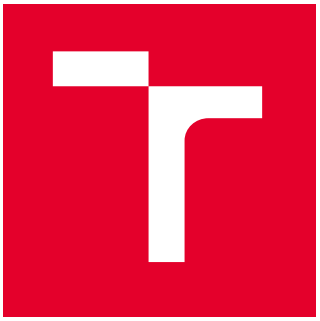


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

ÚSPORNÉ ZABEZPEČOVACÍ ZAŘÍZENÍ LORAWAN

ECONOMICAL LORAWAN SECURITY DEVICE

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Oliver Varhola**
AUTHOR

VEDOUCÍ PRÁCE — **doc. Ing. Vladislav Škorpil, CSc.**
SUPERVISOR

BRNO 2024

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

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

Ústav telekomunikací

Student: Bc. Oliver Varhola ***ID:*** 186731

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

NÁZEV TÉMATU:

Úsporné zabezpečovací zařízení LoRaWAN

POKYNY PRO VYPRACOVÁNÍ:

Navrhněte koncepci jednoduchého detektoru otevření dveří/oken/prostoru pomocí magnetického kontaktu a LoRaWAN modulu. Detektor bude napájen bateriově a připojen do sítě The Things Network, nebo jiné vhodné LoRaWAN sítě, např. Helium. Pomocí MQTT bude komunikovat s vlastním řešením postaveným na MQTT brokeru, NodeRed, InfluxDB a OpenHAB frameworku. Systém emailem upozorní na narušení prostoru a zápisem události do vhodné cloudové služby provede záznam o narušení prostoru pro případné podrobné zpětné prohlížení. Důraz při návrhu je přenositelnost zařízení a dlouhá provozní doba.

DOPORUČENÁ LITERATURA:

Podle pokynů vedoucího práce.

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

Vedoucí práce: doc. Ing. Vladislav Škorpil, CSc.
Konzultant: Ing. Ondřej Pavelka

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

ABSTRAKT

Diplomová práca obsahuje návrh riešenia ekonomicky a energeticky úsporného zabezpečovacieho zariadenia s komunikačnou časťou v sieti LoRaWAN. Teoretická časť práce popisuje najrozšírenejšie LPWAN siete, t.j. siete pre zariadenia s nízkym výkonom akými sú NB-IOT na báze technológie LTE, Sigfox a LoRaWAN. Takisto stručne analyzuje bezpečnostné hrozby v prípade útoku na komunikačný kanál a to najmä zarušením kanála a podrobne opisuje zabezpečenie siete LoRaWAN. V praktickej časti je realizované kompletné riešenie od hardvéru, napájania, mechanického riešenia vrátane krytu zariadenia. Návrh softvéru, zahŕňa obsluhu požadovaných udalosti. Boli realizované nevyhnutné požiadavky na úsporu energie a interval odosielania správ. Z hľadiska riešenia aplikačnej vrstvy sú využité komponenty systému - LoRaWAN sieťový server a aplikácie bežiace na virtuálnom stroji: MQTT broker, NodeRED, OpenHAB a cloudovú databázu InfluxDB s vizualizáciiou dát v aplikácii Grafana.

KĽÚČOVÉ SLOVÁ

LoRaWAN, úsporné, ekonomické, zabezpečovacie, zariadenie, virtuálny privátny stroj, cloudové aplikácie

ABSTRACT

This master thesis contains a proposal of the solution for economical and energy saving security device with its communications part in a LoRaWAN network. Theoretical part of the thesis describes the most widespread LPWAN networks, i.e. the networks for low-power devices, such as NB-IOT based on LTE technology, Sigfox and LoRaWAN. Also briefly analyses security threats in case of the interference exploitation of the communication channel and describes LoRaWan security in detail. In the practical part there is hardware, power, mechanical solution implemented including the cover of the device. Realization of the software part covers, which types of events should be operated, power saving methods and mesage sending inverval are described. All requirements were implemented at application layer utilizing - LoRaWAN network server and virtual machine applications: MQTT broker, NoreRED, OpenHAB and cloud database InfluxDB with visualisation of the data in Grafana application.

KEYWORDS

LoRaWAN, low-power, economical, security, device, virtual private server, cloud applications

Vysadené pomocou balíčku `thesis` verzie 4.09; `https://latex.fekt.vut.cz/`

VARHOLA, Oliver. *Úsporné zabezpečovací zařízení LoRaWAN*. Diplomová práca. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2024. Vedúci práce: doc. Ing. Vladislav Škorpil, CSc.

Vyhlásenie autora o pôvodnosti diela

Meno a priezvisko autora:	Bc. Oliver Varhola
VUT ID autora:	186731
Typ práce:	Diplomová práca
Akademický rok:	2023/24
Téma závěrečnej práce:	Úsporné zabezpečovací zařízení LoRaWAN

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 konzultantovi Ing. Ondřejovi Pavelkovi za odborné vedenie a podnetné návrhy a vedúcemu diplomovej práce pánu Doc. Ing. Vladislavovi Škorpilovi, CSc. za odborné vedenie, trpezlivosť a usmernenie k práci.

Obsah

Zoznam obrázkov

Úvod

S rozvojom internetu sa od 90-tych rokov minulého storočia spájala najmä dominancia komunikácie *human-to-machine* (H2M), ktorú formovali služby World-wide web, e-maily, webové vyhľadávače a podobne. V úvode milénia sa takmer paralelne s fenoménom sociálnych sietí začali objavovať aj nové siete a protokoly pre komunikáciu *machine-to-machine* (M2M). Miniaturizácia výpočtových jednotiek a pokrok v oblasti rádiového prenosu dát nás priviedli k všeobecne známemu slovnému spojeniu *internet vecí - Internet of Things (IOT)*. Ako sa postupne dostávame k zovšeobecňujúcemu *Internetu všetkého - Internet of Everything (IoE)* stávajú sa aj technológie pre komunikáciu a senzory čoraz viac bežnými až do takej miery, že ich považujeme za súčasť každodenného života. Technológia sa pre nás stáva transparentnou, zjednodušuje nám každodenné aktivity, pomáha nám predvídať a chráni naše najvyššie hodnoty - zdravie, život či majetok.

LoRaWAN je jednou z komunikačných technológií pre prenos dát na veľké vzdialenosti, zároveň však s nízkou energetickou náročnosťou. Táto technológia umožňuje prenos s nízkou šírkou prenosového pásma a zároveň úsporu energie, s čím súvisí aj účinnosť prenosu. LoRaWAN patrí do skupiny technológií LPWAN, ktoré sa vyznačujú nízkymi nárokmi na napájanie, pomerne veľkým dosahom a menšou šírkou pásma než existujúce mobilné siete. V súťaži o čo najúspornejšie riešenie zabezpečovacieho zariadenia je po ekonomickej, či energetickej stránke na výber viacero LPWAN technológií, ktoré uvádzam a rozoberám v prvej kapitole. Zdôvodnenie výberu LoRaWAN je v prvej časti druhej kapitoly, ktorá sa tiež venuje analýze možností pre výber hardvérovej platformy. Tretia kapitola obsahuje praktický popis riešenia hardvérovej časti ako aj technické prevedenie jednotlivých komponentov. Štvrtá kapitola je venovaná softvérovému riešeniu a nastaveniu komponentov pre komunikáciu.

Ciele práce

Hlavným cieľom práce je návrh koncepcie jednoduchého detektora otvorenia okien a dverí pomocou magnetického kontaktu a LoRaWAN modulu. Detektor má byť napájaný batériovo a pripojený do siete The Things Network. Úsporné zabezpečovacie zariadenie LoRaWAN slúži ako bezpečnostné zariadenie pre kontrolu a ochranu odlúčených objektov, ktoré sú v dosahu LoRaWAN sietí, ale nemajú možnosť pripojenia k elektrickej alebo dátovej sieti. Dôraz pri návrhu je prenositeľnosť zariadenia a dlhá prevádzková doba.

