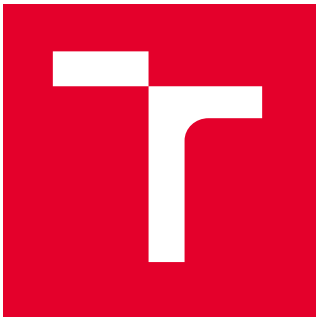


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

ŘÍZENÍ A SPRÁVA DOBÍJECÍCH STANIC PRO ELEKTRICKÁ VOZIDLA S VYUŽITÍM TECHNOLOGIÍ LPWA.

EV CHARGING STATION CONTROL AND MANAGEMENT UTILIZING LPWA TECHNOLOGIES.

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE — Martin Mačina

AUTHOR

VEDOUCÍ PRÁCE — Ing. Radim Dvořák

SUPERVISOR

BRNO 2023

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Student: Martin Mačina ***ID:*** 230620

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

NÁZEV TÉMATU:

Řízení a správa dobíjecích stanic pro elektrická vozidla s využitím technologií LPWA.

POKYNY PRO VYPRACOVÁNÍ:

Cílem bakalářské práce je popsat aktuální stav problematiky komunikace mezi dobíjecími stanicemi elektrovozidla a centrálním systémem pro správu těchto stanic v místech, kde nejsou dostupné konvenční metody připojení k Internetu. V rámci práce bude vytvořen program pro simulaci nabíjecí stanice v programovacím jazyce Python implementující protokol OCPP v2.0.1. Student navrhne ideální scénář zabezpečení přenosu dat a autentizace zařízení, které bude následně implementováno. Vytvořený program bude následně upraven pro přenos pomocí technologií LPWA (NB-IoT, LTE Cat-M). Následně budou otestovány parametry přenosu dat protokolu OCPP v2.0.1 skrze technologie LPWA v oblastech vhodných pro umístění dobíjecích stanic (podzemní/nadzemní garáže, parkoviště, čerpací stanice).

DOPORUČENÁ LITERATURA:

Podle pokynů vedoucího práce.

Termín zadání: ***Termín odevzdání:*** 17.8.2023

Vedoucí práce: Ing. Radim Dvořák

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

ABSTRAKT

Bakalárska práca sa zaoberá prenosom OCPP (Open Charge Point) protokolu pomocou LPWA (Low – Power Wide Area technologii). Na začiatku teoretickej časti je popísaný protokol OCPP, kde je kladený dôraz na bezpečnosť protokolu. Ďalej sú popísané LPWA technológie a ich parametre. V praktickej časti je predstavená komunikácia medzi OCPP klientom a OCPP serverom a popísané kľúčove prvky sprostredkovania tejto komunikácie. Ďalej sa zaoberá dokončením implementácie protokolu OCPP v jazyku Python a skompletovaním merania pomocou modulu BG77. Výsledkom praktickej časti je skompletované meranie pomocou LPWA modulu na lokalitách, ktoré sú zobrazené na vytvorenej mape. Výsledkom práce je popis nameraných hodnôt a zhodnotenie využitia LPWA technológii na prenos OCPP protokolu.

KĽÚČOVÉ SLOVÁ

centrálny systém, komunikácia, klient, nabíjacia stanica, protokol server, technológie,

ABSTRACT

The bachelor thesis deals with the transmission of OCPP (Open Charge Point) protocol using LPWA (Low – Power Wide Area technology). At the beginning of the theoretical part is described the OCPP protocol, where the emphasis is put on the security of the protocol. Next, the LPWA technologies and their parameters are described. In the practical part, the communication between the OCPP client and the OCPP server was introduced and the key elements are described mediating this communication. It further discusses the completion of the implementation of the OCPP protocol in Python and the completion of the measurement using the BG77 module. The practical part results in a completed measurement using the LPWA module on the sites that are shown on the generated map. The result of the work is a description of the measured values and an evaluation of the use of LPWA technology for OCPP protocol transmission.

KEYWORDS

client, central system, communication, charge point, protocol, server,

Vysadené pomocou balíčku `thesis` verzie 4.07; `http://latex.feec.vutbr.cz`

MAČINA, Martin. *Riadenie a správa dobíjacích staníc pre elektrické vozidlá s využitím technológií LPWA*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2023, 61 s. Bakalárska práca. Vedúci práce: Ing. Radim Dvořák

Vyhlásenie autora o pôvodnosti diela

Meno a priezvisko autora:	Martin Mačina
VUT ID autora:	230620
Typ práce:	Bakalárska práca
Akademický rok:	2022/23
Téma závěrečnej práce:	Riadenie a správa dobíjacích staníc pre elektrické vozidlá s využitím technológií LPWA

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 bych poděkoval vedoucímu bakalářské práce panu Ing. Radimovi Dvořákovi, za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Obsah

Zoznam obrázkov

Zoznam tabuliek

Úvod

V dnešnom svete, kde elektronika vládne skoro v každej oblasti našich životov nie je prekvapením, že sa tento fakt pretavil aj do automobilového priemyslu. Dopyt po elektromobiloch za posledné roky stúpa raketovou rýchlosťou, vďaka čomu dochádza k nárastu dopytu po nabíjacích staniciach pre tieto automobily. Možno očakávať, že po vydaní Európskeho predpisu, ktorý má od roku 2035 zakázať predaj automobilov využívajúce fosílne palivá, bude tento dopyt ešte viac stúpať. Momentálna situácia mestskej infraštruktúry nie je pripravená na takýto vysoký počet vozidiel, avšak je viditeľné, že postupne dochádza k jej budovaniu. Nabíjacie stanice bude nutné umiestniť na všetky miesta s veľkým výskytom automobilov. Toto môže spôsobiť určité problémy (nadmerné vyťaženie siete) s dodávkou energie v obytných oblastiach ako sídliská, kde má každá domácnosť minimálne jedno vozidlo. Po pripojení vysokého počtu elektromobilov do lokálnej nabíjacej siete môže nastať spomalenie nabíjania, v niektorých prípadoch aj výpadok elektrickej siete z dôvodu preťaženia, takže je potrebné riadiť nabíjanie z hľadiska dostupnej kapacity siete. Ďalším problémom, ktorý je potrebné adresovať je zjednotenie komunikácie medzi nabíjacími stanicami rôznych výrobcov. Rada výrobcov využíva pre správu a riadenie svojich nabíjacích staníc proprietárne protokoly, prípadne riadenie nabíjacích staníc vôbec neimplementujú, čo výrazne znižuje možnosti pre efektívne riadenie dobíjania s ohľadom na možnosti siete. Riešenie tohto problému je skrytý vo vývoji otvorených (open-source) protokolov pre riadenie nabíjania a správu komunikácie medzi nabíjacími stanicami a elektromobilmi.

Najznámejší a najpoužívanejší je Open Charge Point Protocol (OCPP), ktorý je otvoreným štandardom pre správu nabíjacích staníc. Protokol OCPP bol vyvinutý v Holandsku. Do budúcna je predpoklad, že by sa protokol OCPP mal stať globálnym štandardom pre riadenie dobíjania a správu nabíjacích staníc a vyriešiť tak problém komunikácie nabíjacích staníc rôznych dodávateľov. Treba brať do úvahy aj široko-plošné pokrytie, z čoho vyplýva umiestnenie nabíjacích staníc aj na miesta so zhoršeným prístupom bez možnosti káblového pripojenia (staré podzemné garáže bez infraštruktúry, odľahlé parkoviská, mimo mesto atď.). Riešením môže byť využitie bezdrôtových technológií, ktorých nasadenie nevyžaduje ďalší zásah do rozvodovej infraštruktúry v inštalovaných oblastiach.

Je možnosť nasadiť bezdrôtové siete v mesh štruktúre (Wi–Fi alebo Bluetooth), čo ale nie je vhodné pre rozsiahle miesta. Ďalšou možnosťou sú technológie licenčného pásma NB–IoT a LTE Cat–M, ktoré by do budúcna mohli zaistiť konektivitu pre nabíjačky v týchto lokalitách.

Cieľom tejto práce je popis a dokončenie implementácie protokolu OCPP v programovacom jazyku Python s kladeným dôrazom na bezpečnosť a autentizáciu. Ná-

sledne testovanie vhodnosti aplikácie licenčných technológií LPWA pre prenos aplikačných dát protokolu OCPP pomocou technológií NB-IoT a LTE Cat-M v rámci rôznych prostredí s horším prístupom na internet.

1 Open Charge Point Protocol

Z dôvodu nárastu enviromentálnych problémov vzniká vo svete tlak na udržateľné postupy kvôli životnému prostrediu. Tým pádom zaznamenal enormný nárast sektor elektrických vozidiel. Tento nárast sľubuje výrazné zníženie emisii, pričom hlavným využitým prostriedkom je Open Charge Point Protocol (OCPP).

Protokol OCPP je open-source aplikačný protokol, ktorý slúži ku komunikácii medzi nabíjačkou elektrického vozidla a riadiacim systémom nabíjacích staníc CSMS (Charging Station Management System).

Cieľom tohto protokolu je zjednotenie komunikačného rozhrania a dátových formátov nabíjacích staníc od rôznych výrobcov. [1]. Protokol bol vytvorený holandskou nadáciou ELaadNL v roku 2009. Dnes je OCPP spravovaný Open Charge Aliance, ktorá tiež sídli v Holandsku. Je používaný veľkým množstvom dodávateľov a nabíjačiek po celom svete [2].

1.1 Štruktúra OCPP

Štruktúra pozostáva z riadiaceho systému nabíjacích staníc a nabíjacej stanice, ktorá disponuje nabíjacím zariadením pre elektrické vozidlo. Nabíjacia stanica je zložená z dvoch hlavných komponentov, ktoré sú nabíjacie zariadenie EVSE (Electric Supply Equipment) a konektor.

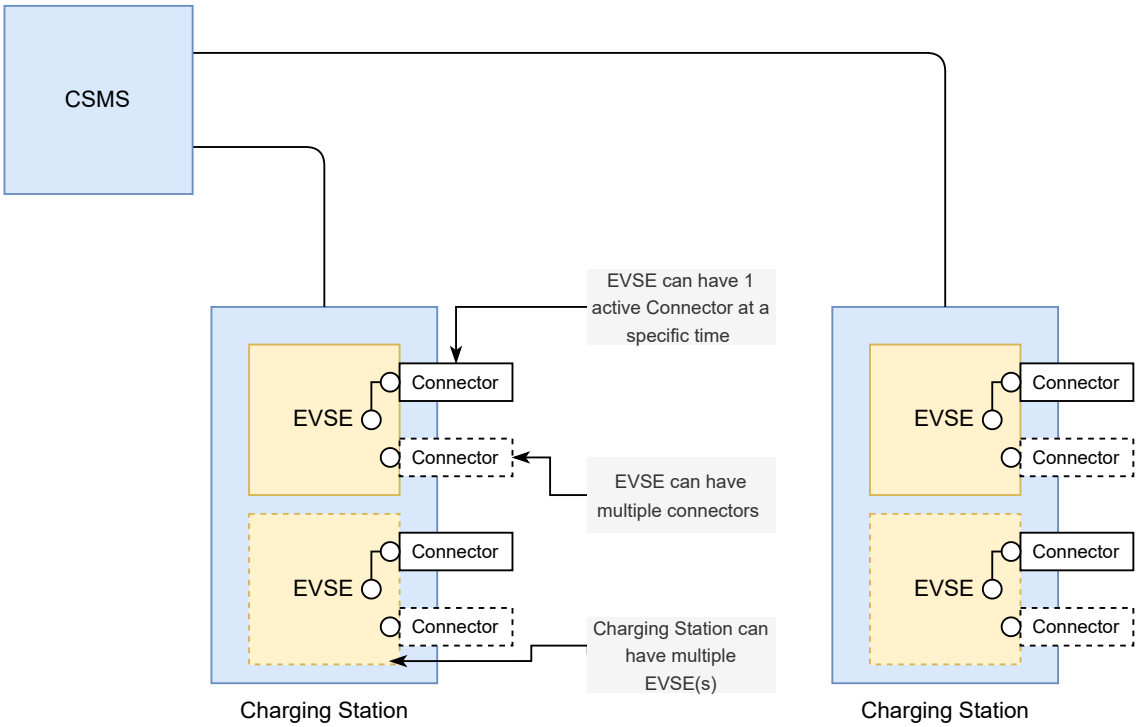
Nabíjacou stanicou sa rozumie fyzický systém, kde môže byť nabíjané elektrické vozidlo. Stanica môže mať viacero nabíjacích zariadení. EVSE je považované za časť nabíjacej stanice, ktorá dokáže doručiť energiu jednému elektrickému vozidlu. Konektor je považovaný za nezávisle prevádzkovanú a riadenú elektrickú zásuvku na čerpacej stanici. V niektorých prípadoch EVSE môže mať niekoľko typov zásuviek alebo usporiadania viazaného kábla alebo konektora pre možnosť nabíjania rôznych typov vozidiel. Štruktúru možno vidieť na obrázku 1.1 [3].

1.2 Verzie OCPP

Doposiaľ bolo vytvorených niekoľko verzií protokolu OCPP, pri čom dnes je najaktuálnejšia verzia 2.0.1 [1].

Staršie verzie protokolu OCPP

- **OCPP 1.2** – verzia podobná OCPP 1.5, ktorá má však menej funkcionalít.
- **OCPP 1.5** – je opísaných 25 operácií, z ktorých je 10 iniciovaných nabíjacou stanicou ďalších 15 centrálnym riadiacim systémom.



Obr. 1.1: Štruktúra OCPP

1.2.1 OCPP 1.6

Verzia 1.6 poskytuje niekoľko kľúčových funkcií, do ktorých sú napríklad zahrnuté vzdialené ovládanie umožňujúce centrálnemu systému vzdialene spustiť, zastaviť a monitorovať nabíjanie. Ďalšou funkciou je možnosť predošlej rezervácie nabíjacej stanice. Taktiež obsahuje správu firmvéru, ktorá umožňuje centrálnemu systému manažment firmvérových aktualizácií. Ďalej verzia umožňuje základné funkcie inteligentného nabíjania a spracovanie transakcií, ktoré zachytáva informácie o konkrétnom nabíjaní. Táto verzia umožňuje výmenu správ pomocou SOAP (Simple Object Access Protocol) a JSON (JavaScript Object Notation)[4].

SOAP je protokol na výmenu správ medzi odosielateľom a prijímateľom v decentralizovanom a distribuovanom prostredí. Tento protokol je schopný spolupracovať s rôznymi aplikačnými protokolmi ako sú HTTP (Hyper–text Transfer Protocol), TCP (Transmission Control Protocol), UDP (User Datagram Protocol). SOAP vracia odosielateľovi dáta v XML (Extensible Markup Language) formáte.

JSON je odľahčený formát na výmenu údajov, ktorý je ľahko čitateľný pre človeka. Tento formát je postavený na páre atribút–hodnota a je možné ho použiť v rôznych programovacích jazykoch [5].

1.2.2 OCPP 2.0.1

Verzia OCPP 2.0.1 bola navrhnutá, aby rozšírila a vylepšila schopnosti OCPP 1.6. Obsahuje všetky funkcie verzie 1.6 a niekoľko nových funkcií. Týmito funkciami sú napríklad:

- Vylepšené ovládanie komponentov umožňujúce detajlnejšiu kontrolu komponentov nabíjacej stanice
- Zvýšená bezpečnosť, ktorá zahŕňa TLS a autentizáciu založenú na certifikátoch.
- Zobrazenie správ poskytujúce dôležité informácie v reálnom čase pre vodiča vozidla.
- Plug-and-Charge funkcia, ktorá umožňuje automatickú autentizáciu elektrického vozidla so začiatkom nabíjania po pripojení nabíjacej stanice do vozidla. Táto funkcia využíva štandard ISO 15188, čo je medzinárodný štandard definujúci komunikáciu medzi elektrickým vozidlom a nabíjacou stanicou[6].

1.2.3 Porovnanie verzií OCPP 1.6 a OCPP 2.0.1

Zatiaľ čo obe verzie poskytujú funkcie ako je transfer dát, stav dostupnosti, ktorý udáva informáciu o dostupnosti nabíjacej stanice alebo funkcie inteligentného nabíjania, tak verzia 2.0.1 poskytuje viac pokročilé funkcie zlepšujúce celkové nabíjanie. Rozdiel je aj vo formáte, v ktorom sú správy posielané, čo znamená, že s príchodom novšej verzie bola odstránená podpora SOAP formátu správ.

