}},
4                                                 {{9, 8, 8, 8, 8}},
5                                                {{10, 9, 8, 8, 8}},
6                                               {{11, 10, 9, 8, 8}},
7                                              {{12, 11, 10, 9, 8}},
8                                             {{13, 12, 11, 10, 9}},
9                                            {{14, 13, 12, 11, 10}}}};
10 }
11
12 void
13 LorawanMacHelper::ConfigureForUsRegion (Ptr<GatewayLorawanMac> gwMac)
       const {
14   if (gwPhy) // If cast is successful, there's a GatewayLoraPhy
15     {
16       std::vector<double> frequenciesDL;
17
18       for (double i=923.3; i <= 927.5; i+0.6){
19         frequenciesDL.push_back (i);
20       }
21       for (auto &fDL : frequenciesDL)
22         {
23           gwPhy->AddFrequency (fDL);
24         }
25     }
26 }
27
28 void
29 LorawanMacHelper::ApplyCommonUsConfigurations (Ptr<LorawanMac>
       lorawanMac) const {
30   channelHelper.AddSubBand (922, 928, 0.015, 30);
31
32   Ptr<LogicalLoraChannel> lc2 = CreateObject<LogicalLoraChannel> (923.3,
       8, 13);
33   channelHelper.AddChannel (lc2);
34
35   lorawanMac->SetLogicalLoraChannelHelper (channelHelper);
36 }
```

B Obsah elektronickej prílohy

- `/` ..... koreňový adresár priloženého archívu
  - `ns-3.30.1/` ..... zložka so súbormi pre NS-3
    - `scratch/` ..... zložka so zdrojovým kódom
      - `complete-network-example.cc` ..... zdrojový kód
    - `src/` ..... zložka s modulmi
      - `lorawan/` ..... zložka s lorawan modulom
        - `.github/`
        - `doc/`
        - `examples/`
        - `helper/`
        - `model/`
        - `test/`
        - `.gitignore`
        - `.travis.yml`
        - `generate_docs.sh`
        - `LICENSE`
        - `NS3-VERSION`
        - `README.md`
        - `VERSION`
        - `wscript`
  - `xbahna00_DP.pdf` ..... elektronická verzia diplomovej práce