Prednostne má byť použitý Heltec modul s STM32L151, alebo s ASR605x ARM

- https://heltec.org/project/lora-node-151/ alebo https://heltec.org/project/lora-kit-151/
- https://heltec.org/project/htcc-ab02a/ alebo https://heltec.org/project/htcc-ab01-v2/

Zabezpečovacie zariadenie umožňuje pripojiť externe:

- Mechanický/magnetický spínací kontakt
- Mechanický/magnetický rozpínací kontakt

V prípade aktivity (zmeny stavu) senzoru odosiela zariadenie telemetrické dáta + informácie o poplachu = aktivity (či došlo k spojeniu alebo rozpojeniu) Zabezpečovacie zariadenie periodicky posiela s periódou 1 hodiny telemetrické dáta obsahujúce:

- Napätie batérie
- Teplotu
- Silu signálu pri príjme z predchádzajúcej správy a stavy čidiel (pripojené/nepripojené/aktívne/neaktívne)
- Napájanie zabezpečovacieho zariadenia bude pomocou LiION (LiPol) batérie s menovitým napätím 3.6VDC (ideálne rozmer 18650 – jednoduchá výmena vybitého za nabitý článok).
- Systémový teplotný senzor bude umiestnený priamo vo vnútri krabičky, nemožno ho odpojiť.
- Senzor bude pripojený do siete TTN LoRaWAN (alebo inej - napr. Helium)
- Dáta sú z tejto siete preposielané pomocou MQTT protokolu do MQTT brokera umiestneného na VPS (Virtual Private Server), spolu s ďalšími komponentmi.
- Prijaté dáta MQTT brokerom sú pomocou Node-Red jednak uložené do InfluxDB 3.0 databázy. Ďalej sú tieto dáta zobrazované ako užívateľské grafy pomocou programu Grafana a OpenHAB umiestnených na VPS. Systémy Grafana aj OpenHAB umožňujú zobraziť jednak verejné dáta – teplotu a vlhkosť, po zadaní hesla aj ďalšie dáta – stav batérie, stav čidiel, aktivácia/deaktivácia jednotlivých senzorových vstupov

- Užívateľ je pomocou správ (email, telegram, whatsapp, messenger, pushbullet a iné) informovaný o aktivácii čidiel, tu alarmového stavu. Tieto kanály je možné nastaviť napr. v OpenHAB systéme – tlf. čísla, príp. emaily.
- Užívateľ je upozornený špeciálnou správou na kritický stav napätia batérie, teda požiadavkou na dobitie alebo výmenu.

1 Technológie LPWAN

LPWAN označuje kategóriu bezdrôtových komunikačných technológií, vyvinutých na podporu pripojenia zariadení do siete IoT. Technológie LPWAN majú zaistiť najmä: pokrytie veľkých oblastí i v situáciách, keď sa zariadenie nachádza pod zemou alebo hlboko v budovách; veľmi nízku spotrebu elektrickej energie; masívne nasadenie aj miliónov zariadení, lacný telekomunikačný hardware a nenáročný prenos dát.

1.1 Narrowband IOT (NB-IOT)

Narrowband IOT - je úzkopásmový systém. Ide o nízkorozpočtové a nízkoenergetické širokopásmové mobilné pripojenie pre internet vecí. Systém je založený na technológii LTE (Long Term Evolution) a podporuje väčšinu funkcií LTE avšak s podstatnými zjednodušeniami za účelom zmenšenia konštrukčnej zložitosti zariadenia. Zavedením potrebných opatrení sa dosahuje zníženie režijných nákladov, zníženie spotreby energie a zvýšenie kapacity. Medzi dizajnové ciele systému NB-IoT patria zariadenia vyznačujúce sa zjednodušením konštrukcie, zlepšením pokrytia, dlhšej životnosti batérie a dostatočná kapacita informačného kanála. Latencia nie je prioritou a povolené oneskorenie je tolerované až do 10 sekúnd.

1.1.1 Parametre NB-IOT

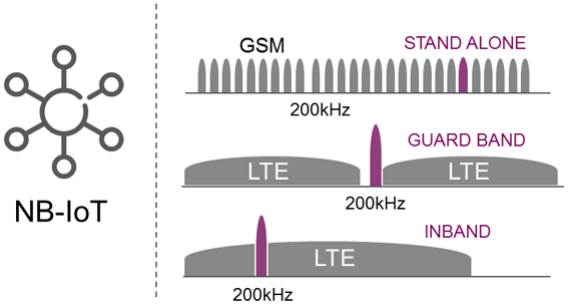
NB-IOT pracuje vo všetkých frekvenčných pásmach určených pre LTE. Ide o licencované spektrum. Šírka kanála je 180kHz, teda jeden základný fyzický blok LTE - Physical Resource Block (PRB). Pre aplikáciu sa v praxi používajú tri spôsoby - Obrázok 1.1.1:

1. Samostatné - využíva 200kHz kanály nevyužívaného GSM pásma
2. Bloky ochranného pásma - využívajúc "medzeru"medzi dvoma susednými kanálmi LTE
3. "V pásme"tzv. in-band - rezervácia jedného fyzického bloku LTE v prípade ak je šírka kanála viac ako 1,4MHz

Kvôli koexistencii s LTE aj frekvenčné bloky vyhradené pre *Uplink* (UL) a *Downlink* DL sú rozdelené na sub-nosné po 15kHz. $12 \times 15 = 180kHz$. Časová os je rozdelená do time-slotov, z ktorých každý trvá 0.5ms a pozostáva zo 7 symbolov OFDM/SC-FDMA.

Hlavné vlastnosti NB-IoT:

- Potrebná šírka pásma: 180 kHz



Obr. 1.1: Možnosti aplikácie NB-IOT v rámci frekvencií pre LTE[1]

- Download (max): 250 kbit/s
- Upload (max): 250 kbit/s (multi-tone) /20 kbit/s (single-tone)
- Latencia: 1.6s–10s
- Duplex: half duplex
- Vysielací výkon: 23/27 dBm (UL/DL)
- Citlivosť: -141/-138 dBm (UL/DL)
- Počet antén: 1
- Prijímač: 1 (SISO)
- Zabezpečenie: LTE security
- Spotreba (idle): 4uA v deep-sleep režime
- Spotreba (Rx): ≈ 100mA
- Spotreba (Tx): ≈ 250mA

1.1.2 Zhrnutie

NB-IOT je derivátom technológie pre mobilnú komunikáciu - LTE a je definovaný v 3GPP LTE rev. 13. Jeho parametre a fakt, že dokáže koexistovať so sieťami LTE a prenášať dáta cez existujúcu sieť základňových staníc štvrtej generácie (4G) mu predurčujú sľubnú budúcnosť aj 5G sieťach. Prevádzka zariadení NB-IOT, ktoré majú nízke obstarávacie náklady môže operátorom prinášať dodatočné zisky z využitia pásma. Ide však o platenú službu, čím je užívateľ závislý od operátora z hľadiska jeho cenovej politiky.

1.2 LoRaWAN

Technológia LoRaWAN je LPWAN technológia pracujúca v nelicencovanom pásme - ISM (Industry, Scientific, Medicine). Základ technológie LoRaWAN tvori LoRa

[1]Zdroj: https://www.4gltemall.com/ue-category/lte-cat-nb1.html

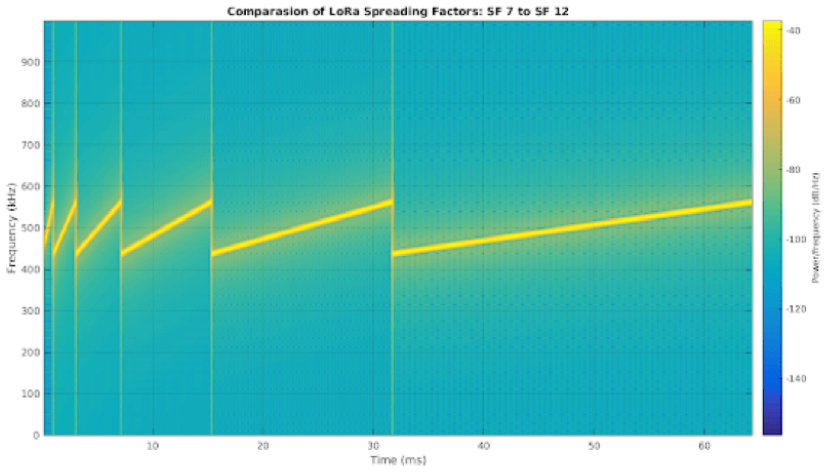
fyzická vrstva s proprietárnou moduláciou CHIRP s rozprestretým spektrom a nad touto vrstvou je z hľadiska OSI/ISO modelu definovaná MAC vrstva ktorá už tvorí základ štandardu. Pri vývoji modulácie bol dôraz na komunikáciu na dlhé vzdialenosti a rýchlosť prenosu nebola rozhodujúcim faktorom. V otvorenom priestore je dosiahnuteľná komunikačná vzdialenosť až 15km a to pri 25mW (14dBm) vysielacom výkone[2] Technológia LoRa bola pôvodne vyvinutá francúzskou firmou Cycleo, ktorú v 2012 odkúpil Semtech, ktorý vyrába komunikačné čipy LoRa pre výrobcov komunikačných modulov.