Celkovo sa dá verzia 2.0.1 považovať za celkovo bezpečnejšiu a sofistikovanejšiu verziu ako 1.6, ktorá poskytuje vylepšené funkcie, zlepšené nabíjanie a zvýšenú úroveň zabezpečenia[4],[6].

1.3 Nové funkcie OCPP 2.0

OCPP 2.0 prináša nové funkcionality a vylepšenia oproti OCPP 1.6, kvôli ktorým nie je možná spätná kompatibilita s predošlými verziami OCPP.

1.3.1 Správa zariadenia

Správa zariadenia (Device Management), taktiež známy ako Device Model, je dlho očakávaná funkcia uvítaná najmä operátormi nabíjacích staníc CSOs (Charging Station Operators), ktorí riadia komplexnú sieť nabíjacích staníc od rôznych dodávateľov[6].

Poskytuje nasledovné funkcionality:

- Reporty inventára
- Vylepšené hlásenia chýb a stavu
- Vylepšenú konfiguráciu
- Prispôsobiteľné monitorovanie

Toto by malo CSOs pomôcť znížiť náklady na prevádzkovanie siete nabíjacích staníc. Výrobcovia nabíjacích staníc si môžu určiť, koľko detailov chcú zverejniť pomocou Device Managementu[7].

1.3.2 Zlepšená manipulácia veľkého množstva transakcií

Jedna správa pre všetky funkcionality súvisiace s transakciou

Tým, že rastie počet elektromobilov, s ktorým súvisí nárast počtu nabíjacích staníc, tým rastie aj počet transakcií na správu pre CSMS. Štruktúra a metóda na report transakcií je v OCPP 2.0 unifikovaná. Vo verziách 1.x je report dát o transakcií rozdelený do viacerých správ StartTransaction, StopTransaction, MeterValue a StatusNotification. Všetky StartTransaction, StopTransaction, a s transakciou spojené MeterValue a StatusNotification správy sú nahradené správou „TransactionEvent“. StatusNotification správa stále existuje pre správy, ktoré nesúvisia s transakciami ale s notofikáciami o dostupnosti konektora[6].

Redukcia dát

S použitím JSON formátu oproti WebSocketom, čo prišlo vo verzii 1.6 nastala možnosť dosiahnuť výrazné zníženie nákladov na mobilné dáta. Vo verzii 2.0 prišla podpora WebSocket kompresie, ktorá ešte viac redukuje množstvo dát[7].

1.3.3 Vylepšenia kybernetickej bezpečnosti

Funkcionality posilňujúce OCPP proti kybernetickým útokom:

- Bezpečnostné profily (3 úrovne) pre autentizáciu nabíjacej stanice a/alebo CSMS a bezpečnosť komunikácie.
- Správa kľúčov pre certifikáty na strane klienta.
- Aktualizácie bezpečnostného firmvéru.
- Logy bezpečnostných eventov[7].

1.3.4 Podpora ISO 15118

ISO 15118 je nový protokol pre komunikáciu medzi EVSE a elektrickým vozidlom EV (Electric Vehicle). Umožňuje mnoho nových funckií a viac bezpečnú komunikáciu medzi EVSE. Novo pridané funkcie sú:

- **Plug & Charge** – technológia umožňujúca vodičom bezpečne a jednoducho sa identifikovať na nabíjacej stanici jednoduchým pripojením.
- **Inteligentné nabíjanie vrátane vstupu z EV**[7].

1.3.5 Vylepšenia OCPP-J

OCCP–J je varianta protokolu, postavená vo verzii 1.6, ktorá využíva JSON formát. Pokiaľ sa niekde v komunikácii medzi klientom a serverom objaví správa nereprezentovaná pomocou JSON formátu, tak nebude pre danú komunikáciu valídna.

Zrušená podpora pre SOAP

OCPP 2.0 naďalej nepodporuje SOAP. Rozhodli o tom členovia OCA (Open Charge Aliance), ktorí veria, že protokol už nie je vhodný pre obmedzené výpočtové zdroje, pod ktorými pracujú mnohé nabíjacie stanice. Verbozita protokolu mohla viesť k pomalšej výkonnosti s vyžadovaním vyššej šírky pásma, ktorá v mnohých prípadoch vedie k vyššej cene mobilných dát. SOAP je ťažko podporovteľný, ak komunikácia prebieha prostredníctvom lokálnej siete[7].

Jednoduché smerovanie správ

Pri implementácii lokálneho kontroléra je pre niektoré topológie vyžadované smerovať OCPP–J správy. Toto vylepšenie má za úlohu to, že smerovanie správ bude fungovať pre akúkoľvek nabíjaciu stanica a CSMS[7].

1.3.6 Vylepšenia zákaznickej skúsenosti

Oproti predchádzajúcim verziám protokolu OCPP, verzia 2.0 prináša niktoré vlastnosti navrhnuté pre zlepšenie zákazníckej skúsenosti pri používaní nabíjacích staníc využívajúcich tento protokol. Medzi vylepšenia patrí:

- **Viac spôsobov autorizácie** – Predošlé verzie OCPP 1.x boli z veľkej časti navrhnuté na autorizáciu vodiča EV nabíjaciou stanicou pomocou RFID karty alebo tokenu. Ak bol použitý iný spôsob autorizácie alebo spojenie viacerých autorizačných spôsobov, tak musí CSMS vedieť, ktorý spôsob bol použitý pre konkrétnu autorizáciu.

OCPP 2.0 bolo rozšírené o podporu autorizácie pomocou 15118 Plug & Charge, platobných terminálov, lokálnych mechanických kľúčov, mobilných telefónov a ďalších metód pre autorizáciu užívateľa.

- **Voľba preferovaného jazyka** – OCPP 2.0 ponúka možnosť zobrazovania správ na nabíjacej stanici v preferovanom jazyku, ktorý si vodiči zvolia.
- **Sadzba a náklady** – Nová implementácia protokolu OCPP 2.0 umožňuje nabíjacej stanici zobraziť užívateľovi cenu na základe aktuálnych tarifov pred začatím nabíjania vozidla. Taktiež umožňuje zobrazenie priebežného súčtu nákladov počas nabíjaceho procesu, prípadne celkové náklady po dokončení nabíjacieho procesu [7].

1.4 Bezpečnosť OCPP

Bezpečnostná časť OCPP bola vytvorená s cieľom posilniť a rozvíjať budúcu štandardizáciu a vývoj protokolu. Je založený na end-to-end bezpečnostnom dizajne, ktorý vytvorilo LaQuSo (Laboratory for Quality Software). Bezpečnostné požiadavky sú zahrnuté v bezpečnostných opatreniach nabíjacích staníc a CSMS pre podporu užívateľov OCPP. V rámci dizajnu bezpečnosti bol navrhnutý bezpečnostný funkčný blok tak, aby mohol byť nasadený do prístupu, ktorý OCPP poskytuje. Vždy keď je možné tak sa používajú štandardné webové technológie, ktoré zaručujú nákladovo efektívnu implementáciu využívajúcu dostupné webové knižnice a software. Nepoužívajú sa žiadne bezpečnostné opatrenia na aplikačnej vrstve[6].

Na základe týchto úvah je bezpečnosť OCPP založená na TLS a kryptografii pomocou verejného kľúča využívajúca X.509 certifikáty. Pretože CSMS sa zvyčajne chová ako server, nie sú implementovaní rôzni užívatelia alebo riadenie prístupu na základe rolí na nabíjacej stanici. Pre zmiernenie problému sa odporúča implementovať riadenie prístupu na CSMS. Aby bolo isté, že implementované mechanizmi nemožno obísť, nemalo by byť OCPP používané kvalifikovanými pracovníkmi, ktorý vykonávajú údržbu nabíjacích staníc, keďže na údržbu môžu byť použité iné protokoly[6].

1.4.1 Transport Layer Security

Transport Layer Security (TLS) je kryptografický protokol, ktorý sprostredkováva zabezpečenú komunikáciu v rámci počítačovej siete tak, že pracuje nad transportnou vrstvou. TLS sa zameriava na zabezpečenie komunikácie medzi komunikujúcimi stranami. Jeho hlavnou úlohou je zaistiť integritu pomocou symetrickej kryptografie a pripadnú autentizáciu pomocou certifikátov. Vďaka využitiu certifikátov je

užívateľ pri komunikácii uistený, že komunikuje so správnym serverom a pri výmene informácií, dáta nebudú napadnuté a zamenené za nepravdivé [8].

Funkcie TLS

Šifrovanie je použité k ochrane dôvernosti prenášaných dát. Dáta sú v zmenenej forme, v ktorej ich je schopný prečítať iba vlastník správneho dešifrovacieho kľúča. Toto zaručí, že pokiaľ budú dáta zachytené treťou stranou, tak ich nebude možné prečítať.

Autentizácia slúži k overeniu strán zahrnutých v komunikácii. K tomuto sa využívajú digitálne certifikáty vydané Certifikačnou Autoritou (CA). Certifikáty slúžia ako prevencia proti man–in–the–middle útokom. Vlastník a aj certifikát sú overený CA, to znamená, že nie je možné útok vykonať, pretože útočník nie je schopný dešifrovať prenášané správy. Server predloží svoj certifikát klientovi, aby preukázal svoju totožnosť klientovi. TLS taktiež umožňuje overenie totožnosti klienta serveru. Táto možnosť je však využívaná v prípadoch, kde je potrebná zvýšená bezpečnosť[8].

Zaistená integrita znamená, že sa predchádza možnému manipulovaniu s dátami počas prenosu, pomocou kontrolného súčtu message authentication code (MAC). Odosielateľ vypočíta MAC, ktorý pošle súčasne so správou. Prijímateľ vypočíta svoj MAC a porovná ho s prijatým kontrolným súčtom. Pokiaľ sa zhodujú, tak so správou nebolo manipulované počas prenosu [8].

Architektúra TLS

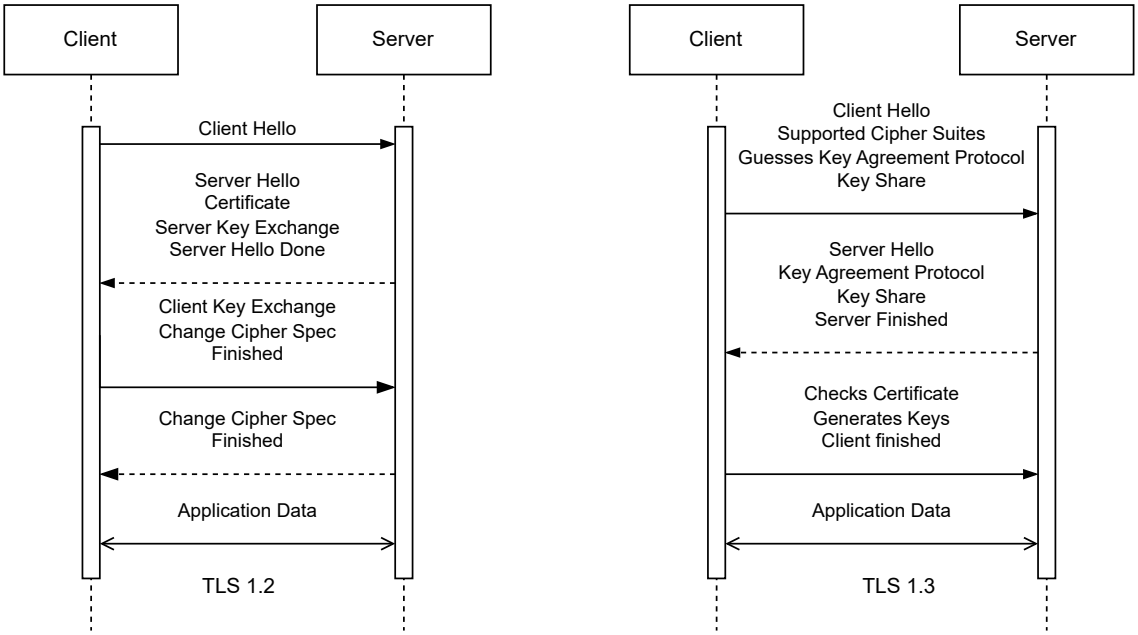
Architektúra TLS pozostáva z dvoch hlavných komponentov: TLS Record protokol a TLS Handshake protokol.

TLS Record protokol poskytuje bezpečnosť pripojenia s určitým stupňom šifrovania. Dáta sú šifrované pomocou symetrickej kryptografie. Pre každé pripojenie je generovaný unikátny kľúč, ktorý je dohodnutý pomocou ďalšieho protokolu (TLS Handshake). Pracuje nad spoľahlivým transportným TCP protokolom a zabezpečuje dôvernosť a integritu prenášaných dát. Jeho úloha spočíva v prijímaní dát na prenos, vo fragmentácii dát do zvládnuteľných blokov, voliteľne komprimuje dáta. Ďalej aplikuje MAC, šifruje ho a odosiela výsledok. Na výpočet MAC sa využívajú bezpečné hashovacie funkcie[8],[9].

TLS Handshake protokol je používaný k autentizácii servera a k vyjednaniu šifrovacieho algoritmu a kryptografických kľúčov pred tým, než aplikačný protokol odošle alebo príjme prvé dáta. Pokiaľ vyjednávanie z nejakého dôvodu zlyhá, na základe daného dôvodu sa môže pokúsiť o opakované nadviazanie spojenia, avšak je nutné zistiť presnú príčinu zlyhania. [8],[9].

TLS Handshake

TLS Handshake je proces, v ktorom klient a server zostavujú zabezpečené spojenie a dohadujú sa na kryptografických kľúčoch prípadne certifikátoch. Najskôr sa dohodnú pomocou asymetrického kľúča na symetrickej šifre a symetrickom kľúči, ktorý využijú na šifrovanie aplikačných dát. Tento proces má chrániť prenášané správy pred manipuláciou, falšovaním a odpočúvaním. Z obrázku 1.2 je vidieť, že verzia TLS 1.3 má omnoho jednoduchší priebeh, čo vo výsledku znižuje oneskorenie, zatiaľ čo je handshake v procese[10].



Obr. 1.2: TLS 1.2 a TLS 1.3 Handshake.

1.4.2 Štandard X.509

X.509 je štandardný formát definujúci certifikáty verejného kľúča. Využíva sa v rôznych protokoloch, ako je napríklad TLS, ktorý je základom pre Hyper Text Transfer Protocol Secure (HTTPS), čo je zabezpečený protokol slúžiaci k prehliadaniu internetu. Pri tomto využití sa užívateľ pripojí k HTTPS stránke a tá predloží X.509 certifikát prehliadaču na overenie jej totožnosti[11].

Ďalej sa tento štandard využíva aj pre digitálne dokumenty, ktoré spájajú páry kryptografických kľúčov s identitami. Tieto identity môžu byť webové stránky, organizácie alebo jednotlivci. Taktiež je štandard používaný aj v oblasti online bankovníctva a zabezpečení e–mailovej komunikácie.

Certifikát štandardu X.509 obsahuje verejný kľúč, identitu a je podpísaný CA alebo je možnosť využiť vlastnoručný podpis certifikátu[11].

Štruktúra X.509

Štruktúra X.509 je zostavená nasledovne:

- **Verzia** – verzia štandardu, podľa ktorej bol certifikát formátovaný.
- **Sériové číslo** – unikátne číslo, pridelené certifikátu CA.
- **ID algoritmu** – názov a parametre algoritmu použitého na podpis certifikátu.
- **Vydavateľ** – názov CA, ktorá vydala a podpísala certifikát.
- **Platnosť** – časový úsek počas, ktorého je certifikát platný obsahujúci dátum začiatku a konca platnosti.
- **Subjekt** – názov entity, pre ktorú bol certifikát vystavený (osoba, organizácia, počítač).
- **Informácie o verejnom kľúči subjektu** – obsahuje verejný kľúč vlastníka certifikátu.
- **Rozšírenia** – voliteľné dodatočné polia, ako použitie kľúča a ďalšie informácie o použití certifikátu.

Vďaka verejnému kľúču CA môže entita, ktorej bol predložený certifikát, overiť jeho pravosť dešifrovaním podpisu vydavateľa certifikátu[11].

1.4.3 Bezpečnostné profily

V tejto podkapitole sú rozpísané tri bezpečnostné profily viď tabuľka 1.1, ktoré štandard OCPP 2.0.1 podporuje.

Tab. 1.1: Bezpečnostné profily.