1.2.1 Parametre LoRaWAN

Modulácia CSS (Chirp spread spectrum) je veľmi flexibilná a môže pracovať v rozsahu od 137 do 1020MHz. V tomto rozsahu sú ISM pásma 169, 433, 868 a 915MHz. Šírka pásma je 125 alebo 250kHz. Podľa potreby je možná modifikácia troch kľúčových parametrov modulácie:

- Činiteľ rozprestretia - Spreading factor - (SF) = {7..12}
- Šírka pásma - Bandwidth (BW)
- Kódovací pomer - Coding ratio (CR)

CHIRP (Compressed High Intensity Radar Pulse)



Obr. 1.2: LoRa SF - Spreading factor SF=7 .. 12[3]

Chirp je zmena frekvencie f v čase t. Je definovaný *up-chirp* ako zmena od f_{low} po f_{high} a *down-chirp* ako zmena od f_{low} po f_{high}. Trvanie zmeny frekvencie je

[2].

[2]V ČR a SR tak ako aj inde v EÚ je povolený vysielací výkon 14dBm pri striede 1%

[3]Zdroj: https://nicbkw.com/technical-overview-of-lora-LoRaWAN-and-the-things-network/

ovplyvnené parametrom *SF*, pričom zvýšenie *SF* o jednotku zvýši *on-air time* na dvojnásobok ako je zrejmé z obrázku 1.2.1. Jeden chirp sa skladá z chipov. Skupina 2^{SF} chipov je jeden symbol. Každý symbol nesie *SF* bitov. Chip vyjadruje jedinečnú hodnotu signálu v rámci chirp modulácie.

SF	Chip/Sym	Limit SNR	Bitrate
7	128	-7,5dB	5469 b/s
8	256	-10dB	5469 b/s
9	512	-12,5dB	1758 b/s
10	1024	-15dB	977 b/s
11	2048	-17,5dB	537 b/s
12	4096	-20dB	293 b/s

Tab. 1.1: Vplyv činiteľa rozprestretia na citlivosť prijímača

V rámci európskych smerníc sa pre LoRaWAN používa sub-GHz ISM pásmo a to frekvencie v oblasti 868MHz. V tomto pásme je vyhradených až 56 kanálov so šírkou 125kHz ale v praxi sa kvôli eliminácii vzájomného rušenia používa len 10. Ďalším obmedzením je využitie ISM pásma 868MHz. Koncové zariadenie smie vysielať len 1% z celkovej doby uptime.T.j. ak je zariadenie v prevádzke hodinu môže vysielať len 36s, zvyšných 3564s môže len prijímať.

Koncové zariadenia LoRaWAN sa podľa spôsobu komunikácie so základňovou stanicou (gateway) zaraďujú do 3 tried, pričom zariadenie sa môže prepínať medzi jednotlivými triedami:

- **Trieda A** - komunikácia plne riadená koncovým bodom. Koncové zariadenie komunikuje len v určitých intervaloch aebo podľa potreby odosielania dát. Po Tx relácii nasledujú dve okná na príjem správ zo siete. Trieda A je energeticky najúspornejšia.
- **Trieda B** - Prijímanie správ zo siete sa realizuje nielen po odoslaní správ, ale v pravidelných intervaloch. Zariadenie sa pravidelne aktivuje pre príjem správ zo siete a očakáva príjem správy. Je nutná synchronizácia so sieťou pomocou synchronizačných impulzov, ktoré sú vysielané každých 128s.
- **Trieda C** - príjem dát zo siete je trvale povolený. Ide o energeticky najnáročnejší režim. Uplatní sa najmä ak je zariadenie pripojené k zdroju el. energie.

1.2.2 Zabezpečenie LoRaWAN

Bezpečnosť je základnou potrebou vo všetkých aplikáciách a v rámci LoRaWAN je jej súčasťou od samého začiatku. Téma bezpečnosti zahŕňa viacero vlastností. Najmä kryptografické mechanizmy používané na implementáciu bezpečnosti LoRaWAN si

zaslúžia detailnejšie vysvetlenie. Predstavíme bezpečnostné vlastnosti obsiahnuté v špecifikácii LoRaWAN, potom podrobnosti o ich implementácii a vysvetlenie bezpečnostného dizajnu LoRaWAN.

Zabezpečenie LoRaWAN je navrhnuté tak, aby vyhovovalo všeobecným kritériám dizajnu LoRaWAN: nízka spotreba energie, jednoduchosť implementácie, nízke náklady a škálovateľnosť. Pre zariadenia nasadené v teréne na dlhé časové obdobia (roky), je potrebné zaistiť bezpečnosť. Bezpečnostný dizajn LoRaWAN sa drží najmodernejších princípov: používanie štandardných, preverených algoritmov a bezpečnosť „end-to-end“. Základné vlastnosti, ktoré sú súčasťou v zabezpečenia LoRaWAN:

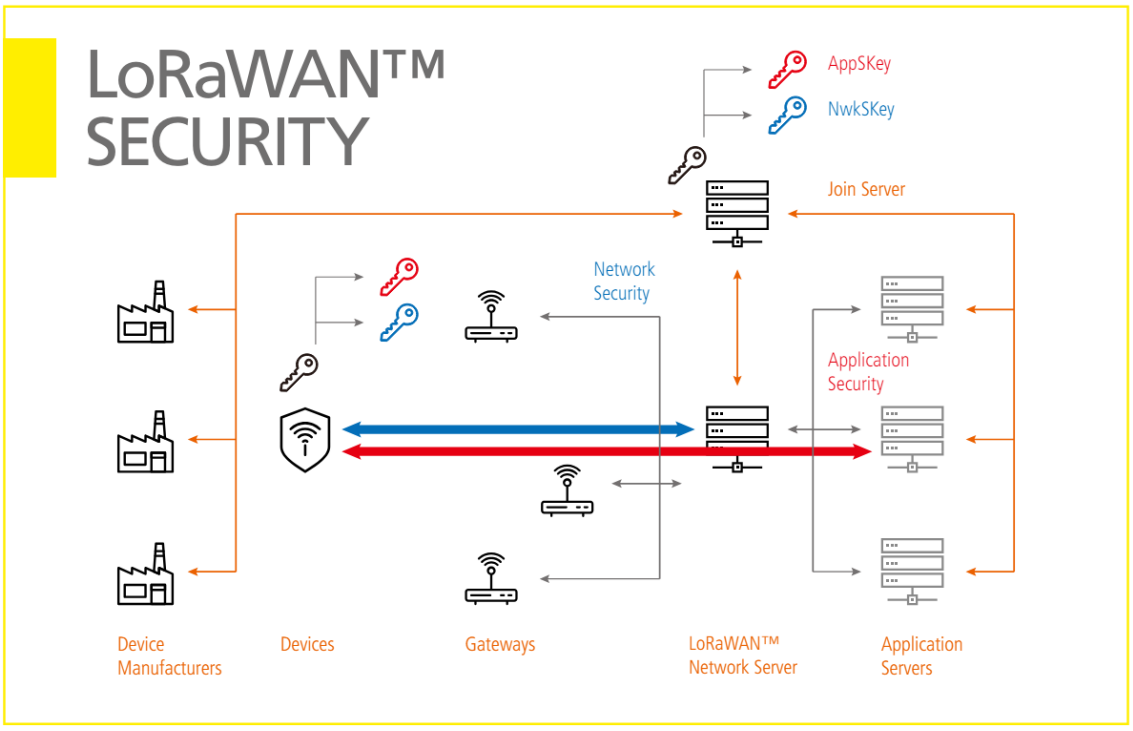
- vzájomná autentifikácia
- ochrana integrity a dôvernosti

Vzájomné overovanie medzi koncovým zariadením LoRaWAN a sieťou LoRaWAN je súčasťou procesu pripojenia k sieti. To zaisťuje, že iba originálne a autorizované zariadenia môžu komunikovať so sieťou a zariadeniami v nej. LoRaWAN MAC a aplikačné správy majú zabezpečenú autenticitu, ochranu integrity, replay-ochranu a šifrovanie. Táto ochrana, kombinovaná so vzájomnou autentifikáciou, zabezpečuje že sieťová prevádzka je nezmenená, pochádza z legitímneho zariadenia, nie je zrozumiteľná pre odpočúvajúcich a nebola zachytená a prehraná útočníkom. Zabezpečenie LoRaWAN ďalej implementuje end-to-end šifrovanie pre aplikáciu užitočného obsahu „payload“, ktorý si vymieňajú medzi sebou koncové zariadenia a aplikačné servery. LoRaWAN je jedna z mála sietí internetu vecí, ktorá implementuje end-to-end šifrovanie. V niektorých tradičných mobilných sieťach je prevádzka šifrovaná pri prenose vzduchom, ale prenáša sa ako obyčajný text v sieti operátora. V dôsledku toho sú koncoví používatelia sú nútení pridávať bezpečnostnú vrstvu (VPN alebo zabezpečenie prostredníctvom aplikačnej vrstvy - zabezpečenie šifrovaním, ako je TLS). Tento prístup nie je vhodný pre siete LPWAN, kde dodatočné bezpečnostné vrstvy znamenajú vyššiu spotrebu, zložitosť a cenu.

Spomínané bezpečnostné mechanizmy sú založené na osvedčených a štandardizovaných AES kryptografických algoritmoch. Tieto algoritmy sú analyzované kryptografickou komunitou už mnoho rokov a sú široko prijímané ako najlepšie praktické zabezpečenie pre uzly s obmedzenými zdrojmi.

Zabezpečenie LoRaWAN používa AES kryptografické primitíva v kombinácii s niekoľkými režimami prevádzky: CMAC na ochranu integrity a CTR pre šifrovanie. Každé zariadenie LoRaWAN disponuje jedinečným 128-bitovým AES kľúčom (AppKey) a celosvetovo jedinečným identifikátorom (DevEUI založený na EUI-64), oba sa používajú počas procesu autentifikácie zariadenia. Prideľovanie EUI-64 identifikátorov vyžaduje, aby mal správca pridelený jedinečný identifikátor organizácie (OUI) od registračnej autority IEEE. Podobne siete LoRaWAN sú identifikované pomocou

24-bitového globálne jedinečného identifikátora prideleného LoRa Allianciou.



Obr. 1.3: Kryptografické zabezpečenie siete LoRaWAN

Užitočný obsah „payload“ aplikácií LoRaWAN je medzi koncovým zariadením a aplikačným serverom vždy šifrovaný. Ochrana integrity správ je poskytovaná spôsobom hop-by-hop, t.j. jeden skok cez vzduch prostredníctvom ochrany integrity poskytovanej protokolom LoRaWAN a druhý skok medzi sieťou a aplikačným serverom pomocou bezpečných transportných riešení, ako sú HTTPS a VPN.

Počas over-the-air aktivácie (OTAA) si koncové zariadenie a sieť vzájomne preukážu, že majú znalosť AppKey. Tento dôkaz je založený na výpočte AES-CMAC (pomocou AppKey) na žiadosť zariadenia o pripojenie a koncového prijímača. Z toho sú potom odvodené dva kľúče, jeden na ochranu integrity a šifrovania príkazov LoRaWAN MAC a obsahu (NwkSKey) a jeden pre end-to-end šifrovanie obsahu aplikácie (AppSKey). NwkSKey je distribuovaný do siete LoRaWAN na preukázanie/overenie pravosti a integrity paketov. AppSKey sa distribuuje na aplikačný server v poradí na šifrovanie/dešifrovanie obsahu aplikácie. AppKey a AppSKey umožňuje zabezpečiť prenos cez prevádzkovateľa siete tak, že nebude schopný dešifrovať obsah správy aplikácie.

Niektoré zdroje uvádzajú, že LoRaWAN kryptografia používa iba XOR a nie AES. V skutočnosti, ako už bolo spomenuté, AES sa používa v štandardizovanom CTR režime, ktorý využíva kryptografickú XOR operáciu (ako mnoho iných režimov

ako CBC). To posilňuje AES algoritmus pomocou jedinečného kľúča AES pre každú blokovú šifru. [1]

Hlavné vlastnosti LoRaWAN

- Potrebná šírka pásma: 125kHZ
- Download (max): 0,3 - 50 kbit/s
- Upload (max): 0,3 - 50 kbit/s
- Latencia: 1.6s–10s
- Duplex: half duplex
- Vysielací výkon: 14 dBm (UL/DL)
- MCL: 157dB
- Zabezpečenie: AES-128, DevEUI/AppEUI/AppKey

1.2.3 Zhrnutie

LoRaWAN nájde uplatnenie v komunikácii IOT na dlhé vzdialenosti kde je potrebná obojsmerná komunikácia. Výhodou siete LoRaWAN je, že Gateway môže prevádzkovať ktokoľvek a pomocou otvorenej platformy thethingsnetwork.com sa akékoľvek zariadenie môže do siete LoRaWAN pripojiť. Podobne aj v prípade siete Helium ide o verejnú sieť, ktorá je prevádzkovaná jednotlivcami. Ide o prvú z aplikácií momentálne sa rozvíjajúceho trendu DePIN (Decentralized Physical Infrastructure Networks). Cieľom projektov DePIN je vytvoriť demokratizované technológie, ktoré budú konkurovať centralizovaným technologickým ponukám, čo umožní jednotlivcom prispieť k rozšíreniu a decentralizácii služby a dostávať odmenu vo forme kryptomeny [9], [12].

1.3 Sigfox

Sigfox pracuje v sub-GHz bezlicenčnom pásme podobne ako LoRaWAN a takisto ide o proprietárnu technológiu vyvinutú francúzskou spoločnosťou Sigfox. Na rozdiel od LoRaWAN u Sigfoxu je sieť budovaná a rozširovaná integrátormi v jednotlivých krajinách. V Českej republike a na Slovensku je prevádzkovateľom spoločnosť SimpleCell, pričom v každej krajine ide o samostatnú právnickú osobu. Sieť je vo svojej podstate verejná a nie je možné budovať privátnu sieť s vlastným cloudom. V súčasnosti operuje v 75 krajinách vrátane Českej Republiky, „0G network“ ako Sigfox pomenoval svoju sieť, pokrýva viac ako 1.4 miliardy ľudí. V roku 2021, Sigfox pripájal 19.5 milióna pripojených zariadení a 76 miliónov správ odoslaných každý deň. Od Januára 2022 je Francúzska spoločnosť Sigfox pod ochranou súdu proti veriteľom a pre svoj ďalší rozvoj hľadá investora[11].

Obr. 1.4: Pokrytie Sigfox v Januári 2020[4]

1.3.1 Parametre Sigfox

Sigfox pracuje v pásme 868,034 - 868,226 MHz a využíva tak pásmo o šírke 192kHz. Pre prenos správ sa využívajú nosné s veľmi úzkym pásmom (Ultra narrow Band) v smere uplink 100 Hz a moduláciou DBPSK (Differential Binary Phase Shift Keying). Mierne odlišnosti oproti EÚ sú v regiónoch Ázie a USA, kde sú použiteľné frekvenčné pásma 915 MHz a 433 MHz v USA je možné použiť šírku pásma až 600Hz. Technológia Sigfox bola pôvodne navrhnutá len pre Uplink (UL), t.j. zasielanie správ od koncového zariadenia k základňovej stanici. neskôr sa pristúpilo aj ku komunikácii Downlink (DL). Pre DL sa využíva pásmo 868,40 - 869,65 MHz a teda široké 1,5kHz. Vo výsledku prostredníctvom modulácie GFSK (Gaussian Frequency Shift keying) poskytuje prenosovú rýchlosť 600 b/s. Vplyvom regulácie v EÚ je v pásme 868 MHz povolené vysielanie 1% celkového uptime času čo v rámci jedného dňa 86400s umožňuje stanici vysielať 864s. Za tento čas je možné preniesť 140 správ o veľkosti 24B (192bit). Každá správa sa vysiela 3x na troch rôznych frekvenciách. Vysielací výkon v smere UL je 14 dBm a v smere downlink 27 dBm. MCL (Maximum Coupling Loss) má hodnotu 156 dBm. Dosiahnuteľná vzdialenosť vo vidieckych oblastiach je 30-50 km, v meste 3-10 km. Pre správy v smere downlink (DL) sa využíva 20s okno

[4]Zdroj: https://www.sigfox.com/en/coverage

po odoslaní prvej správy od koncovej stanice. Počas tohoto okna môže koncová stanica prijímať správy downlink. Na zabezpečenie Sigfox sa používa sekvenčné číslo správy v kombinácii s MAC tokenom pre odosielané správy. Vo výrobe je každému zariadeniu poskytnutá unikátna sada symetrických kľúčov. Dáta z koncových staníc sú dostupné cez webové alebo API rozhranie operátora Sigfox pomocou callbackov.