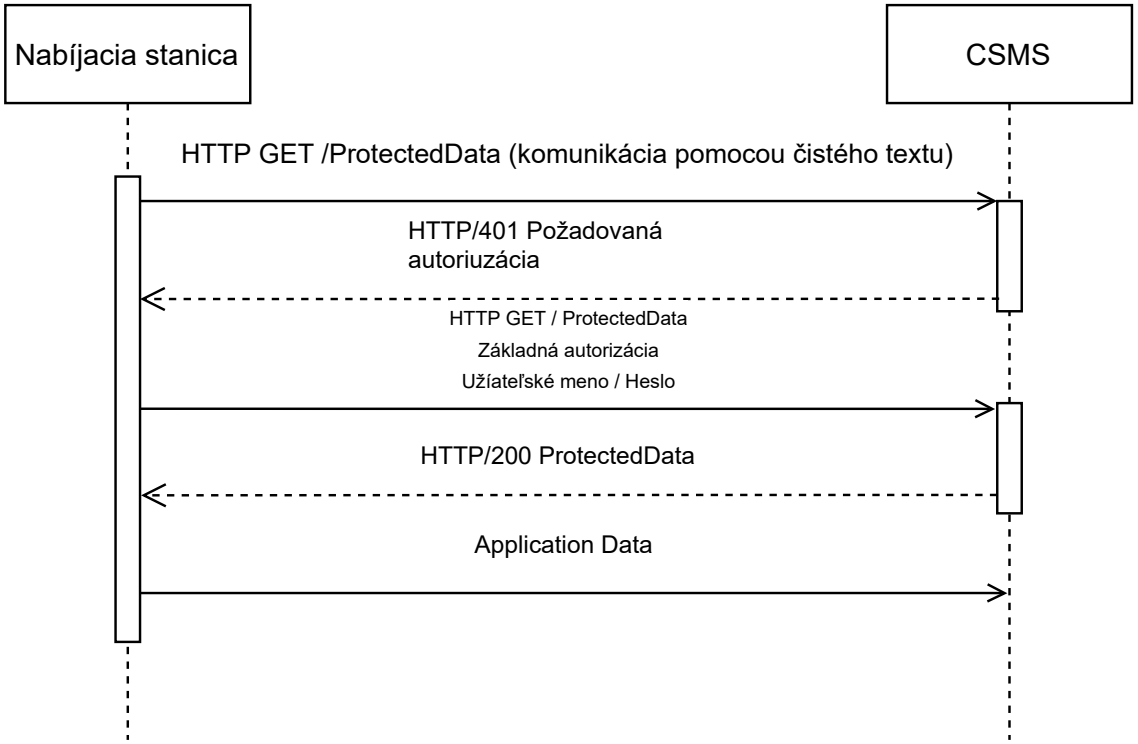
Profil	**Autentizácia nabíjacej stanice**	**Autentizácia CSMS**	**Bezpečnosť komunikácie**
Nezabezpečený prenos so základnou autentizáciou	Základná HTTP autentizácia		
TLS so základnou autentizáciou	Základná HTTP autentizácia	TLS autentizácia pomocou certifikátov	Transport Layer Security (TLS)
TLS s certifikátmi	TLS autentizácia pomocou certifikátov	TLS autentizácia pomocou certifikátov	Transport Layer Security (TLS)

Bezpečnostné profily majú niekoľko požiadavkov, ktoré sa nachádzajú v dokumentácii v tabuľke 12 [6].

Nezabezpečený transport so základným profilom overovania

Nezabezpečený prenos so základným overovaním poskytuje nízku úroveň zabezpečenia. Overovanie nabíjacej stanice sa vykonáva prostredníctvom používateľského mena a hesla. Nevykonávajú sa žiadne opatrenia na zabezpečenie komunikačného kanála. Pre autentizáciu nabíjacej stanice sa používa jednoduchá HTTP (Hypertext Transfer Protocol) autentizácia. V tomto profile sa CSMS neautentizuje voči nabíjacej stanici. Nabíjacia stanica musí veriť, že server, ku ktorému sa pripája, je skutočne CSMS. Taktiež nie sú zahrnuté žiadne opatrenia na zabezpečenie komunikácie[6].

Tento bezpečnostný profil nezahŕňa autentizáciu pre CSMS alebo opatrenia pre nastavenie bezpečného komunikačného kanála. Preto by sa mal používať len v dôveryhodných sieťach, napríklad v sieťach, v ktorých existuje VPN (Virtual Private Network) medzi CSMS a nabíjacou stanicou. Pri prevádzke v teréne sa odporúča používať bezpečnostný profil s TLS. V niektorých prípadoch (napr. laboratórne inštalácie, testovacie nastavenia atď.) možno uprednostniť použitie OCPP 2.0.1 bez implementácie zabezpečenia. Hoci je to možné, nepovažuje sa to za platnú implementáciu OCPP 2.0.1[6].

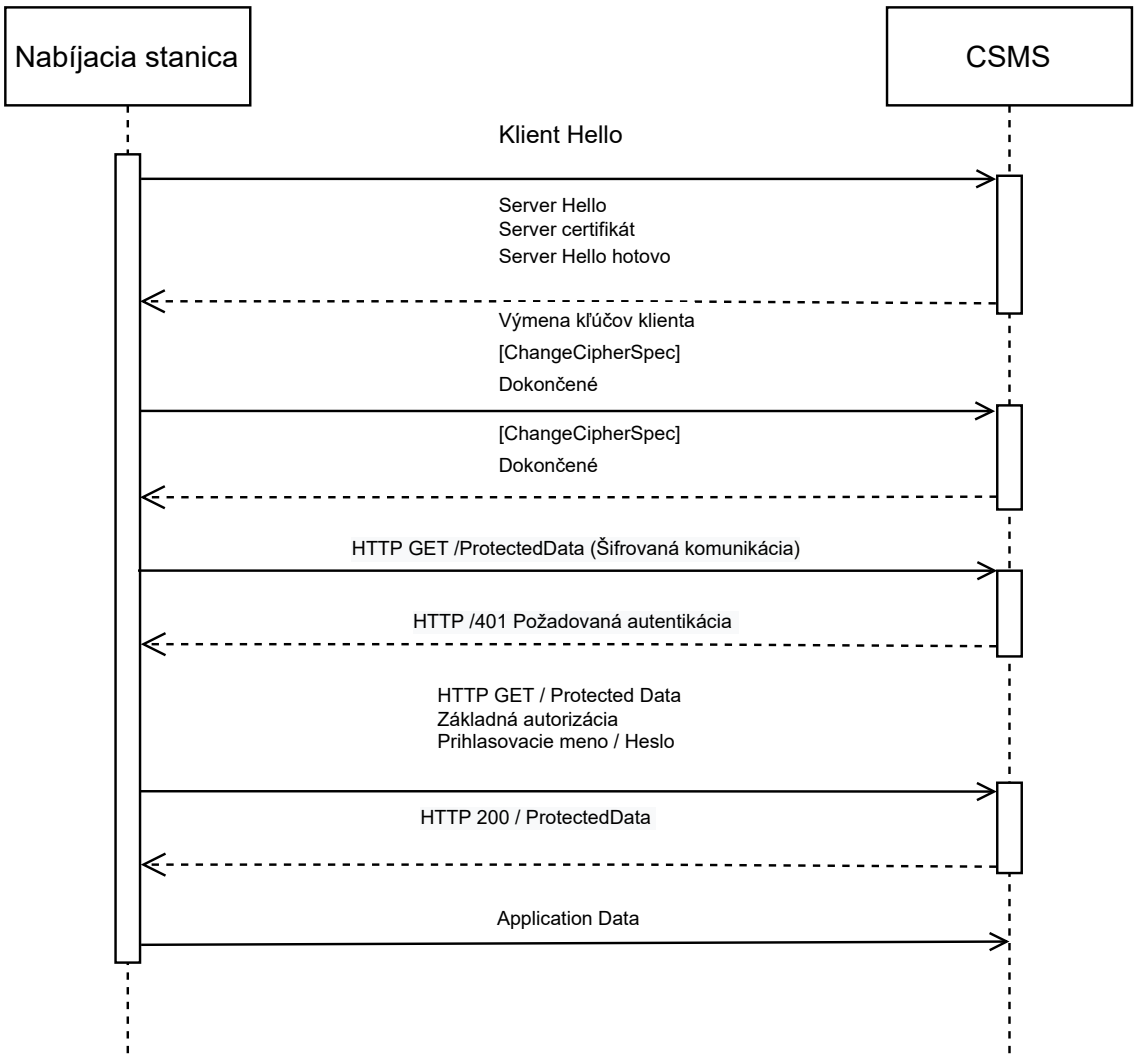


Obr. 1.3: Základný profil overovania.

TLS so základným profilom overovania

V profile TLS so základným overovaním je komunikačný kanál zabezpečený pomocou protokolu TLS. CSMS sa overuje pomocou TLS certifikátu servera. Nabíjacie stanice sa overujú pomocou základnej autentizácie HTTP.

Na overenie nabíjacej stanice sa používa overenie HTTP Basic. Keďže sa v tomto profile používa TLS, heslo sa posiela zašifrované, čím sa znižuje riziko pri používaní tejto metódy overovania. Nabíjacia stanica overuje CSMS prostredníctvom TLS certifikátu servera. Komunikácia medzi nabíjacou stanicou a CSMS je zabezpečená pomocou TLS[6].

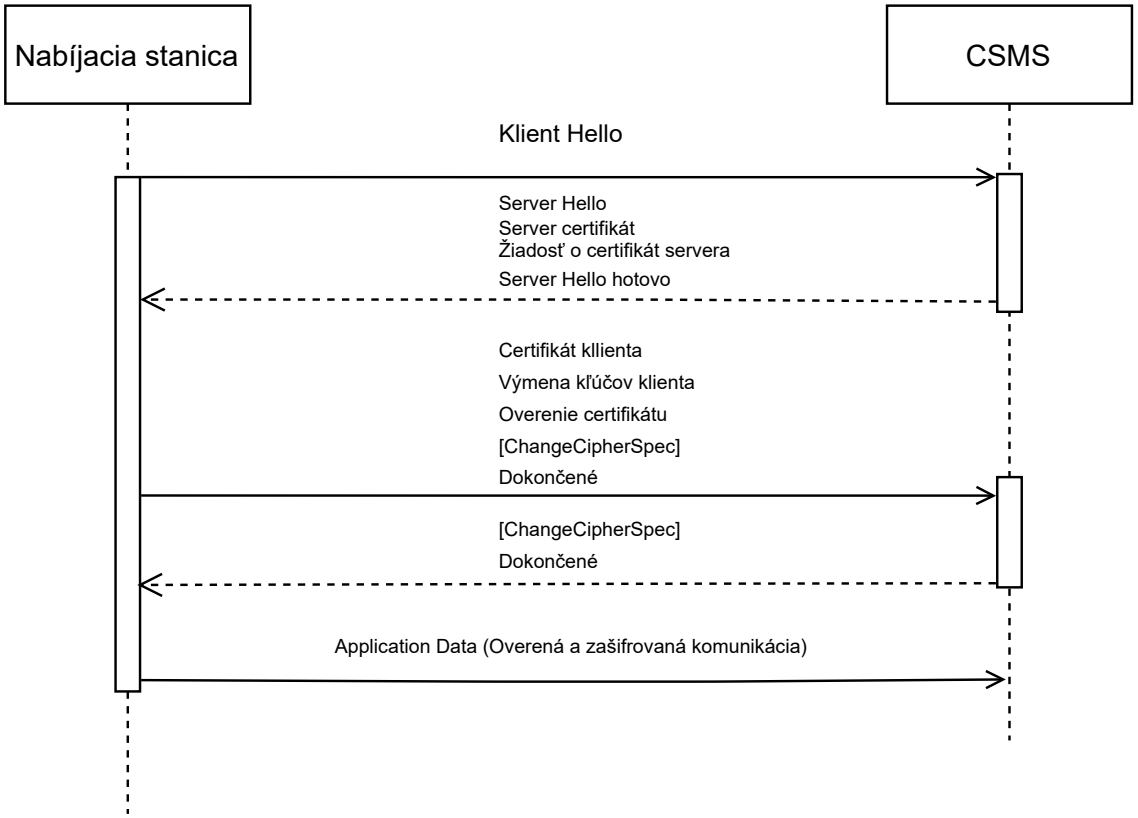


Obr. 1.4: Profil TLS so základným profilom overenia.

TLS s certifikátmi na strane klienta

V profile TLS s certifikátmi na strane klienta je komunikačný kanál zabezpečený pomocou protokolu TLS. Nabíjacia stanica aj CSMS sa overujú pomocou certifikátov. CSMS overuje nabíjaciu stanicu prostredníctvom klientskeho certifikátu TLS.

Nabíjacia stanica overuje CSMS prostredníctvom TLS certifikátu servera. Komunikácia medzi nabíjacou stanicou a CSMS je zabezpečená pomocou TLS[6].



Obr. 1.5: Profil TLS s certifikátmi na strane klienta.

1.4.4 Kľúče používané v OCPP

OCPP používa na zabezpečenie niekoľko párov verejných a súkromných kľúčov. Pre správu kľúčov na nabíjacej stanici, boli do OCPP pridané správy. Aktualizácia kľúčov v CSMS alebo u výrobcu je vykonávaná pomocou OCPP. Ak sa používa profil TLS s certifikátmi na strane klienta, nabíjacia stanica vyžaduje certifikát nabíjacej stanice na overenie voči CSMS[6].

Certifikáty používané v bezpečnostni OCPP

- **CSMS certifikát** – Kľúč používaný na overenie CSMS. Súkromný kľúč je uložený v CSMS.
- **Certifikát nabíjacej stanice** – Kľúč používaný na overenie nabíjacej stanice. Súkromný kľúč je uložený v nabíjacej stanici.
- **Certifikát na podpisovanie firmvéru** – Kľúč používaný na overenie podpisu firmvéru. Súkromný kľúč je uložený u výrobcu.
- **Certifikát State Elections Enforcement Commission (SEEC)** – Certifikát používaný podľa normy ISO15118-2 na nastavenie TLS medzi nabíjacou stanicou a elektrickým vozidlom. Súkromný kľúč je uložený v nabíjacej stanici[6].

1.4.5 Hierarchia certifikátov

Protokol OCPP podporuje používanie dvoch samostatných hierarchií certifikátov:

1. Hierarchia prevádzkovateľa nabíjacej stanice, do ktorej spadá CSMS a certifikáty nabíjacej stanice.
2. Hierarchia výrobcu, do ktorej spadá certifikát na podpisovanie firmwéru.

CSMS môže aktualizovať koreňové certifikáty operátora nabíjacej stanice uložené v nabíjacej stanici pomocou správy **InstallCertificateRequest**[6].

1.4.6 Zrušenie platnosti certifikátu

V niektorých prípadoch môže certifikát stratiť platnosť pred uplynutím doby platnosti.

Medzi takéto prípady patria napríklad:

- Zmena názvu organizácie.
- Kompromitácia súkromného kľúča certifikátu.
- Podozrenie na kompromitáciu súkromného kľúča certifikátu.

V takýchto prípadoch treba certifikát zrušiť alebo uviesť, že už nie je platný. Zrušenie certifikátu neznamená, že pripojenie musí byť uzavreté, pretože spojenie môže zostať otvorené dlhšie ako 24 hodín [6].

Tab. 1.2: Zrušenie certifikátov.

Certifikát	**Zrušenie**
CSMS certifikát	Rýchle vypršanie platnosti
Certifikát nabíjacej stanice	Online verifikácia
Certifikát na podpis firmvéru	Online verifikácia

1.5 Typy správ a ich odpovedí

Pre prenos informácie využíva protokol OCPP viacero typov správ, ktoré obsahujú informácie relevantné k danej komunikácii. Formát a štruktúra správ je pevne definovaná v štandarde protokolu OCPP. V nasledujúcej sekcii budú popísané vybrané správy protokolu OCPP pre komunikáciu medzi nabíjacou stanicou a CSMS, ktoré sú relevantné pre celkovú funkcionalitu systému[6].

1.5.1 Správa Data Transfer

Prenos dát je používaný ak nabíjacia stanica potrebuje doručiť správu pre centrálny riadiaci systém. Nabíjacia stanica pošle žiadosť na prenos dát `DataTransferRequest`, ktorá obsahuje niekoľko atribútov. Centrálny systém odpovedá správou `DataTransferResponse`.