Hlavné vlastnosti Sigfox:

- Šírka pásma: 100 Hz
- Downlink (max): 1,5 kbit/s
- Upload (max): 100 b/s
- Latencia: niekoľko sekúnd
- Duplex: simplex
- Vysielací výkon: 14 / 27 dBm (UL/DL)
- MCL: 156dB
- Zabezpečenie: kontrola integrity správ, šifrovanie je užívateľsky voliteľné

1.3.2 Zhrnutie

Sigfox je komerčná sieť pre prenos IOT dát. Jej výhodou je veľké pokrytie, nízke mesačné poplatky (˜ 1 USD), garantované SLA 99% a automatický medzinárodný roaming. Nevýhodou je pomerne obmedzená komunikácia v smere ku koncovej stanici. Sigfox je teda vhodne použiteľný pre aplikácie, kde je potrebné dáta odosielať od koncovej stanice do siete.

1.4 Porovnanie technológií LPWAN

V nasledujúcej tabuľke sú zhrnuté technológie popísané v predchádzajúcich kapitolách.

Vzhľadom na zadanie projektu nebudem vyberať vhodnú technológiu, nakoľko táto je už vybraná v zadaní. Pre porozumenie prečo je LoRaWAN vhodnou technológiou pre požadované riešenie je potrebné vychádzať z požiadaviek na:

- výdrž batérie,
- dosah (Radio Link Budget),
- zriaďovacie a priebežné náklady.

Z technológií uvedených v tejto kapitole sa ďalšej kapitole zameriam len na NB-IOT a LoRaWAN, keďže spoločnosť Sigfox ako prevádzkovateľ rovnomennej centralizovanej siete vo Februári 2022 požiadala o ochranu pred veriteľmi Francúzsky obchodný súd v Toulouse. Budúce udržanie a rozvoj tejto platformy je teda otázne.

	NB-IoT	LoRa	Sigfox
Modulácia	QPSK	CSS	BPSK
Frekvenčné pásmo	800MHz; 2500MHz	868MHz	868MHz
Šírka pásma	200kHz	250kHz	100Hz
Licencované	Áno	Nie	Nie
Citlivosť prijímača	-141dBm	-136dBm	-142dBm
Max. prenosová rýchlosť	200kb/s	50kb/s	100b/s
Max. veľkosť správy	1600B	243B	12B(UL) / 8B (DL)
Max. počet správ denne	Neobmedzene	Neobmedzene	144
Max. Tx výkon	200mW (23dBm)	25mW (14dBm)	25mW (14dBm)
Zabezpečenie	LTE	AES-128	bez podpory

Tab. 1.2: Porovnanie LPWAN technológií

1.4.1 Porovnanie NB-IOT a LoRaWAN

Nedávne štúdie ukazujú, že oba protokoly môžu koexistovať na trhu IoT. LoRaWAN bude slúžiť ako nízkonákladový a je vhodný pre nasadenie na veľké vzdialenosti, so zriedkavými prenosmi a obmedzeniami z hľadiska životnosti batérie. Na druhej strane, LoRaWAN nedokáže poskytnúť rovnakú garanciu kvality služby (QoS) ako NB-IoT, pretože NB-IOT používa licencované spektrum a protokol s časovým delením [2]. Pri návrhu zabezpečovacieho zariadenia je nevyhnutné venovať sa spoľahlivosti zariadenia a prenosu. Útok založený na rušení pásma je možný v oboch prípadoch. Kým pri NB-IOT je to napríklad zablokovaním synchronizačných správ, ktoré základňová stanica zasiela koncovým zariadeniam [4] prípadne selektívnym útokom [6], reláciu LoRaWAN útočník môže zablokovať rušením príjmu základňovej stanice [3], [5]. Ako teda vidíme, úmyselné rušenie pre zablokovanie prenosu správ predstavuje problém pre obidve technológie.

2 Výber komunikačnej siete IOT a hardvéru

Siete LPWAN popísané v predchádzajúcej kapitole majú svoj význam pre rôzne typy aplikácií. V tejto kapitole sa venujem analýze komunikačných potrieb požadovaného riešenia, špecificky sieťam LoRaWAN a voľbe hardvéru.

2.1 LoRaWAN siete

Na základe analýzy uvedenej vyššie je LoRaWAN je vhodnou komunikačnou platformou pre uvedené zariadenie. LoRaWAN umožňuje komunikáciu na veľké vzdialenosti, rádovo jednotky až desiatky kilometrov v otvorenom priestore a s relatívne malým výkonom 14dBm. LoRaWAN zariadenie pracujúce v triede A môže byť väčšinu času v režime spánku, čím sa zabezpečí jeho minimálna spotreba a výdrž batérie aj niekoľko rokov.

LoRa

je fyzická vrstva. Používa moduláciu Chirp Spread Spectrum (CSS), t.j. s rozprestretým spektrom. Použitie je vhodné všade tam, kde je potrebný prenos malého množstva dát na väčšie vzdialenosti. Typickou aplikáciou môže byť spojenie medzi dvoma koncovými bodmi, napríklad na prenos telemetrických údajov.

LoRaWAN

je z hľadiska OSI/ISO modelu definovaná ako MAC vrstva nad LoRa fyzickou vrstvou. Protokol LoRaWAN je vyvinutý a udržiavaný alianciou LoRa Alliance. Prvá špecifikácia LoRaWAN bola vydaná v januári 2015. V čase písania tejto práce sú najnovšie špecifikácie 1.0.4 (v sérii 1.0) a 1.1 (v sérii 1.1).

Typická sieť LoRaWAN pozostáva z nasledujúcich základných prvkov.

- **Koncové zariadenia** - Senzory alebo akčné členy posielajú bezdrôtové správy modulované LoRa do brán alebo prijímajú správy bezdrôtovo späť z brán.
- **Brány** - Špecializované zariadenia, ktoré prijímajú správy z koncových zariadení a preposielajú ich na sieťový server, ako aj posielajú správy zo sieťového servera na koncové zariadenia.
- **Sieťové servery** - Softvér bežiaci na serveri, ktorý spravuje sieť. Tiež označovaný ako LoRaWAN Network Server/LNS alebo jednoducho sieťový softvér.
- **Aplikačné servery** - Softvér bežiaci na serveri, ktorý je zodpovedný za bezpečné spracovanie údajov aplikácie.

LoRaWAN siete môžeme z hľadiska prevádzkovateľa rozdeliť do troch kategórií:

- Súkromné - Private Networks
- Komunitné - Community networks
- Verejné - Public networks