V správe **DataTransferRequest** su použité tieto atribúty:

- **vendorId**
- **messageId**
- **data**

vendorId – Atribút vendorId identifikuje konkrétnu implementáciu protokolu OCPP, ktorú používajú predajcovia. Použitie tohto atribútu je v rámci prenosu medzi nabíjacou stanicou a centrálnym systémom **požadovaný** a využíva dátový typ string s dĺžkou [0–255].

messageId – Atribút messageId je možné použiť k identifikácii konkrétnej prenášanej správy alebo k indentifikácii použitej implementácie.

data – V tomto atribúte sú uložené prenášané údaje bez špecifikovanej dĺžky alebo formátu. O tom aký bude formát a dĺžka údajov musia rozhodnúť obe komunikujúce strany. Použitie tohto atribútu je **voliteľné**[6].

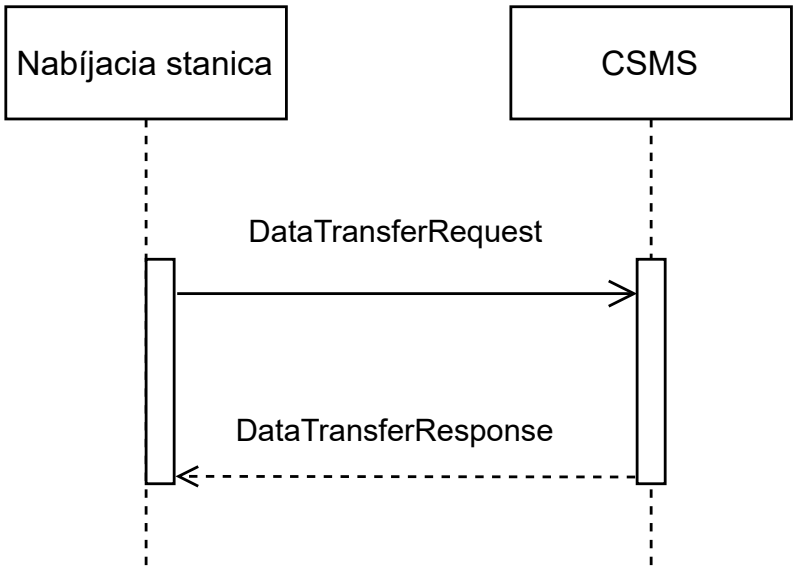
V odpovedi **DataTransferResponse** sa nachádzajú tri atribúty:

- **status**
- **data**
- **statusInfo**

status – Atribút status označuje či je prenos údajov úspešný alebo neúspešný. Tento atribút je pre odpoveď centrálneho systému **požadovaný**. Jeho využívaný dátový typ je DataTransferStatusEnumType.

data – V tomto atribúte sú uložené prenášané údaje bez špecifikovanej dĺžky alebo formátu. O tom aký bude formát a dĺžka údajov musia rozhodnúť obe komunikujúce strany. Použitie tohto atribútu je **voliteľné**.

statusInfo – Tento atribút obsahuje podrobné informácie o stave odpovede pre nabíjaciu stanicu. Použitie tohto atribútu je pri prenose dát **voliteľný**. Dátový typ, ktorý používa tento atribút je StatusInfoType[6].



Obr. 1.6: DataTransfer správa.

1.5.2 Autorizácia

Predtým, ako vodič elektrického vozidla môže začať alebo ukončiť nabíjanie, musí byť centrálnym systémom schválená transakcia. Nabíjacia stanica odošle centrálnemu systému správu `AuthorizeRequest`. Centrálny systém odpovie nabíjacej stanici odpoveďou `AuthorizeResponse`, v ktorej uvedie či je id-tag akceptovaý alebo nie[6].

Odpoveď musí obsahovať idTokenInfo, ktorý označuje prijatie alebo dôvod zamietnutia transakcie. Nabíjacia stanica odomkne konektor na nabíjanie až po úspešnej autorizácii vodiča[6].

V správe **AuhorizeRequest** sú používané tri atributy:

- **idToken**
- **certificate**
- **iso15118CertificateHashDat**

idToken – Atribút idToken obsahuje identifikátor podľa, ktorého je potrebné autorizovať vodiča vozidla. Použitie tohto atribútu je **požadované** a jeho použitý dátový typ je IdTokenType.

certificate – Tento atribút obsahuje certifikát X.509, ktorý je predložený elektrickému vozidlu pri autorizácii a zakódovaný vo formáte PEM (Privacy Enhanced Mail). Využitie tohto atribútu je **voliteľné** a jeho dátový typ je string s dĺžkou [0-5500][6].

iso15118CertificateHashDat – Atribút iso15118CertificateHashDat obsahuje informácie potrebné na overenie zmluvného certifikátu elektrického vozidla prostredníctvom internetového protokolu OCSP (Online Certificate Status Protocol). Použitie tohto atribútu je **voliteľné** a jeho použitý dátový typ je OCSPRequestDataType.

V odpovedi **AuthorizeResponse** sú používané dva atributy:

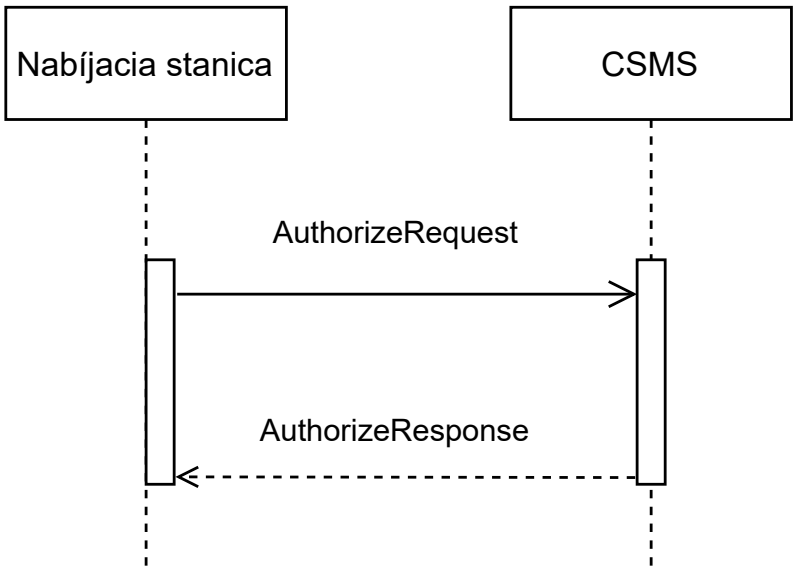
- **idTokenInfo**
- **certificateStatus**

idTokenInfo – Atribút obsahuje informácie o stave autorizácie vodiča, o vypršaní platnosti transakcie a identifikátore skupiny. Použitie tohto atribút je pre odpoveď **požadované**. Použitý dátový typ je IdTokenInfoType[6].

certificateStatus – Tento atribút obsahuje informácie o stave certifikátu. Ak sú všetky certifikáty platné, centrálny systém vráti hodnotu `Accepted`. Ak bol jeden z certifikátov zrušený, centrálny systém vráti hodnotu `CertificateRevoked`. Tento atribút je **voliteľný**. Použitý dátový typ je AuthorizeCertificateStatusEnumType[6].

1.5.3 Zmena dostupnosti

Centrálny systém pošle ChangeAvailabilityRequest, aby požiadal nabíjaciu stanicu o zmenu jej dostupnosti. Centrálny systém môže zmeniť dostupnosť na dva rôzne



Obr. 1.7: Authorize správa.

stavy. Tieto stavy určujú, či je nabíjačka dostupná alebo nedostupná[6].

Stav dostupná (Operative) znamená, že nabíjacia stanica nabíja alebo je pripravené na nabíjanie. Stav nedostupná (Inoperative) znamená, že nabíjacia stanica neumožňuje žiadne nabíjanie. Nabíjacia stanica musí odpovedať pomocou ChangeAvailabitilyResponse, aby uviedla, či je alebo nie je schopná zmeniť svoju dostupnosť. Správa **ChangeAvailabilityRequest** je posielaná centrálnym systémom do nabíjacej stanici a definujú atribúty **operationalStatus** a **evse**[6].

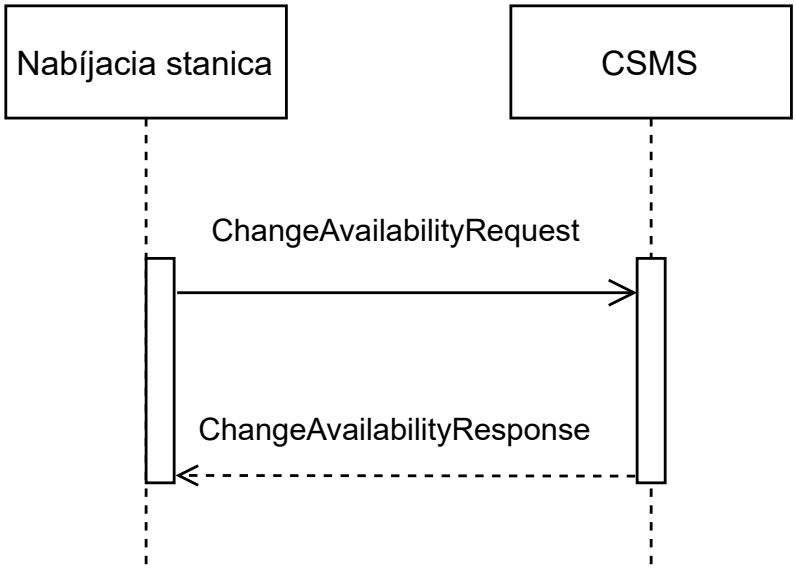
operationalStatus – Atribút operationalStatus obsahuje typ zmeny dostupnosti, ktorú má nabíjacia stanica vykonať. Tento atribút je pri posielaní žiadosti **požadovaný**. Použitý dátový typ je OperationalStatusEnumType.

evse – Atribút evse obsahuje identifikátory na označenie konkrétneho EVSE alebo nabíjaciu prípojku pomocou indexových čísel. Ak sa atribút evse vynechá, správa sa vzťahuje na nabíjaciu stanicu ako celok. Tento atribút je pri posielaní žiadosti **voliteľný**. Použitý dátový typ je EVSEType[6].

ChangeAvailabilityResponse je odpoveďou na žiadosť ChangeAvailabilityRequest a je definovaná atribútmi **status** a **statusInfo**.

status – Atribút status indikuje, či je nabíjacia stanica schopná vykonať zmenu dostupnosti. Tento atribút je pri posielaní **požadovaný**. Použitý dátový typ je ChangeAvailabilityStatusEnumType.

statusInfo – Atribút statusInfo obsahuje podrobné informácie o stave nabíjacej stanice. Tento atribút je pri posielaní odpovede **voliteľný**. Použitý dátový typ je StatusInfoType[6].



Obr. 1.8: ChangeAvailability správa.

1.6 Dátové typy

Dátové typy používané pri výmene správ medzi centrálnym systémom a nabíjacou stanicou sú priamo definované štandardom OCPP[6].

1.6.1 AuthorizationData

Tento dátový typ obsahuje identifikátor použitý k autorizácii. Používa dva atribúty:

- **idTokenInfo**
- **idToken**

idToken – V atribúte idToken je uložený identifikátor konkrétneho vodiča elektrického vozidla, ktorý je potrebné uložiť kvôli úspešnej autorizácii. Použitie tohto atribútu je pri implementácii vyžadované. Tento atribút využíva dátový typ IdTokenType.

idTokenInfo – V tomto atribúte sú uložené informácie o stave autorizácie, vypršaní platnosti a identifikátor skupiny. Pri diferenciálnej aktualizácii sa postupuje dvomi spôsobmi. V prvom prípade, ak je tento prvok prítomný, potom by táto položka

mala byť pridaná alebo aktualizovaná v zozname miestnych autorizácií. V druhom prípade, ak tento prvok chýba, položka pre IdToken sa v miestnom zozname autorizácií vymaže. Použitie tohto atribútu je voliteľné, avšak, ak je UpdateType plný, tak je použitie vyžadované[6].

1.6.2 ChargingProfileType

Inteligentné nabíjacie profily OCPP sú kombináciou priority používania, plánov a obmedzenia výkonu. ChargingProfile pozostáva z ChargingSchedule, ktorý opisuje množstvo energie alebo prúdu, ktoré možno dodať do elektrického vozidla za časový interval[6].
Dátový typ **ChargingProfileType** používa niekoľko atribútov. Popísané atribúty budú tieto:

- **id**
- **chargingSchedule**
- **chargingProfilePurpose**
- **validFrom**

id – Atribút id popisuje identifikátor konkrétneho nabíjacieho profilu patriaci vodičovi vozidla, ktorý práve nabíja. Použitie tohto atribútu je pri implementácii požadované a používaný dátový typ je integer.

chargingSchedule – Atribút chargingSchedule obsahuje rozvrh, v ktorom sú popísané limity na dostupný prúd alebo výkon v priebehu času s cieľom podporiť vyjednávanie o rozvrhu podľa normy ISO 15118. Atribút podporuje najviac tri rozvrhy s príslušnou tarifou, z ktorých si môžete vybrať. Použitie tohto atribútu je požadované a dátový typ, ktorý využíva je ChargingScheduleType[6].

chargingProfilePurpose – Tento atribút definuje účel harmonogramu prenášaný týmto profilom. Použitie tohto atribútu je požadované a dátový typ, ktorý využíva je ChargingProfilePurposeEnumType.

validFrom – Popisuje bod v čase, v ktorom sa profil stáva platný. Ak atribút nie je použitý, profil je platný hneď, ako ho prijme nabíjacia stanica. Použitie tohto atribútu je voliteľné a dátový typ, ktorý využíva je ChargingProfilePurposeEnumType [6].

2 Low–power Wide Area

Low–power Wide Area (LPWA) je súbor technológií, ktoré sú navrhnuté na prenos dát s využitím nízkych rýchlostí na veľké vzdialenosti. LPWA technológie disponujú vysokým komunikačným dosahom v rámci fungovania internetu vecí.

Technológie LPWA umožňujú komunikáciu vysokého počtu zariadení a poskytujú vysoké pokrytie signálom aj na miestach nedostupných konvenčným bezdrôtovým technológiám. Toto vedie k využitiu jednoduchých zariadení, ktoré znamenajú nižšie cenové náklady[12].

Tieto technológie sú využívané v rámci rôznych odvetví, čo môžu byť inteligentné domácnosti, monitorovanie infraštruktúry, logistika alebo poľnohospodárstvo. Z dôvodu nasadenia vysokého počtu senzorových jednotiek využívajúce tieto technológie, je kladený dôraz na nízku cenu komunikačného modulu a v prípade zariadení napájaných pomocou batérií aj na zníženie spotreby danej komunikačnej jednotky.

Je dôležité spomenúť fakt, že tieto technológie zvládajú operácie na dlhé vzdialenosti s nízkou spotrebou energie na úkor prenosových rýchlostí a vyššej latencie. Prenosové rýchlosti sa pohybujú od desiatok kb/s po niekoľko Mb/s. Čo sa týka oneskorenia komunikácie, to sa pohybuje v rádoch milisekúnd až niekoľkých minút. Toto znamená, že LPWA technológie nie sú určené, aby zastrešovali každý prípad využitia v rámci Internet of Things (IoT), ale sú určené pre určitú skupinu prípadov. Ich využitie je vhodné pre prípady, kde nie je kladený dôraz na vysoké prenosové rýchlosti a dĺžku oneskorenia, zatiaľ čo sú požadované nízke náklady s nízkou spotrebou energie [12].

Technológie LPWA sa dajú rozdeliť na dve skupiny. Technológie využívajúca bezlicenčné pásmo a technológie využívajúca licenčné pásmo.

2.1 Rozdiel medzi licenčným a bezlicenčným pásmom

Medzi technológie LPWA licenčného pásma patrí technológia LTE–M (Long Term Evolution for Machines), taktiež označované ako LTE Cat–M, a technológia NB–IoT (Narrowband IoT)[13].

Poskytujú niekoľko výhod oproti bezlicenčnému pásmu. Zariadenia se pripájajú už do existujúcich mobilných sietí operátora. Nie je teda potrebné budovať novú infraštruktúru. Za kvalitu služieb ručí operátor. Operátor má plnú kontrolu nad frekvenčným spektrom – zabránenie rušenia. Zabezpečenie dát na rádiovom rozhraní rieši operátor. Poskytuje neobmedzenú vysielaciu dobu a vysielací výkon (v rámci štandardov pre mobilné siete). Ďalej poskytuje neobmedzenú veľkosť správy (v rámci danej technológie väčšinou 1500B). Licenčné pásma sú pridelené operátorom na základe aukcie, ktoré usporiadava správca frekvenčného spektra v danej oblasti. Pre

Českú Republiku je daným správcom ČTÚ (Český telekomunikačný úrad). Nevýhodou je spoplatnený prístup do frekvenčného pásma[14].

Nelicenčné technológie LPWA siete sú LoRa a SigFox, ktoré v Európe využívajú pásmo 868 MHz. Jednou z hlavných výhod nelicenčného pásma je možnosť nezávislého povolenia súkromných sietí. Toto pásmo nezastrešuje žiadny operátor, takže frekvencie nie sú vyhradené. Rôzne regióny majú svoje rôzne frekvencie. Zatiaľ čo Európa používa pásmo 865–868 MHz, tak v USA je nutné použiť 902–928 MHz. Vo výsledku prináša náročnejšie plánovanie a vývoj produktov, pričom nie je nutné riešiť poplatky a zmluvy pásma ISM [1] v Českej Republike.

Nevýhody nelicenčných technológií sú veľké množstvo nelicencovaných zariadení čo môže mať za následok rušenie a nevyspytateľnosť rádiových podmienok, obmedzenie vysielacieho výkonu, obmedzenie doby vysielania, obmedzenie rýchlosti, obmedzenie veľkosti dátových jednotiek. Je nutné budovanie infraštruktúry pre plošné nasadenie [13, 14].

2.1.1 Metódy úspory elektrickej energie technológií licenčného pásma

Pre technológie licenčného pásma NB-IoT a LTE–M sú funkcie úspory energie nevyhnutnou súčasťou. Štandardizačná skupina 3GPP (3rd Generation Partnership Project) pre ne zaviedla dva štandardy úspory energie PSM (Power Saving Mode) a eDRX (Extended Discontinuous Reception).

Režimy úspory PSM

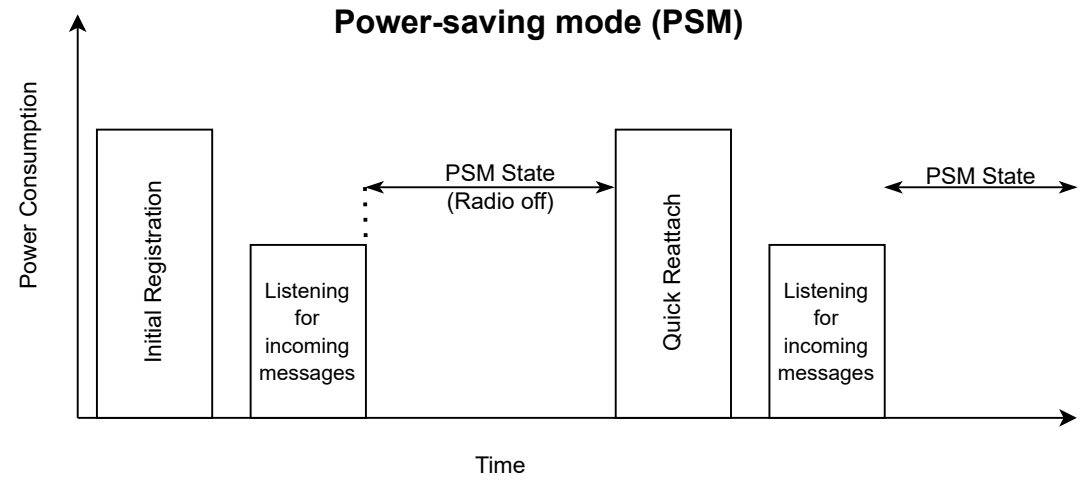
Režim úspory energie (PSM) bol zavedený v Release 12 3GPP s cieľom zlepšiť výdrž batérie zariadení IoT. Najdôležitejší benefit tohto režimu zlepšuje kontrolu správy napájania pri aplikáciach mobilných zariadení. Existuje množstvo aplikácií IoT, kde je dôležitá správa napájania mobilných zariadení a implementáciou PSM predísť preťaženiu siete. PSM umožňuje zariadeniam vstup do režimu spánku vypnutím väčšiny ich obvodov, zatiaľ čo ich pripojenie je stále registrované v sieti. Taktiež môžu byť kedykoľvek zobudené na prenos dát [15].

Režimy úspory eDRX

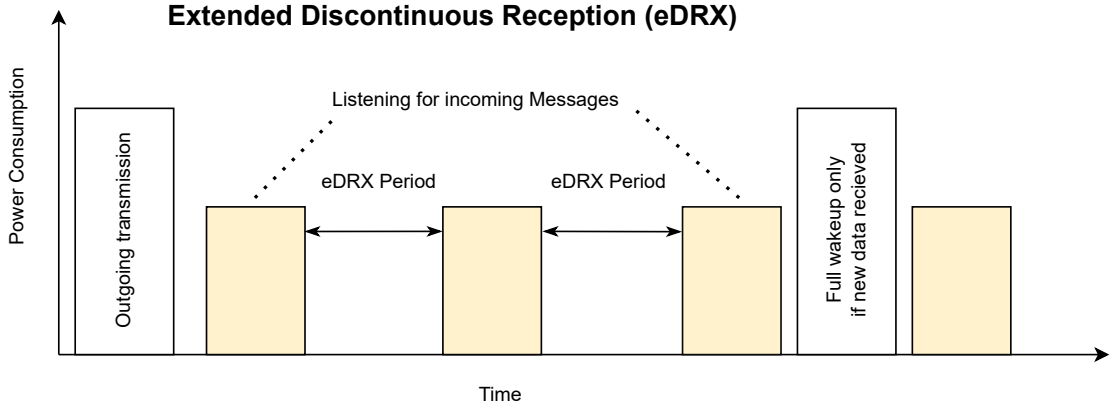
Režim úspory eDRX umožňuje zariadeniam IoT zostať v neaktivite dlhšie časové obdobie. Zariadenia sa periodicky zobúdzajú načúvajú na paging, či neprichádza nová správa. Interval, kedy sa zariadenia prebúdzajú je určený na základe dohody

[1] Industrial, Scientific and Medical Networks – Priemyselné, vedecké a medicínske siete

medzi užívateľským zariadením a základňovou stanicou, kde stanica vždy odpovedá posledné. [15].



Obr. 2.1: Režim úspory PSM.



Obr. 2.2: Režim úspory eDRX.

2.1.2 Technológia licenčného pásma NB–IoT

Narrowband IoT je bezdrôtová LPWA technológia. Bola vyvinutá skupinou 3GPP (Third Generation Partnership Project) pre umožnenie pripojenia nových zariadení do existujúcich celulárnych sietí vybudovaných operátorom. [16].

Táto rádiová technológia je najmä vhodná pre implementáciu v lokalitách s nízkou úrovňou pokrytia signálom (vnútri budov, pivnice, odľahlé lokality). Umožňuje pripojenie veľkého počtu zariadení s požiadavkom na dlhú výdrž batérie a nízku

cenu komunikačného modulu. Technológia NB-IoT disponuje prenosovou rýchlosťou 26kb/s vo verzii Cat-NB1 (3GPP Release 13) a 127kb/s vo verzii Cat-NB2 (3GPP Release 14). Technológia NB-IoT je navrhnutá podľa komunikačných princípov technológie LTE (Long Term Evolution) a disponuje šírkou pásma 180 kHz čo korešponduje so šírkou jedného fyzického zdrojového bloku PRB (Physical Resource Block) technológie LTE. To umožňuje jednoduché nasadenie tejto technológie do existujúcej infraštruktúry sietí štvrtej a piatej generácie. V závislosti od dostupnosti frekvenčného spektra sa môže byť NB–IoT zavedený buď samostatne ("standalone operation"), v ochranných pásmach existujúceho frekvenčného spektra LTE ("guardband operation") alebo v rámci existujúceho nosného pásma LTE ("inband operation") [17].

Nasadenia technológie NB-IoT

- **Stand Alone** – technológia môže používať frekvenčné pásmo GSM[2] s 200 kHz šírkou pásma a s ochranným intervalom 10 kHz na oboch stranách frekvenčného pásma.
- **Guard Band** – scenár, pri ktorom sa blok nevyužitých prostriedkov používa v rámci ochranného pásma operátora LTE.
- **In–Band** – režim, v ktorom dochádza k spoluexistencii v pásme operátora LTE [18].

Zobrazenie operačných módov je možné videit na obrázku 2.3.

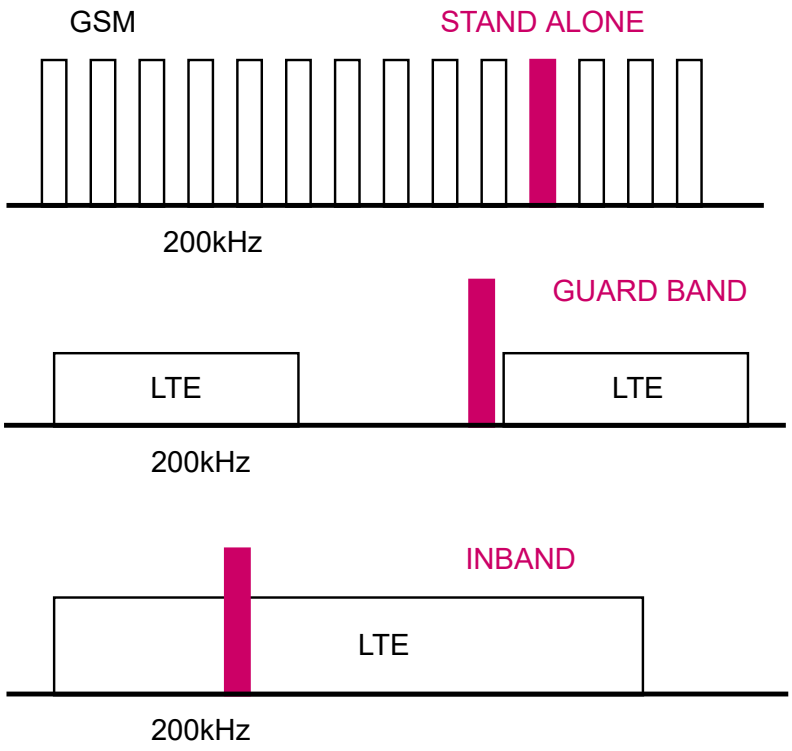
Keďže dizajn NB–IoT je založený na existujúcich funkciách LTE, poskytuje možnosť opätovne použiť rovnaký hardware a zdieľať frekvenčné pásmo, kde bude pripojený väčší počet zariadení, pričom nevznikne problém vzájomného rušenia[19].

Úrovne zlepšenia pokrytia NB-IoT

Rôzne úrovne zlepšenia pokrytia (ECL[3]) na základe rádiových podmienok, v ktorých sa dané zariadenie nachádzajú určujú nastavenie využitých modulačných a kódových schém pre prenos dát v oboch smeroch komunikácie (uplink, downlink) a zvyšujú tak robustnosť komunikácie aj v prípade, že sa zariadenie nachádza v prostredí so zhoršeným rádiovým signálom. Ďalej taktiež ovplyvňujú maximálny počet opakovaných pokusov o odoslanie správy. Tento počet opakovaní je v každej úrovni ECL vopred definovaný sieťou [20].

[2]Groupe Special Mobile

[3]Extended Coverage Level



Obr. 2.3: Operačné módy NB-IoT.

Popis jednotlivých úrovní:

- **ECL úroveň 0** – normálne pokrytie s MCL[4] ≈ 144 dB a s 15 kHz rozostupom medzi sub-poskytovateľmi.
- **ECL úroveň 1** – robustné pokrytie s MCL ≈ 154 dB a s 15 kHz rozostupom medzi sub-poskytovateľmi.
- **ECL úroveň 2** – extrémne pokrytie s MCL ≈ 164 dB a s 3,75 kHz rozostupom medzi sub-poskytovateľmi.

Výber úrovne pokrytia závisí na rádiových podmienkach vysielacieho kanála. Normálna úroveň pokrytia zodpovedá vysokej úrovni prijímaného signálu, zatiaľ čo extrémny level pokrytia zodpovedá nízkej úrovni prijímaného signálu. Všetky zvolené levely definujú parametre prenosu a počet opakovaní uplinkových a downlinkových správ [21].

2.1.3 Technológia licenčného pásma LTE–M

LTE–M je technológia LPWA licenčného spektra umožňujúca pripojenie zariadení so strednými nárokmi na prenosovú rýchlosť. LTE–M je technológia založená na štandarde LTE, kde je znížená zložitosť zariadení vzhľadom k požiadavkom technológií

[4]Maximum coupling loss

LPWA (odstránená podpora MIMO [5], implementácia režimov pre znížený potrebu). Jeho operácie môžu pracovať v nasadení **Stand Alone** alebo **In-Band**. Štandardizačná skupina 3GPP zaviedla v rámci LTE–M niekoľko nových funkcií a vlastností. Tieto funkcie boli uvedené skupinou 3GPP vo vydaní 12 (Release 12) a sú označované ako režim zníženej spotreby PSM a eDRX, a režim rozšírenia pokrytia A/B, atď.

Táto technológia je vhodná na prepojenie v stacionárnych aj mobilných prípadoch použitia aktív (napr. mobilná správa vozového parku alebo mobilné sledovanie aktív) za predpokladu, že v mieste zariadenia je pokrytie sieťou [22, 23].

Rozšírenie pokrytia CE

Technológia LTE–M podporuje dva režimy rozšírenia pokrytia: CE režim A a CE režim B. Oba tieto modely umožňujú režimu rozšírenia využívať opakovacie techniky pre dátové a kontrolné kanály. CE režim A dovoľuje pre dátový kanál 32-násobné opakovanie pri čom CE režim B dovoľuje až 2048-násobné opakovanie.

CE režim A je normálnym režimom pre operácie na LTE–M zariadeniach a LTE–M sieťach, poskytujúci dobré podmienky a je využívaný celý potenciál technológie. Jeho dizajn spĺňa výhody vyšších prenosových rýchlostí, hlasových hovorov a mobilitu v režime pripojenia, ktoré ponúka technológia LTE–M.

CE režim B je voliteľné rozšírenie poskytujúce ešte vyššie pokrytie. Úskalím je obmedzená funkcionalita a mobilita. Tento režim bol navrhnutý, aby zabezpečil pokrytie v rámci budov, vďaka čomu je viac vhodný pre stacionárne aplikácie alebo pre pešie aplikácie, ktoré vyžadujú obmedzené objemy prenosu dát a rýchlostí za mesiac [24].

[5] Multiple–Input Multiple–Output

3 Knižnica protokolu OCPP

K demonštrácii bola použitá knižnica vytvorená autorom *The Mobility House*, ktorá je dostupná na GitHube[1].

Komunikácia medzi dvomi stranami je postavená na protokole WebSocket, pomocou ktorého sú prenášané správy a odpovede. Tieto strany sú OCPP klient a OCPP server. Pred dotváraním požadovaných metód mala knižnica implementovanú komunikáciu na úrovni, kedy klient odoslal na server správu **BootNotificationRequest**, kedy server odpovedal pomocou **BootNotificationResponse**.

3.1 Obsah pôvodnej knižnice

Pred úpravami mala knižnica implementovanú len správu BootNotification. Táto správa indikuje zmenu stavu nabíjacej stanice z vypnutej na zapnutú, aby mohla vykonávať požadovanú aktivitu. Posielaná žiadosť nabíjacou stanicou sa nazýva **BootNotificationRequest** a jej odpoveďou je **BootNotificationResponse**.

3.1.1 BootNotificationRequest

Táto žiadosť obsahuje datové jednotky PDU (Protocol Data Units) posielané nabíjacou stanicou do centrálneho systému.

BootNotificationRequest obsahuje dva atribúty, ktorých použitie je vyžadované v rámci implementácie protokolu OCPP. Prvý atribút je **reason** s použitým dátovým typom **BootReasonEnumType**. Tento atribút vraví o dôvode, prečo bola žiadosť odoslaná centrálnemu systému. Druhý použitý atribút je **chargingStation**, ktorého dátový typ je **ChargingStationType**. Identifikuje konkrétnu nabíjaciu stanicu, ktorá odoslala žiadosť[6].

3.1.2 BootNotificationResponse

BootNotificationResponse je odpoveďou na BootNotificationRequest s konkrétnymi PDU, ktorú posiela centrálny systém nabíjacej stanici.