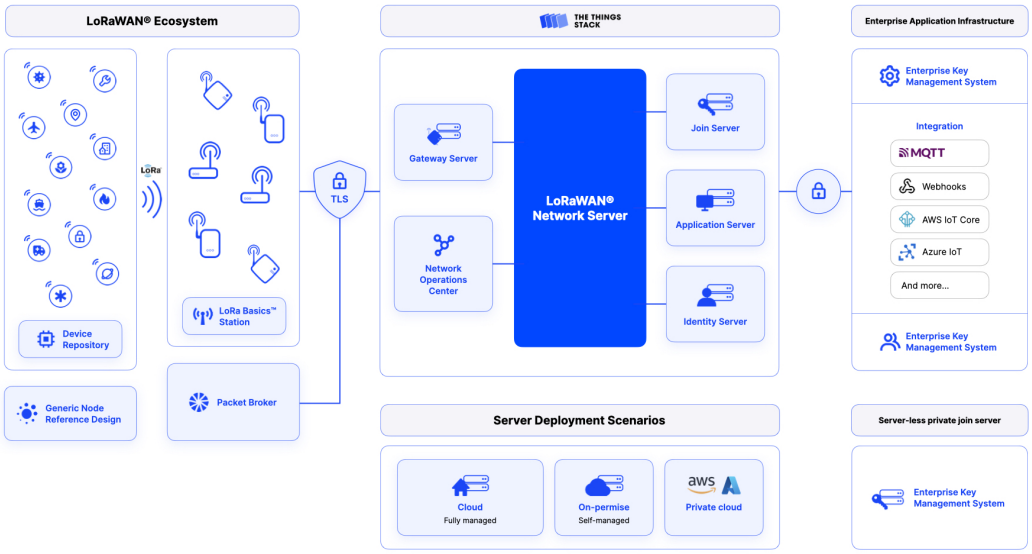
Vybudovanie vlastnej (privátnej) LoRaWAN siete a jej prevádzka dáva zmysel najmä vo vnútropodnikových aplikáciách. Náklady na zriadenie LoRaWAN brány sa pohybujú okolo 5-10 tisíc Kč. Okrem toho je možné použiť niektorú z verejných alebo komunitných sietí. Siete Helium a TTN, ktoré popíšem v nasledujúcej podkapitole sú na rozhraní medzi verejnými a komunitnými sieťami. Kým komunitnou sieťou by sa dala nazvať každá sieť, ktorá poskytuje služby bez komerčného prospechu, verejnou sieťou bude naopak sieť, ktorej prevádzkovateľ ju poskytuje s cieľom zisku. Tu by bolo dobré ozrejmiť, že poskytovanie služby siete LoRaWan, napriek fyzickej spoľahlivosti použitého hardvéru je v samotnom prenosovom médiu bez garancie kvality služby (Service Level Agreement - SLA). V rádiovom spektre, ktoré je zdieľané tisíckami iných zariadení by úvaha o prípadnom SLA pomerne rýchlo narazila na limitáciu zdieľaných a nelicencovaných frekvenčných blokov.

2.1.1 Prenos správ v sieťach LoRaWAN

Koncové zariadenia komunikujú s najbližšími **bránami** a každá brána je pripojená k sieťovému serveru. Siete LoRaWAN používajú protokol ALOHA, pričom koncové zariadenia sa nemusia spárovať so konkrétnymi bránami. Správy odoslané z koncových zariadení sú prijaté všetkými bránami v dosahu.Brány posielajú správy na **sieťový server**. Ak sieťový server prijal viacero kópií tej istej správy, ponechá si jednu kópiu správy a ostatné zahodí, čo sa nazýva aj de-duplikácia správ. Sieťový server oddeľuje servisné dáta so sieťovými nastaveniami od samostatne zašifrovaných dát aplikácie (senzora) a posiela ich aplikačnému serveru. **Aplikačný server** dešifruje údaje aplikácie a sprístupní ich používateľovi prostredníctvom integračných služieb danej siete. Správy, ktoré pochádzajú z koncového zariadenia voláme **Uplink**. Správy opačným smerom (zo sieťového servera a/alebo aplikačného servera a odoslané do koncových zariadení) voláme **Downlink**.

2.1.2 The Things Network (TTN)

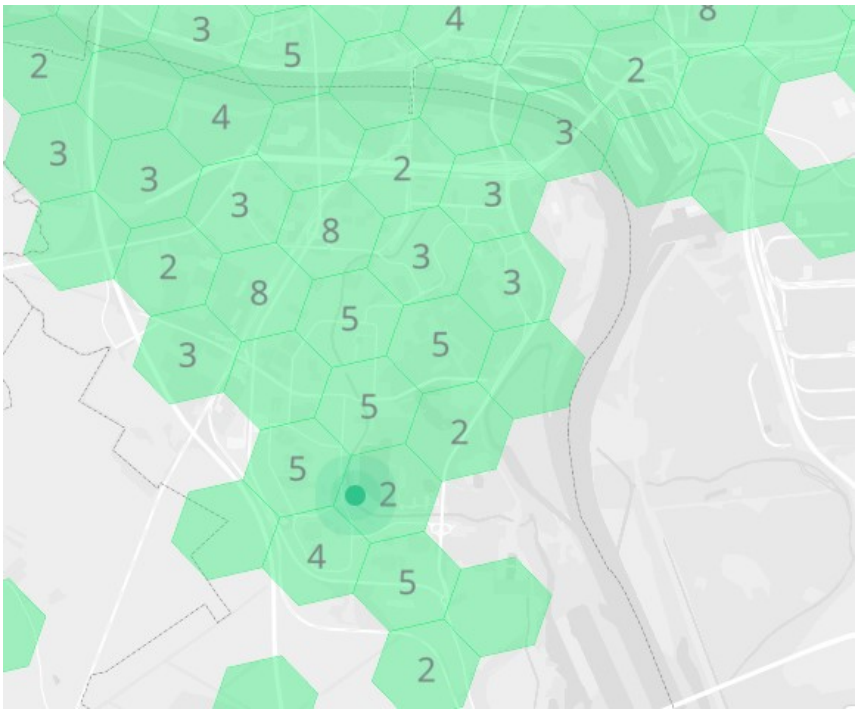
The Things Network je súbor nástrojov a globálna otvorená sieť pre aplikácie internetu vecí. TTN využíva brány LoRAWAN siete prevádzkované jednotlivcami a komunitami. Okrem toho prevádzkuje The Things Stack v úlohe sieťového a aplikačného servera. Prevádzka v sieti je bezplatná v prípade programu **Discovery** do 10 koncových zariadení a 10 brán. Platené programy **Standard** a **Plus** umožňujú pripojenie veľkého počtu zariadení a 99.9% uptime SLA.



Obr. 2.1: Architektúra siete TTN

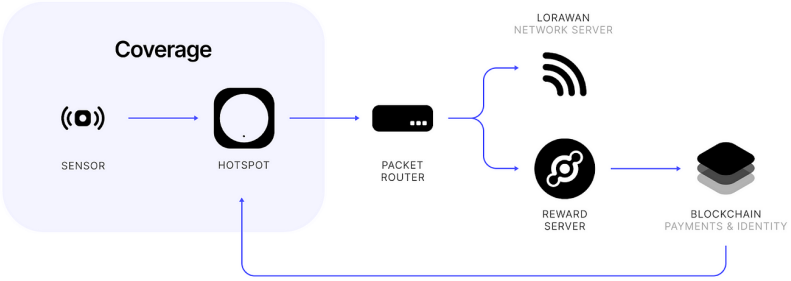
2.1.3 Sieť Helium IOT

Za vznikom siete Helium v roku 2019 stojí nadácia Helium Foundation, Inc. Ide o sieť ktorej základ tvorí blockchain PoC (Proof of Coverage) a otvorené aplikácie, ktorých zdrojové kódy su prístupné na Github https://github.com/helium. Koncept odmeňuje prevádzkovateľov rádiových bodov virtuálnou menou IOT za to, že obsluhujú určitú oblasť. Overovanie aktuálneho pokrytia konkrétneho rádiového bodu (brány, resp. hotspotu) prebieha niekoľkokrát denne pomocou blockchain protokolu PoC (Proof of Coverage). Algoritmus vytvorí zoznam náhodne vybraných hotspotov, ktoré sa majú prezentovať zaslaním tzv. majáku (beaconu). Na celom svete je každú polhodinu teda vybraných do zoznamu približne 20-tisíc hotspotov. Zvolené hotspoty vyšlú v náhodne zvolenom čase počas polhodinového okna maják, ktorého rádiové parametre zachytia okolité hotspoty - tzv. witness a odošlú report na centrálny validátor. Validátor dáta vyhodnotí, pričom berie do úvahy len 14 správ, ktoré prišli najskôr. Z databázy získa geografické informácie o polohe witness hotspotov a pomocou RSSI (sila prijatého signálu) a SNR vypočíta polohu zdroja signálu. Hotspoty za každý vyslaný alebo prijatý maják získavajú odmenu vo forme virtuálnej meny. Koncept siete alokuje hotspoty do šesťuholníkových oblastí, tzv. hexagonov. Hexagony sú podľa veľkostí zaradené do jednej z 13-tich veľkostných kategórií. Najmenšia úroveň (s indexom 12) sú hexagony s plochou 0,3m^2. Dalšia vyššia úroveň obsahuje 7 takýchto hexagonov a jej plocha je takto sedemnásobne väčšia. Podobne sa na každej ďalšej úrovni plocha hexagonu sedemnásobne zväčšuje. Na najvyššej



Obr. 2.2: Rozloženie hexagonov siete Helium

úrovni (index 0) je plocha hexagonu až 4 250 546km^2 [7]. Dosah stanice nemá priamy súvis s hexagonmi a nezriedka sa stáva, že pokrytie územia jedným hotspotom môže dosahovať aj desiatky či stovky km^2.