Táto odpoveď využíva štyri atribúty, z ktorých tri sú pre implementáciu vyžadované. Atribut **currentTime** využíva dátový typ **dateTime**. Obsahuje konkrétny čas centrálneho systému. **Interval** je atribut využívajúci dátový typ **integer**, a ak centrálny systém odpovie statusom `Accepted`, atribut bude obsahovať heartbeat

[1]Link na použitú knižnicu.

interval udávaný v sekundách. Ak centrálny systém odpovie inak, tak hodnota intervalu indikuje minimálny čas čakania pred odoslaním ďalšej BootNotificationRequest. Atributom **status** je povedané, či je daná nabíjacia stanica zaregistrovaná do centrálneho systému alebo nie. Využíva dátový typ **RegistrationStatusEnumType**. Posledný atribut **statusInfo** nie je nutné použiť pri implementácii. Obsahuje detailný popis informácií o statuse. Použitý dátový typ je StatusInfoType [6].

3.2 WebSocket protokol

Protokol WebSocket je schopný zabezpečiť obojsmernú komunikáciu medzi klientom a serverom, kde klient spúšťa nedôveryhodný kód v kontrolovanom prostredí. Model využitý pre zabezpečenie je origin-based model, ktorý je bežne používaný webovými prehliadačmi. Protokol je zostavený z úvodného handshake, po ktorom sa pokračuje základným rámcovaním správ, navrstvených nad TCP protokolom. Konečným cieľom tejto technológie prenosu je poskytnutie mechanizmu pre aplikácie založené na webovom prehliadači, ktoré potrebujú obojsmernú komunikáciu so servermi najmä v situáciach kedy nie je spoľah na otváranie viacerých HTTP spojení. Tento protokol je stavovým protokolom, čo znamená, že spojenie medzi klientom a serverom zostane funkčné po celý čas, kým ho jedna zo spomenutých strán neukončí. Po uzavretí spojenia buď klientom alebo serverom je spojenie ukončené na oboch stranách. Táto funkčnosť WebSocket protokolu je vhodná na využitie aplikácii v reálnom čase. Dáta sú posielané nepretržite v rámci jedného ustáleného otvoreného spojenia čo zaručuje rýchlosť a zvýšenie výkonu danej aplikácie [25].

3.2.1 Úvodný handshake

Úvodný handshake je prvým krokom nadviazania websocket spojenia. Počas otvárania klient odošle HTTP požiadavok na server, kde hlavička `Upgrade` je nastavená na `websocket` a hlavička `Connection` je nastavená na hodnotu `Upgrade`. Tento požiadavok taktiež zahŕňa hlavičku `Sec-WebSocket-Key`, kde je zakódovaná náhodná hodnota pomocou kódovania Base64. Server odpovedá HTTP odpoveďou so stavovým kódom `101 Switching Protocols`, ktorá znamená, že server prepína na websocket protokol. Odpoveď ešte obsahuje hlavičku `Sec-WebSocket-Accept`, kde je pomocou Base64 zakódovaný SHA1 hash hodnoty `Sec-WebSocket-Key` spojený s preddefinovaným reťazcom. Vďaka tomu sa zabezpečí, že server obdržal platný kľúč zaslaný klientom. Po skončení úvodného handshake si môžu klient a server vymieňať dáta pomocou websocketov [25].

3.3 Testovanie

Nadviazanie komunikácie bol prvý krok testovania. Pre túto demonštráciu bolo zvolené využitie dvoch virtuálnych systémov, na ktorých beží operačný systém Ubuntu. Jeden systém zastáva rolu nabíjacej stanice (klienta), zatiaľ čo druhý systém zastáva rolu centrálneho systému.

3.3.1 Prvotná komunikácia

Hlavným využitým prvkom bola knižnica OCPP, kde je použitá základná implementácia klienta aj centrálneho servera. Táto knižnica implementovala JSON verziu OCPP v jazyku Python. Pre realizovanie tejto demonštrácie bolo potrebné vytvoriť virtuálne prostredie (virtual environment), nainštalovať OCPP pomocou príkazu `$ pip install ocpp` a knižnicu websockets 10.4. Knižnica websockets slúži na vytváranie websocketov pre servery a ich klientov v jazyku Python so zameraním na správnosť, jednoduchosť, robustnosť a výkon [26]. Nadviazaná komunikácia bola zachytená v aplikácii pre analýzu sieťových prenosov Wireshark.

3.3.2 Virtual environment

Virtuálne prostredie je nástroj, ktorý poskytuje jazyk Python. Toto prostredie pomáha oddeľovať závislosti vyžadované projektami tak, že pre ne vytvára vlastné izolované virtuálne prostredia. Je to jeden z najdôležitejších nástrojov, ktoré používa väčšina vývojárov jazyka Python [27].
Na linuxovej distribúcii Ubuntu sa virtual environment nainštaluje pomocou príkazu

```
$ pip install virtualenv
```

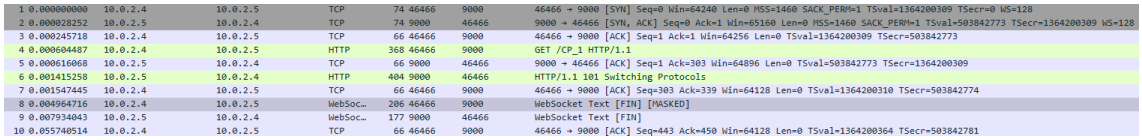
Spustenie je vykonané pomocou príkazu

```
$ source venv/bin/activate
```

3.3.3 Komunikácia - prostredie Wireshark

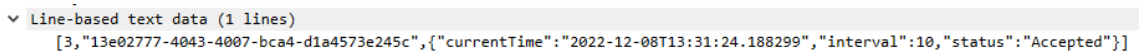
Zachytenú komunikáciu je možné vidieť na obrázku 3.1. Tá prebiehala medzi klientom s IP adresou **10.0.2.4** a serverom s IP adresou **10.0.2.5**. Nadviazanie komunikácie prebehlo pomocou three-way handshake TCP. Nabíjacia stanica sa dotazuje na server. Po nadviazaní spojenia je poslaný Hypertext Transfer Protocol (HTTP) dotaz z nabíjacej stanice, v ktorom je žiadosť na zmenu protokolu z TCP na WebSocket.

Po zmene protokolu je poslaný paket, v ktorom je vidieť BootNotofication poslaný z nabíjacej stanice do centrálneho systému. Táto informácia značí, že sa nabíjacia stanica chystá vykonávať činnosť. Odpoveď riadiaceho systému je aktivácia nabíjacej stanice, tým pádom sa môže začať požadovaná aktivita.



Obr. 3.1: Zachytená komunikácia vo Wiresharku.

Obr. 3.2: Obsah paketu č.8 – BootNotificationRequest.



Obr. 3.3: Obsah paketu č.9 – BootNotificationResponse.

3.4 Skript nabíjacej stanice a centrálneho systému

Najdôležitejšie prvky implementované do skriptov nabíjacej stanice a centrálneho systému boli správy a odpovede zaisťujúce fungovanie nabíjania **TransactionEventRequest** a **TransactionEventResponse** a **StatusNotificationRequest** a **StatusNotificationResponse**. Tieto dve správy sú jedny z najvyužívanejších protokolom OCPP. Tieto správy boli použité v metódach na spustenie a vypnutie nabíjania a spustenie a vypnutie nabíjania, ktoré sú vyžiadané vzdialene. Ďalej boli pridané funkcie, ktoré mali za úlohu sprostredkovať simuláciu nabíjania. Tie boli implementované do skriptu s názvom `emulator.py`. Pomocou tohto skriptu sa spúšťalo a vypínalo nabíjanie skriptu `charge_point.py`.

V blokovej schéme 4.1 predstavuje nabíjacia stanica blok **OCPP CLIENT**, ktorý používa port `65432` a posiela dáta po inicializáci TCP protokolu pomocou websoketov. Centrálny systém predstavuje v blokovej schéme 4.1 **OCPP SERVER** používajúci port `65434`, ktorému prídu dáta tiež pomocou websoketov.

3.4.1 TransactionEventRequest

Táto správa je využívaná v situáciach, kedy nabíjacia stanica informuje server o tom, akú udalosť sa chystá vykonávať a posiela informácie o stave.

TransactionEventRequest obsahuje niekoľko atribútov potrebných k odoslaniu a ich použitie je vyžadované. Prvý atribút je **eventType** využívajúci dátový typ **TransactionEventEnumType**. Tento dátový typ popisuje konkrétny typ vykonávanej udalosti. Prvá správa by mala obsahovať TransactionEvent popisujúci začatie udalosti oznámením `Started` a posledná správa by mala TransactionEvent popisujúci skončenie udalosti oznámením `Ended`. Všetky ostatné by mali obsahovať popis udalostí oznámením `Updated`. Ďalším požadovaným atribútom je **timestamp** využívajúci dátový typ **dateTime**, ktorý poukazuje na dátum a čas výskytu danej transakcie. Atribút **triggerReason** s použitým dátovým typom **TriggerReasonEnumType** uvádza dôvod, za akým učelom nabíjacia stanica posiela konkrétnu správu centrálnemu systému. Ďalším vyžadovaným atribútom je **seqNo**, ktorý má dátový typ **integer** a označuje inkrementáciu sekvenčného čísla pomáhajúce zistiť či boli doručené všetky správy prebiehajúcej transakcie[6].

Posledným vyžadovaným atribútom pre poslanie správy je **trensactionInfo** využívajúci dátový typ **TransactionType**, ktorý obsahuje vnorené atribúty a dátové typy. Využitie atribútu **transactionId** s dátovým typom **identifierString** s počtom charakterov 0 až 36 je vyžadované a popisuje id prebiehajúcej transakcie. Ďalším dôležitým atribútom je **stoppedReason** využívajúci dátový typ **ReasonEnumType** popisujúci dôvod kvôli, ktorému bola transakcia zastavená. Možné dôvody zastavenia transakcie sú napríklad **EmergencyStop** znamenajúci, že k zastaveniu transakcie prišlo použitím núdzového tlačidla stop. Atribút **chragingState** využívajúci dátový typ **ChargingStateEnumType** popisuje, v akom stave je prebiehajúce nabíjanie a je vyžadovaný pokiaľ sa mení stav nabíjania. Definovaný stav nabíjacieho procesu môže byť stav **Charging** uvádzajúci, že prúdi elektrická energia medzi nabíjačkou a elektrickým vozidlom[6].

3.4.2 StatusNotificationRequest

Správa **StatusNotificationRequest** obsahuje atribúty, ktoré sú vyžadované pre jej odoslanie na centrálny systém hovoriace, v akom statuse na práve nachádza nabíjacia stanica. Prvým použitým atribútom je **timestamp** využívajúci dátový typ **dateTime** udávajúci čas, kedy bol daný status reportovaný pre stranu servera. Ďalším atribútom je **connectorStatus** s použitým dátovým typom **ConnectorStatuEnumType**, ktorý popisuje status konektora nabíjacej stanice v danom čase. Typ **ConnectorStatusEnum** má niekoľko stavov ktoré presne určujú status konektora

a z nich sú stavy `Available`, `Reserved` a `Occupied` považované za operatívne. Stavy považované za neoperatívne sú status `Unavailable` a status `Faulted`[6].

Status `Available` predstavuje stav kedy je konektor voľný na použitie novým užívateľom. Status `Reserved` poskytuje informáciu, že daný konektor bol vopred rezervovaný nejakým užívateľom. Stav `Occupied` informuje o tom, že konkrétny konektor je nedostupný pre nového vodiča, ktorý má v pláne nabíjať svoje elektrické vozidlo.

Stav `Faulted` je nastavený, pokiaľ nabíjacia stanica, ktorej patrí konektor, nahlásila chybu a nie je schopná doručovať elektrickú energiu do vozidla [6].

3.4.3 Implementovaná bezpečnosť a autentizácia

V rámci implementácie bezpečnosti bol využitý bezpečnostný profil TLS so základným profilom verifikácie. Tento profil poskytuje tvorbu bezpečnej komunikácie medzi nabíjacou stanicou a centrálnym systémom a tým pádom poskytuje integritu a dôvernosť správ, ktoré sú posielané počas spojenia. V tomto prípade sa nabíjacia stanica overuje pomocou hesla a centrálny systém sa overuje pomocou self–signed certifikátu. Zabezpečená komunikácia bola opätovne zachytená v aplikácii Wireshark, kde bolo možné vidieť, že prenášané aplikačné dáta boli šifrované, tým pádom nečitateľné pri prípadnom napadnutí prenosu a ich následnému zachyteniu. Po rozkliknutí paketu *Server Hello* bolo taktiež možné zistiť, aký bol použitý súbor šifier na zabezpečenie prenosu.

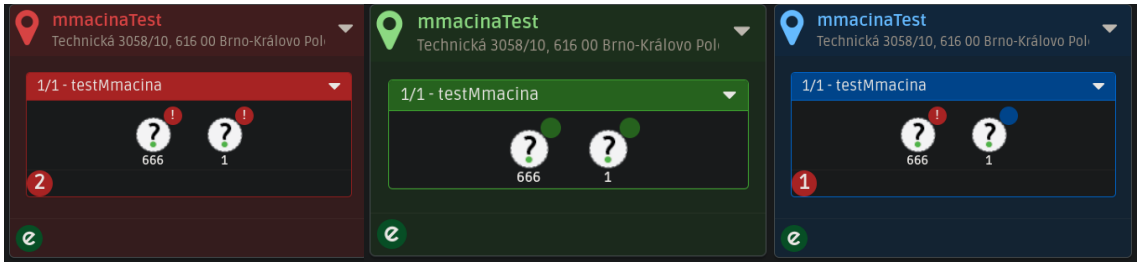
Obr. 3.4: Použitý súbor šifier na zabezpečenie prenosu.

Obr. 3.5: Zašifrované prenášané dáta.

3.5 Pripojenie na server pomocou OCPP 1.6

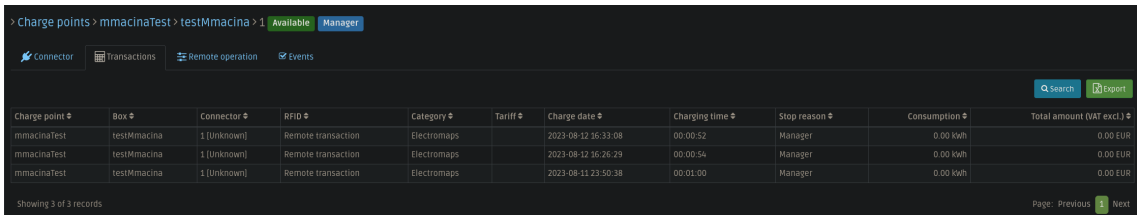
Keďže komerčný server, ktorý mal byť použitý na pripojenie pomocou verzie OCPP 2.0.1 danú verziu nepodporuje, bola vytvorená ukážka pripojenia pomocou verzie OCPP 1.6 na tento server. Zo strany serveru bol poskytnutý manažérsky účet pomocou, ktorého bolo možné vytvárať a manipulovať s nabíjacími stanicami, a zároveň sledovať, čo sa s danou nabíjacou stanicou dialo. To znamená, že je možné sledovať aké správy boli posielané s daným časovým údajom. Taktiež je možné sledovať údaje pre konkrétny konektor. Týmito údajmi môžu byť: dĺžka nabíjania, množstvo kWh, ktoré nabíjacia stanica nabila alebo celková suma za nabíjanie. Všetky tieto údaje sú spojené s dátumom nabíjania.

Na implementáciu bola opäť použitá knižnica OCPP, ktorá je dostupná na stránke GitHub a jej autorom je spoločnosť *The Mobility House* [2]. Do kódu boli doplnené metódy na spustenie a vypnutie nabíjania a taktiež aj metódy na vzdialené spustenie a vypnutie nabíjania. Ďalej bola doplnená metóda posielajúca informácie o zmene dostupnosti nabíjacej stanice. Informácie o dostupnosti nabíjacej stanice je taktiež vidno aj na strane servera. Červenou farbou je nabíjačka označená pokiaľ je vypnutá. Po poslaní **BootNotificationRequest** je označená zelenou farbou. Pokiaľ je v stave nabíjania, tak je označená modrou farbou. Nabíjačku je možné pripojiť na server dvomi spôsobmi a to pomocou **OCPP WebSocket/JSON endpoint** alebo **OCPP SOAP endpoint**. V rámci tejto demonštrácie bol využitý prvý spôsob pripojenia.



Obr. 3.6: Stavy nabíjačky.

[2]Link na použitú knižnicu.



Obr. 3.7: Transkacie vykonané nabíjacou stanicou.