Obr. 2.3: Architektúra siete helium

Hotspoty s takýmto pokrytím zachytávajú aj vzdialené majáky, čím získavajú väčšiu šancu na získanie odmeny. Zároveň algoritmus siete Helium reguluje maximálny počet hotspotov v jednotlivých úrovniach nastavením tzv. vysielacej mierky resp. diskriminátora, ktorý pri veľkom počte hotspotov v danej oblasti pomerne znižuje získanú odmenu. Proces motivácie obsahuje niekoľko ďalších parametrov podľa

[0]https://app.hotspotty.net/

ktorých sa odvíja odmeňovanie prevádzkovateľov, avšak tie priamo nesúvisia so zadaním práce preto ich nebudem rozoberať.

Architektúrou je sieť Helium podobná sieti TTN. Obsahuje prvky popísané v podkapitole 2.1 - brány, sieťové servery a aplikačné servery.

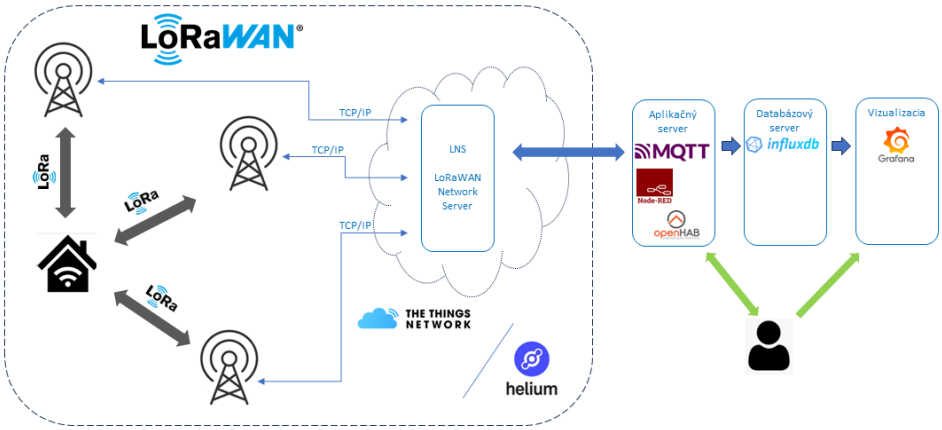
Siete Helium aj TTN sú podobné z hľadiska architektúry. Softvér úsporného zabezpečovacieho zariadenia by mal byť napísaný tak, aby umožnil použitie akejkoľvek verejnej LoRAWAN siete. Zariadenie môže komunikovať len v jednej sieti. Softvér bude umožňovať kompiláciu pre jednotlivé siete pomocou direktívy a voľby parametrov *AppEUI, DevEUI a AppKey*.

3 Realizácia

V tejto kapitole sú popísané komponenty systému, z ktorých systém pozostáva:

- Koncové zariadenie - klient siete LoRWAN, jeho programové vybavenie a zapojenie.
- Verejná sieť LoRaWAN - Helium
- MQTT broker - smerovač správ MQTT
- NodeRed - nástroj pre tvorbu programov na báze JavaScriptu
- InfluxDB - databáza pre uchovávanie dát s časovou značkou
- Grafana - nástroj na vizualizáciu dát
- OpenHAB - Aplikácia pre smart-home a automatizáciu

Graficky je schéma komunikácie znázornená na obrázku. 3.1



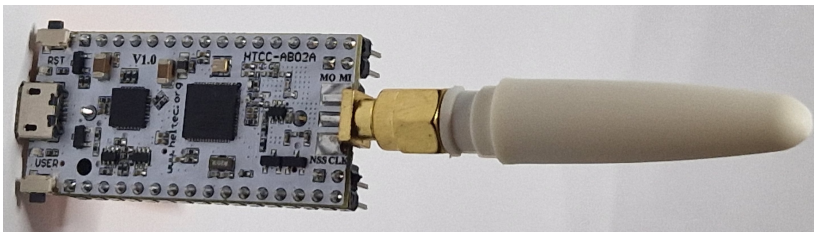
Obr. 3.1: Diagram komunikácie

3.1 Elektronická a komunikačná časť LoRaWAN

Komunikačnou jednotkou koncového bodu *LoRaWAN node* je zariadenie Heltec Cubecell HTCC-AB02A s procesorom ASR65602.

3.1.1 Koncové zariadenie - Heltec HTCC-AB02A

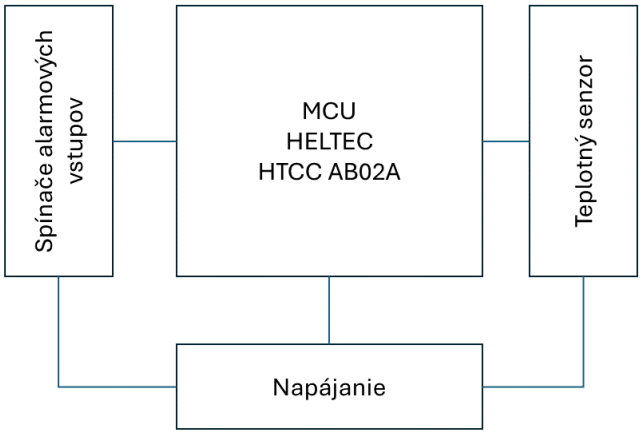
Zariadenie Heltec HTCC-AB02A je vývojárskou verziou CubeCell. Obsahuje procesor ASR6502 (48 MHz ARM® Cortex® M0+ MCU) a LoRa Chipset SX1262



Obr. 3.2: Heltec HTCC-AB02A

pracujúci na frekvenciách pre EU 863 928MHz. Maximálny RF výkon na konektore je 22 ± 1dBm, pre súlad max. povoleným výkonom EIRP je potrebné pripočítať zisk antény, v tomto prípade ide však o 0dB. Max EIRP pre pásmo 868MHz v Europe je 14dBm (25mW). Citlivosť prijímača zariadenia je -135dBm. Zariadenie obsahuje ďalej: 2x UART port; 2x SPI; 2x I2C; SWD; 3x 12-bitový AD prevodník; 8–kanálový DMA; 16 GPIO pinov. Okrem toho 128Kbit FLASH pamäte; 16Kbit SRAM. Spotreba v režime deep-sleep je 3.5μA. Prevádzková teplota -20 70 ℃, rozmery: 56.6 x 24 x 21.5 mm. Zariadenie disponuje jedným Micro USB portom; LoRa Antenna interface(SMA); Rozostup pinov je 16 x 2.54 pin x 2+2 x 2.54 pin x 2. Zariadenie je napájané z Lítium-Iónovej batérie s nominálnym napätím 3,7V a kapacitou 2000mAh.

Blokový diagram zapojenia



Obr. 3.3: Blokový diagram zapojenia

Schéma zapojenia

Schéma zapojenia je uvedená v prílohe C Teplotný senzor DS18B20 je napájaný prostredníctvom Vext, t.j. zdroja, ktorý je možné zapnúť a vypnúť programovo. Vstupy pre alarmové kontakty sú riešené ako NC / NO. V oboch prípadoch je výstup 3,3V privedený na spínací resp. rozpínací kontakt a odtiaľ na príslušný GPIO pin. Impedancia GPIO vstupov je $> 1M\Omega$.

Napätie batérie

Pre meranie napätia batérie je v MCU použitý signál *VBAT ADC Ctrl*.

Senzor teploty

Pre potreby merania vnútornej teploty zariadenia je použitý senzor DS18B20 s protokolom OneWire pripojený na jeden z voľných GPIO portov. Systémový teplotný senzor bude umiestnený priamo vo vnútri krabičky, nemožno ho odpojiť.