4 Modifikácia knižnice pre prenos pomocou LPWA technológii

Cieľom modifikácie bolo skompletovať meranie simulovanej situácie nabíjania nabíjacej stanice pomocou LPWA technológií, kde bol sledovaný prenos medzi nabíjacou stanicou a serverom na vopred určených LPWA lokalitách a lokalitách, kde by bolo vhodné umiestniť nabíjacie stanice v budúcnosti. V nadväznosti na dané požiadavky bol rozšírený skript nabíjacej stanice a k nim boli pridané ďalšie skripty, ktoré mali túto komunikáciu podporovať kvôli použitému hardvéru. Hardvérový prvok v komunikácii bol modul BG77, pomocou ktorého bolo meranie vykonané.

V pôvodnom pláne mal byť testovaný prenos na reálnom funkčnom serveri od poskytovateľa Electromaps. Práca sa opierala o tento plán dlhú dobu a k tomu prislúchalo aj rozvrhnutie jednotlivých postupov, ktoré sa na koniec nepodarilo dokončiť. Zistilo sa, že s verziou protokolu OCPP 2.0.1 je problém s dostupnosťou implementácie na produkčných serveroch. Tým pádom bolo nutné siahnuť na skript centrálneho systému využitého v semestrálnej práci.

4.1 Pridaný Software a Hardware

Softvér je založený na verejne dostupnej knižnici, ktorá bola spomenutá vo výsledkoch semestrálnej práce. Je dostupná na stránke GitHub a jej autorom je spoločnosť *The Mobility House* [1].

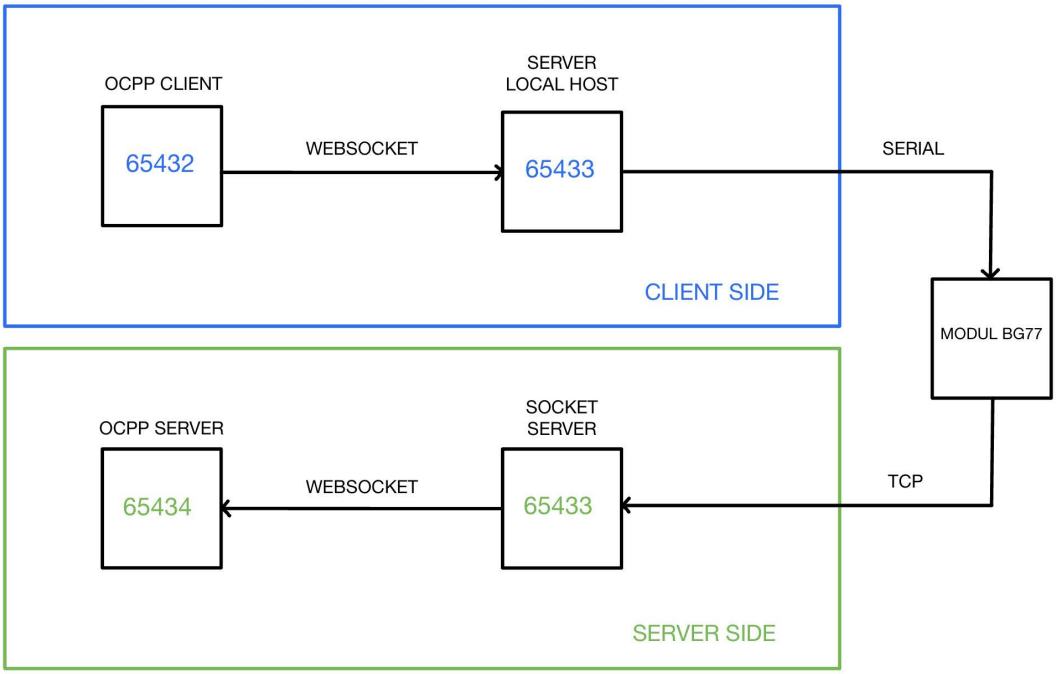
Z knižnice bol upravovaný skript nabíjacej stanice a centrálneho systému. Zvolený postup bol založený na implementácii prvkov, ktoré by boli schopné simulovať jednoduchý proces nabíjania. Ďalej boli doplnené o skript *emulátor*, ktorý toto nabíjanie spúšťal. Po pridaní modulu BG77 bolo nutné zaistiť posielanie dát pomocou modulu na server centrálneho systému. K tomu boli vytvorené dva prostredníky nazvané stredný server pre klienta a stredný server pre centrálny systém. Posledným pridaným prvkom bol skript s názvom *api*, ktorý zaisťuje inicializáciu a operatívne funkcie modulu BG77.

4.1.1 Modul BG77

BG77 je kompaktný USB modul podporujúci LPWA technológie LTE Cat M1 a LTE Cat NB2, ktorý je plne kompatibilný s 3GPP verziou 14. S jeho pomocou bol testovaný spomínaný prenos dát v spomínaných oblastiach, ktoré boli vybrané. Modul

[1] Link na použitú knižnicu.

sa správa ako prostredník medzi stranou nabíjacej stanice odkiaľ prichádzajú požiadavky a centrálnym systémom, ktorý tieto správy spracováva. Flash a RAM pamäte modulu zabezpečujú veľmi nízku náročnosť na spotrebu elektrickej energie. Pokiaľ sa pozrieme na jeho predchodcov, tak procesor využívaný BG77 umožňuje o dosť menšiu spotrebu eDRX prúdu a znižuje únik PSM [28]. Ovládanie modulu, nastavenie parametrov pre prenos, výber použitej technológie, inicializácia a realizácia prenosu je vykonaná pomocou AT príkazov, ktoré spoločnosť Quectel spracoval do dvoch dokumentácii.



Obr. 4.1: Bloková schéma komunikácie.

4.1.2 Pomocný server na strane klienta

Táto implementácia serveru na strane klienta bola pridaná za účelom prepojenia komunikácie tak, aby bolo možné poslať websokety pomocou knižnice `serial` do modulu BG77. Server je v blokovej schéme 4.1 označený ako **SERVER LOCAL HOST** pracujúci na porte `65433`. Dôležitým prvkom klientského servera je skript, ktorý umožňuje spojenie s modulom a zabezpečuje prenos pomocou serial komunikácie prostredníctvom `AT` príkazov ovládajúcimi modul. Pomocou spomínaných príkazov sa modul aktivuje a pripraví na komunikáciu s nasledujúcimi blokmi v schéme. Kľúčovými `AT` príkazmi pri posielaní dát sa stali príkaz `AT+QIOPEN` a `ATO[0]`. Príkaz

`AT+QIOPEN` je využívaný k otvoreniu komunikácie pomocou soketov a nastaveniu jej parametrov. V tomto prípade bol použitý typ prenosu pomocou TCP v móde transparentného prístupu, ktorý sa zapne pomocou príkazu `ATO[0]`. Mód transparentného prístupu umožňuje, že dáta prijaté USB portom budú priamo poslané na internet a dáta prijaté zo strany internetu budú poslané priamo USB portom a zobrazené [29].

4.1.3 Pomocný server na strane centrálneho systému

Server je v blokovej schéme označený ako **SOCKET SERVER**. Úloha tohto servera spočíva v tom, že po jeho spustení sa pripojí na OCPP server a načúva na porte `65433` prichádzajúce dáta odoslané modulom. Následne sú tieto dáta posielané pomocou websoketov do konečnej destinácie OCPP server.

5 Testovanie prenosu pomocou LPWA technológii

Testovanie prebiehalo v okolí budov FEKT VUT (Fakulta elektrotechniky a komunikačných technológií Vysoké učení technické v Brne). Testované zapojenie je možné vidieť na obrázku 4.1. Konkrétne miesta je možné vidieť na obrázku 5.1 a boli to parkovisko pred budovou T12 vrátane jej podzemnej časti, nadzemná garáž pri športovom areáli CESA (Centra športových aktivít), podzemná garáž pod budovou T10 a parkovisko pred budovou T10. Ďalšie testované lokality boli parkovisko neďaleko PPV (pod Palackého vrchem) a parkovisko v lese za fakultou. Otestované parametre boli získané pomocou modulu BG77 s využitím príkazu `AT+QCSQ`. Tento príkaz je používaný k reportu sily signálu využívanej služby. Pokiaľ nie je modulom využívaná žiadna služba, výsledok reportu vráti hodnotu `NO SERVICE`. V tomto scenári bol testovaný mód NB-IoT, ktorý reportuje štyri parametre [29].

RSSI (Received Signal Strength Indicator)

- Parameter intenzity prijatého signálu.
- Meria prijatý výkon na použitom zariadení.
- Taktiež popisuje signál susedných hlavných staníc vrátane vonkajšieho a vnútorného rušenia.
- Jednotky sú udávané v dBm (decibel miliwatoch)[30].

RSRP (Reference Signal Received Power)

- Prijatý výkon referenčného signálu signálu.
- Meria prijatý výkon na použitom zariadení.
- Popisuje odhad výkonu na základe riadiacich signálov, ktoré prichádzajú z aktuálnej hlavnej stanice.
- Hodnota RSRP má vzhľadom na rušenie menšiu numerickú hodnotu než RSSI.
- Jednotky sú udávané v dBm (decibel miliwatoch).

SINR (Signal to Interference plus Noise Ratio)

- Popisuje rušenie signálu a zároveň pomer šumu je vypočítaný ako pomer požadovaného signálu a vonkajšieho rušenia.
- Jednotky sú udávané v dB (decibeloch).

RSRQ (Reference Signal Received Quality)

- Parameter kvality prijímaného referenčného signálu

- Popisuje kvalitu prijímaných pilotných signálov z aktuálnej hlavnej stanice.
- Jednotky RSRPQ sú udávané v dB (decibeloch)[30].

Popis rozsahu hodnôt RSRP:

- viac ako −80 dBm - veľmi dobrá sila signálu s maximálnou rýchlosťou prenosu,
- rozmedzie od −80 dBm do −100 dBm – dobrá sila signálu s dobrou prenosovou rýchlosťou,
- rozmedzie od −100 dBm do −125 dBm – slabá intenzita signálu s častým poklesom prenosovej rýchlosti,
- menej ako −125 dBm – veľmi nízka intenzita signálu spôsobujúca stratu pripojenia.

Popis rozsahu hodnôt SINR:

- viac ako 20 dB – veľmi dobrá sila signálu s maximálnou rýchlosťou prenosu,
- rozmedzie od 13 dB do 20 dB – dobrá sila signálu s dobrou prenosovou rýchlosťou,
- rozmedzie od 0 dB do 12 dB – slabá intenzita signálu s častým poklesom prenosovej rýchlosti,
- menej ako 0 dB – veľmi nízka intenzita signálu spôsobujúca stratu pripojenia [30].

5.1 Priebeh testovania

Samotný priebeh testovania spočíval v tom, že najprv bola spustená serverová časť zapojenia označená v blokovej schéme 4.1 zelenou farbou. Prvý krok bol pripojenie na server s využitím protokolu SSH (Secure Shell). Následne boli v termináli spustené python skripty pomocou príkazov `$ python3 central_system.py`, ktorý spustí OCPP server a `$ python3 mws.py` spúšťajúci socket server. Po spustení socket servera je v konzoli OCPP serveru vidieť, že je socket server pripojený na OCPP server. Druhý krok spočíval v spustení klientskej časti zapojenia, ktorá je v blokovej schéme 4.1 vyznačená modrou farbou. Spustenie servera local host je vykonané pomocou príkazu `$ python3 mwc.py`. Po jeho spustení a inicializácii je v konzoli socket serveru vidieť, že je server local host pripojený na socket server. Posledný krok spočíva v spustení nabíjacej stanice, ktorá sa spustí pomocou príkazu `$ python3 charge_point.py`, čo znamenalo vykonanie komunikácie. Testovací scenár vyzeral nasledovne. Po zapnutí komunikácie nabíjačke oznámi serveru, že je schopná nabíjania. Po dobe 5s bolo spustené nabíjanie. Po uplynutí ďalších 20s bolo nabíjanie odpojené a nasledovalo ukončenie komunikácie.

5.1.1 Popis zaznamenaných hodnôt

Merané parametre boli zachytávané pomocou technológie NB–IoT a princíp získavania hodnôt spočíval v tom, že po výmene správy a odpovede medzi nabíjacou stanicou a centrálnym systémom bol do modulu poslaný príkaz `AT+QCSQ`, ktorým boli získané požadované hodnoty merania. S ohľadom na časté opakovanie príkazu boli pozorované minimálne odchýlky a do tabuľky 5.1 boli vybrané stredné hodnoty nameraných parametrov.

Tab. 5.1: Namerané hodnoty pomocou technológie NB–IoT

Lokalita	**RSSI [dBm]**	**RSRP [dBm]**	**SINR [dB]**	**RSRQ [dB]**
Podzemie 1 – T10	−48	−49	14	−11
Podzemie 2 – T10	−88	−99	12	−11
Podzemie 3 – T10	−92	−98	11	−10
Podzemie 1 – T12	−46	−56	19	−10
Podzemie 2 – T12	−58	−63	10	−11
Parkovisko 1 – CESA	−62	−65	20	−10
Parkovisko 2 – CESA	−57	−69	5	−12
Parkovisko 3 – CESA	−56	−68	5	−12
Parkovisko T10	−44	−56	13	−10
Parkovisko T12	−36	−44	12	−11
Parkovisko PPV	−42	−53	21	−10
Parkovisko les	−65	−75	13	−11

5.1.2 Výsledky merania

Výsledky merania sú priemerom šiestich prijatých hodnôt získaných po poslaní príkazu `AT+QCSQ` počas prenosu v rámci jednej lokality. Hodnoty sú spriemerované, pretože boli minimálne rozdielne. Prvou nameranou lokalitou bola podzemná garáž v budove T10. Meranie začalo na poslednom poschodí podzemnej garáže, kedy nastala komplikácia, že nebolo možné spustiť komunikáciu kvôli slabej intenzite signálu. Z toho dôvodu bol zvolený presun do tretieho poschodia, kde bolo možné komunikáciu úspešne spustiť. Získaná hodnota RSSI predstavovala −92 dBm čo značí slabú intenzitu signálu. Hodnota RSRP bola −98 dBm predstavujúca výkon na základe pilotných signálov z aktuálnej hlavnej stanice, ktorá značí slabú intenzitu znamenajúcu pokles prenosovej rýchlosti. Hodnota SINR udávala 11 dB čo znamená slabú intenzitu signálu a pokles rýchlosti prenosu dát. Táto hodnota predstavuje výpočet pomeru medzi požadovaným signálom a rušením z vonkajších zdrojov. Nameranou hodnotou RSRQ bolo −11 dB označujúca kvalitu prijímaných

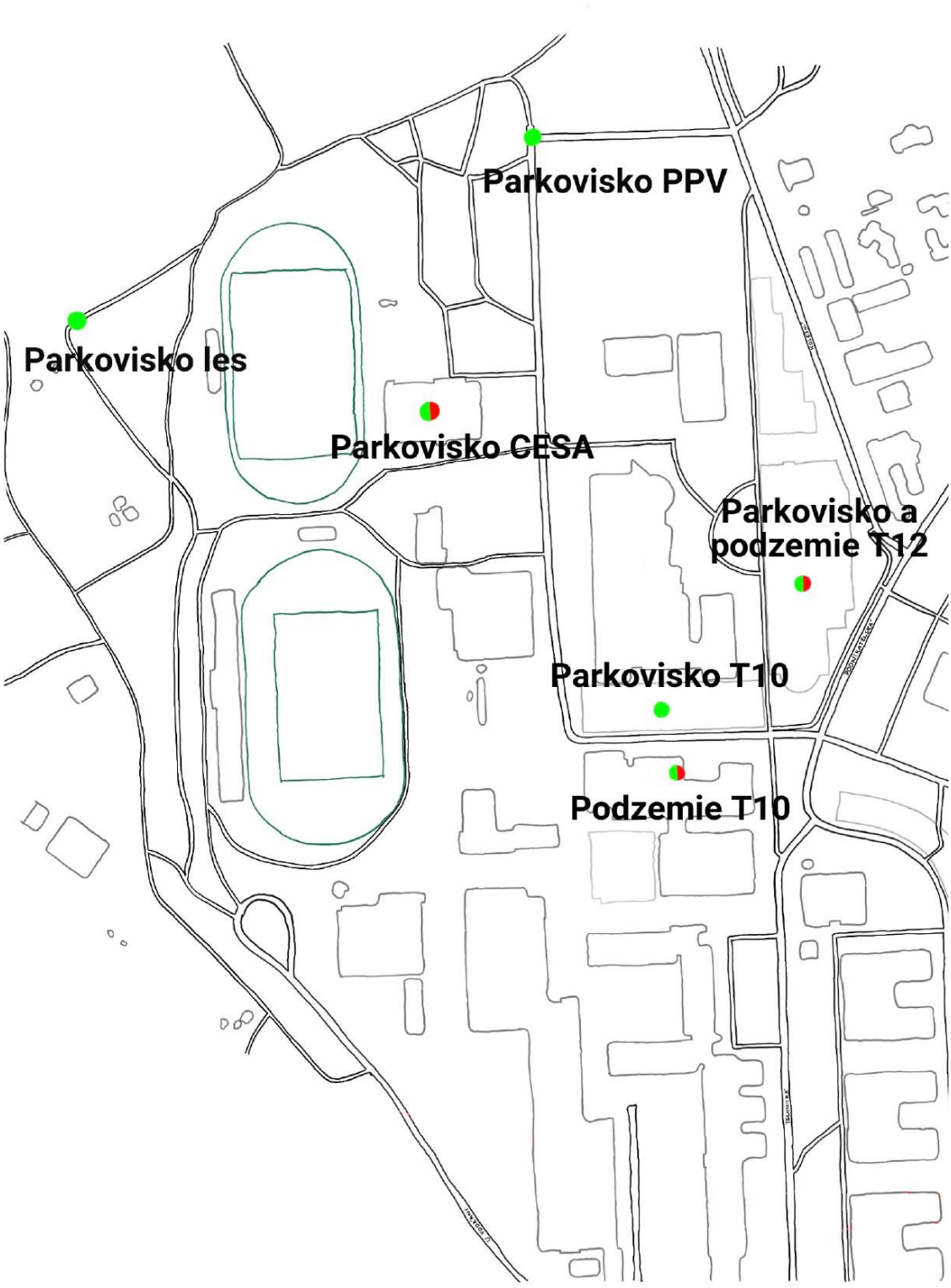
riadiacich signálov z aktuálnej hlavnej stanice. Táto hodnota vraví o silnom signále a optimálnej prenosovej rýchlosti. Následne sa meranie presunulo na poschodie dva a poschodie jedna. Hodnota SINR na druhom poschodí bola 12 dB, čo nepredstavuje zmenu pre intenzitu signálu a rýchlosť prenosu dát. Avšak hodnota SINR na prvom poschodí predstavovala 12 dB, čo znamená dobrú intenzitu signálu a dobrú prenosovú rýchlosť dát.

Druhá meraná lokalita bolo parkovisku T10 bolo, kde bola nameraná odlišná hodnota RSSI predstavujúca -44 dBm značiaca silnú intenzitu signálu. Zmena bola tiež viditeľná pri hodnote RSRP predstavujúca silnú intenzitu -56 dBm. Hodnota SINR 13 dB znamenala dobrú silu signálu a optimálnu prenosovú rýchlosť dát.

Treťou meranou lokalitou bol parkovací komplex pred budovou T12. Namerané hodnoty pod zemou boli s jemnými odchýlkami rovnaké v podzemnej garáži T10 s výnimkou parametru SINR, ktorý udával hodnotu 12 dB, čo znamená slabú intenzitu signálu a pokles prenosovej rýchlosti.

Štvrtou meranou lokalitou bolo poschodové parkovisko pri budovách CESA. V rámci meraných hodnôt sa výrazne menil parameter SINR, kde na prvom poschodí mal hodnotu 20 dB a na druhom a treťom hodnotu 5 dB. Z toho je možno usúdiť, že na prvom poschodí bola intenzita signálu veľmi dobrá s maximálnou prenosovou rýchlosťou. Na druhom a treťom poschodí predstavovala hodnota 5 dB slabú intenzitu s poklesom prenosovej rýchlosti. Na parkovisku PPV nachádzajúce sa neďaleko poschodovej garáže bola nameraná hodnota SINR 21 dB znamenajúca veľmi dobrú intenzitu signálu, pri ktorej je dosiahnutá maximálna rýchlosť prenosu dát. Posledná meraná lokalita sa nachádzala za športovým areálom CESA, kde nameraná hodnota SINR predstavovala dobrú silu signálu s dobrou prenosovou rýchlosťou.

Miesta s dobrou kvalitou signálu sú vyznačené na obrázku 5.1 zelenou farbou a miesta so zlou kvalitou signálu sú zobrazené na obrázku 5.1 červenou farbou.



Obr. 5.1: Mapa lokalít merania.

Závěr

Cieľom bakalárskej práce bol detailný popis protokolu OCPP a popis technológií LPWA (LowPower Wide–Area). V rámci popisu OCPP bol kladený dôraz na popis bezpečnosti tohto protokolu a pri LPWA bol kladený dôraz na popis technológií licenčného pásma.

V praktickej časti bola knižnica OCPP implementovaná v jazyku Python do štádia kedy bolo možné spustiť simulovanú komunikáciu medzi nabíjacou stanicou a centrálnym systémom. Zabezpečenie tejto komunikácie prebehlo pomocou protokolu TLS, pretože je špecifikovaný štandardom OCPP a je vhodný na šifrovanie prenosu aj na autetizáciu protistrán. Demonštrácia mala pôvodne prebiehať na serveri, ktorý je v bežnej produkcii, čo sa nakoniec nepodarilo. Problém sa týkal konkrétne verzie protokolu 2.0.1. Zistilo sa, že server, ktorý bol súčasťou pôvodného plánu má implementovanú iba verziu 1.6. Pokus o nájdenie iného servera zlyhal, takže bol vytvorený záložný plán.

Záložným plánom bola implementácia vlastného jednoduchého servera schopného odpovedať na správy nabíjacej stanice, ktorá prebehla. Spôsob implementácie bol založený na funkčnosti nabíjacej stanice, kde server dostal implementáciu odpovedí na požiadavky nabíjacej stanice. Následne bola overená funkcionalita voči vytvorenému serveru pre verziu OCPP 2.0.1 a taktiež aj overenie funkcionality verzie OCPP 1.6 na komerčnom serveri, kvôli vyššie spomenutému problému s podporou verzie OCPP 2.0.1.

Ďalším krokom bolo upraviť implementáciu, aby bolo možné viesť komunikáciu pomocou modulu BG77 a dokončiť meranie pomocou LPWA technologií. Úprava prebehla pomocou implementácie pomocného servera na strane OCPP klienta a pomocného servera na strane OCPP servera, ktorých úlohou bolo konvertovať komunikáciu z websoketov na TCP tunel a naspäť pomocou serial modulu. Ďalším krokom bolo skompletovanie merania na vybraných lokalitách v okolí fakulty FEKT VUT. Zoznam spomínaných lokalít je možné vidieť na mape na obrázku 5.1. Z nameraných hodnôt je vidno, že na parkoviskách v lese, na T10 a na PPV nebol problém s prenosom. Na daných lokalitách boli dobré hodnoty SINR a RSRP. Podzemné parkoviská mali ideálne hodnoty signálov prevažne vo vrchných poschodiach, hlavne v prvom, zatiaľ čo spodné poschodia ukazovali stratu signálu. Na najnižších poschodiach nebolo možné otestovať prenos, kvôli minimálnej až žiadnej intenzite signálu. Nadzemné parkovisko dosiahlo tiež postačujúce výsledky, kde sa ukázal pokles intenzity signálu na druhom a treťom poschodí.

Čo sa týka prenosu protokolu OCPP je vidieť jednoznačný potenciál vo využití LPWA technológii a v budúcnosti by to mohlo znamenať krok vpred v nabíjaní elektromobilov.

Literatúra

[1] Cristina Alcaraz, Javier Lopez, and Stephen Wolthusen. Ocpp protocol: Security threats and challenges. *IEEE Transactions on Smart Grid*, 8(5):2452–2459, 2017.

[2] Dawn Kitai. Understanding OCPP and its significance to ev charging • evreporter, Sep 2020. URL: `https://evreporter.com/ocpp-and-ev-charging/`.

[3] Open Charge Alliance. *OCPP 2.0.1 Part 1 - Architecture & Topology*, March 2020. URL: `https://www.openchargealliance.org/protocols/ocpp-201/`.

[4] Open Charge Alliance. *OCPP 1.6 edition 2 - Specification*, September 2017. URL: `https://www.openchargealliance.org/protocols/ocpp-16/`.

[5] Thota Venkata Pruthvi, Niladri Dutta, Phaneendra Babu Bobba, and B Sai Vasudeva. Implementation of ocpp protocol for electric vehicle applications. In *E3S Web of Conferences*, volume 87, page 01008. EDP Sciences, 2019.

[6] Open Charge Alliance. *OCPP 2.0.1 Part 2 - Specification*, March 2020. URL: `https://www.openchargealliance.org/protocols/ocpp-201/`.

[7] Open Charge Alliance. *OCPP 2.0.1 Part 0 - Introduction*, March 2020. URL: `https://www.openchargealliance.org/protocols/ocpp-201/`.

[8] Tim Dierks and Eric Rescorla. The transport layer security (tls) protocol version 1.2. Technical report, 2008.

[9] Ivan Ristic. *Bulletproof SSL and TLS: Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications*. Feisty Duck, 2013.

[10] An overview of the ssl/tls handshake, November 2022. URL: `https://www.ibm.com/docs/en/ibm-mq/9.1?topic=tls-overview-ssltls-handshake`.

[11] David Cooper, Stefan Santesson, Stephen Farrell, Sharon Boeyen, Russell Housley, and William Polk. Internet x. 509 public key infrastructure certificate and certificate revocation list (crl) profile. Technical report, 2008.

[12] Usman Raza, Parag Kulkarni, and Mahesh Sooriyabandara. Low power wide area networks: An overview. *IEEE Communications Surveys Tutorials*, 19(2):855–873, 2017. URL: `https://ieeexplore.ieee.org/document/7815384`.

[13] Sjoerd Van Leeuwen. Licensed lpwan market now bigger than the unlicensed lpwan market., Aug 2022. URL: https://thingsdata.com/informatie/licensed-lpwan-market-now-bigger-than-the-unlicensed-lpwan-market/.

[14] 1NCE. Licensed vs. unlicensed radio technology, Jul 2020. URL: https://1nce.com/en/blog/licensed-vs-unlicensed-radio-technology/.

[15] Ashish Kumar Sultania, Pouria Zand, Chris Blondia, and Jeroen Famaey. Energy modeling and evaluation of nb-iot with psm and edrx. In *2018 IEEE Globecom Workshops (GC Wkshps)*, pages 1–7. IEEE, 2018.

[16] Linda Rosencrance. What is narrowband iot (nb-iot)?, Apr 2020. URL: https://www.techtarget.com/whatis/definition/narrowband-IoT-NB-IoT.

[17] Ansuman Adhikary, Xingqin Lin, and Y.-P. Eric Wang. Performance evaluation of NB-IoT Coverage. In *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*, pages 1–5, 2016. doi:10.1109/VTCFall.2016.7881160.

[18] Franck Muteba, Karim Djouani, and Thomas Olwal. A comparative survey study on lpwa iot technologies: Design, considerations, challenges and solutions. *Procedia Computer Science*, 155:636–641, 2019.

[19] Rapeepat Ratasuk, Benny Vejlgaard, Nitin Mangalvedhe, and Amitava Ghosh. NB-IoT system for M2M communication. In *2016 IEEE Wireless Communications and Networking Conference*, pages 1–5, 2016. URL: https://ieeexplore.ieee.org/abstract/document/7564708?casa_token=x-lIrn5F6JYAAAAA:I-4TPkEuBhl-4lXKKUeHMgGAyRbPgX9b2LPKTKxDOAMt8wEkJFradyo-dcSil1F\protect\discretionary{\char\hyphenchar\font}{}{}iojvMwUECWw.

[20] IOTCREATORS. NB-IoT Network Information. URL: https://docs.iotcreators.com/docs/nb-iot-network-information.

[21] Jacques Palicot Marwa Chafii, Faouzi Bader. *Enhancing Coverage in Narrow Band-IoT Using Machine Learning*, April 2018. URL: https://hal.archives-ouvertes.fr/hal-01705715/document.

[22] Amazon Web Services. Implementing Low-Power Wide-Area Network LPWAN Solution with AWS IoT:AWS Whitepaper. URL: https://docs.aws.amazon.com/whitepapers/latest/implementing-lpwan-solutions-with-aws/lte-m.html.

[23] GSMA. Long term evolution for machines: LTE-M, May 2022. URL: https://www.gsma.com/iot/long-term-evolution-machine-type-communication-lte-mtc-cat-m1/.

[24] GSM Association et al. LTE-M deployment guide to basic feature set requirements, 2018.

[25] Ian Fette and Alexey Melnikov. The websocket protocol. Technical report, 2011. URL: https://www.rfc-editor.org/rfc/rfc6455.html#.

[26] PyPI. Websockets. URL: https://pypi.org/project/websockets/.

[27] Real Python. Python Virtual Environments: A primer, Nov 2022. URL: https://realpython.com/python-virtual-environments-a-primer/#what-is-a-python-virtual-environment.

[28] Quectel Wireless Solutions Co. LPWA BG77 Cat M1/NB2, May 2023. URL: https://www.quectel.com/product/lte-bg77-cat-m1-nb2.

[29] Quectel Wireless Solutions Co. AT Commands Manual, 2019. URL: https://auroraevernet.ru/upload/iblock/374/3741d2f676995196d4a36527c5d75e07.pdf.

[30] Vadims Kalejs. What is RSSI, SINR, RSRP, RSRQ?, Feb 2022. URL: https://www.rangeful.com/what-is-rssi-sinr-rsrp-rsrq-how-does-this-affect-signal-quality/.

Zoznam symbolov a skratiek

3GPP	Third Generation Partnership Project
ACK	Acknowledge
CA	Certifikačná Autorita
CE	Coverage Enhancemen
CESA	Centra športových aktivít
CSMS	Charging Station Management System
CSOs	Charging Station Operators
ČTÚ	Český telekomunikačný úrad
dB	decibel
dBm	decibel milliWatt
ECL	Extended Coverage Leve
eDRX	Extended Discontinuous Reception
EV	Electric Vehicle
EVSE	Electric Supply Equipment
FEKT	Fakulta elektrotechniky a komunikačních technologií
HTTP	Hypertext Transfer Protocol
IoT	Internet of Tings
IP	Internet Protocol
JSON	JavaScript Object Notation
LaQuSo	Laboratory for Quality Software
LoRa	Long Range Wide
LPWA	Low–power Wide Area
LTE	Long Term Evolution
LTE–M	Long Term Evolution for Machines

MAC	Message Authentication Code
MCL	Maximum Coupling Loss
MIMO	Multiple-input multiple-output
MPDCCH	MTC Physical Downlink Control Channel
NB–IoT	Narrowband IoT
OCA	Open Charge Aliance
OCPP	Open Charge Point Protcol
OCSP	Online Certificate Status Protocol
PDU	Protocol Data Units
PEM	Privacy Enhanced Mai
PPV	pod Palackého vrchem
PRB	Physical Resource Block
PSM	Power Saving Mode
RSRP	Reference Signal Received Powe
RSRQ	Reference Signal Received Quality
RSSI	Received Signal Strength Indicator
SEEC	State Elections Enforcement Commission
SINR	Signal to Interference plus Noise Ratio
SOAP	Simple Object Access Protocol
SSH	Secure Shel
SYN–ACK	Synchronize–Acknowledge
SYN	Synchronize
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol

VPN Virtual Private Network

VUT Vysoké učení technické v Brně

XML Extensible Markup Language

A Elektronické prílohy

- `/` ..... domovský priečinok
  - `codes` ..... priečinok obsahujúci kódy
    - `ocppv201` ..... priečinok obsahujúci kódy verzie 2.0.1
      - `ocpp-client` ..... priečinok kódu klienta
        - `charge_point.py` ..... python skript nabíjacej stanice
        - `emulator.py` ..... python skript simulácie
      - `ocpp-server` ..... priečinok kódu servera
        - `central_system.py` ..... python skript centrálneho systému
      - `middle_servers` ..... priečinok obsahujúci pomocné servery
        - `mwc.py` ..... python skript pomocného serveru OCPP klienta
        - `mws.py` ..... python skript pomocného serveru OCPP servera
    - `ocppv16` ..... priečinok obsahujúci kód verzie 1.6
      - `charge_point.py` ..... python skript nabíjacej stanice
    - `wireshark` ..... priečinok wireshark
      - `ocpp_com.pcapng` ..... zachytená komunikácia vo wiresharku
      - `ocpp_secured.pcapng` .... zachytená šifrovaná komunikácia vo wiresharku