Priradenie jednotlivých GPIO

GPIO	**prvok**	**popis**
GPIO1	NC1	Normally Closed 1
GPIO2	DS18B20	Teplotný Senzor
GPIO3	NO1	Normally Open 1
GPIO5	NC2	Normally Closed 2
GPIO6	NO2	Normally Open 2

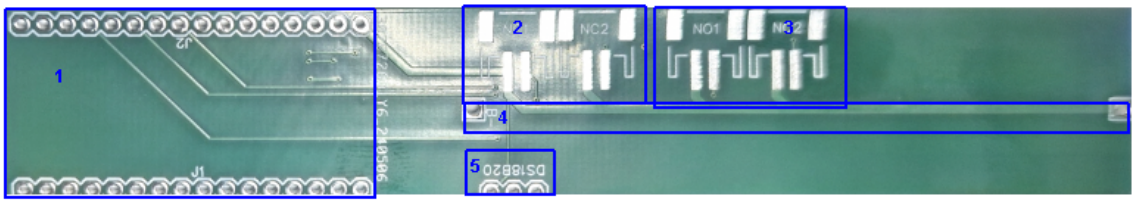
Tab. 3.1: Priradenie jednotlivých kontaktov k GPIO pinom

Doska plošných spojov

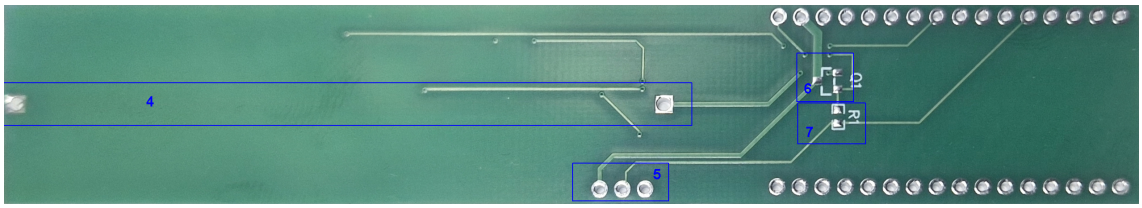
Zariadenie je osadené na DPS pre rozbočenie potrebných kontaktov. Legenda k obrázkom 3.4 a 3.5: *1 - pätica pre modul HTCC AB02A, 2 - kontakty NC (normally closed), 3 - kontakty NO (normally open), 4 - držiak batérie 18650, 5 - senzor teploty DS18B20, 6 - MOSFET 1N2007 proti prepólovaniu batérie, 7 - rezistor 4k7* Pre osadenie modulu HTCC AB02A sú použité dve pätice 1x16 pinov. Pre úsporu miesta som z modulu odspájkoval držiak 1/2AA batérie.

Gerber súbory pre výrobu DPS sú v elektronickej prílohe D.

Usporiadanie dosky po osadení je zrejmé z obrázka 3.6.



Obr. 3.4: DPS spodná vrstva



Obr. 3.5: DPS vrchná vrstva

Napájanie modulu

Napájanie modulu zariadenia zabezpečuje lítium-iónový akumulátor 3,7V s kapacitou 2000mAh. Nabíjanie akumulátora sa nevyžaduje, avšak bolo by možné ho realizovať pripojením vhodného solárneho panelu na pin *Vin*, ktorého vstupné napätie je v rozmedzí 4,7 - 6V. Nameraná spotreba modulu v režime hlbokého spánku je $5,5 - 6\mu A$. Pre výpočet výdrže batérie uvažujeme spotrebu počas jednej hodiny. Odber zariadenia počas vysielania pri 14dBm je podľa produktového listu[8] $i_{tx} = 90mA$. Pri napájaní z batérie v režime *DeepSleep* $i_{DS} = 6\mu A$ po dobu $t_{DS} = 3591s$. Interval vysielania $T = 1h$, po dobu $t_{tx} = 9s$. Kapacita článku 18650 s menovitým napätím 3,7V je $C = 2500mAh$. Odhadovaná výdrž batérie by teda mala byť:

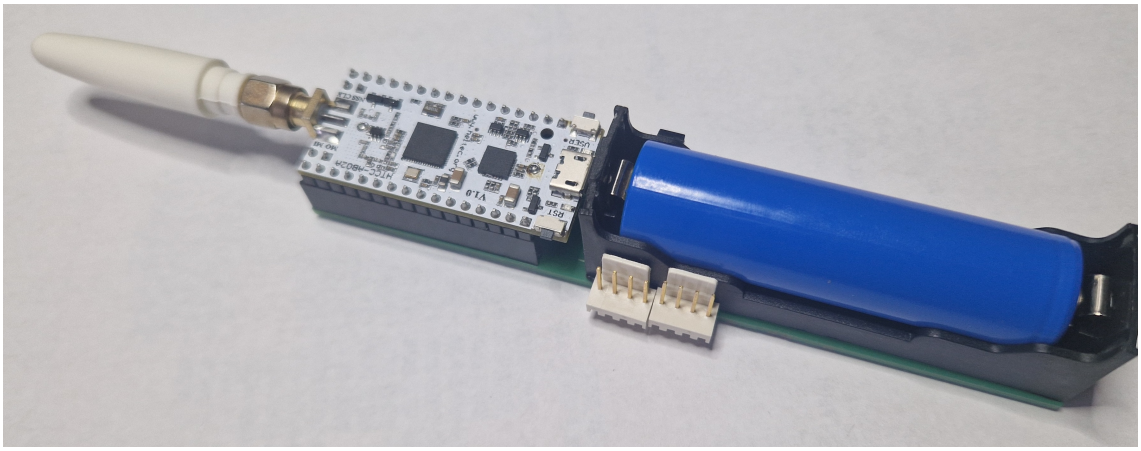
$$t = \frac{C \cdot 3600}{t_{tx} \cdot i_{tx} + t_{DS} \cdot i_{DS}} = \frac{2500 \cdot 3600}{9 \cdot 90 + 3591 \cdot 0,006} \sim 87765h$$

čo predstavuje približne 10 rokov.

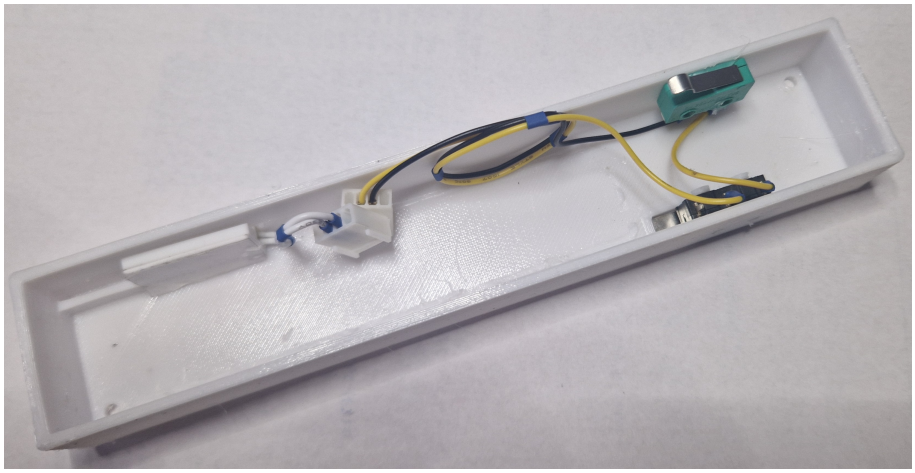
Mechanické riešenie a kryt

Kryt zariadenia je navrhnutý v programe Autodesk Fusion 360. STL súbory jednotlivých častí krytu sú prílohou tejto práce v Prílohe A. Krabička je vytlačená na 3D tračiarni Creality Ender 3 pre ktorú sú nastavenia tlače v súbore v prílohe B. Použitý materiál je PETG. Rozmery krabičky sú 190 x 37 x 30 mm (šírka x výška x hĺbka).

V krabičke sú namontované dva kontakty narušenia zariadenia a jeden magnetický rozpínací kontakt.



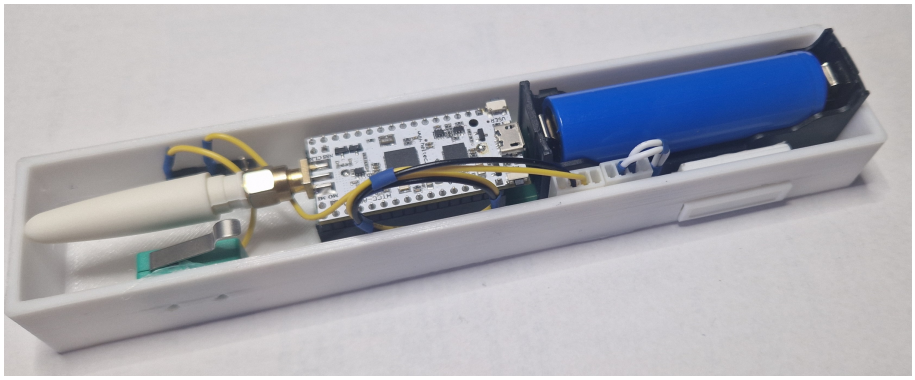
Obr. 3.6: DPS osadená



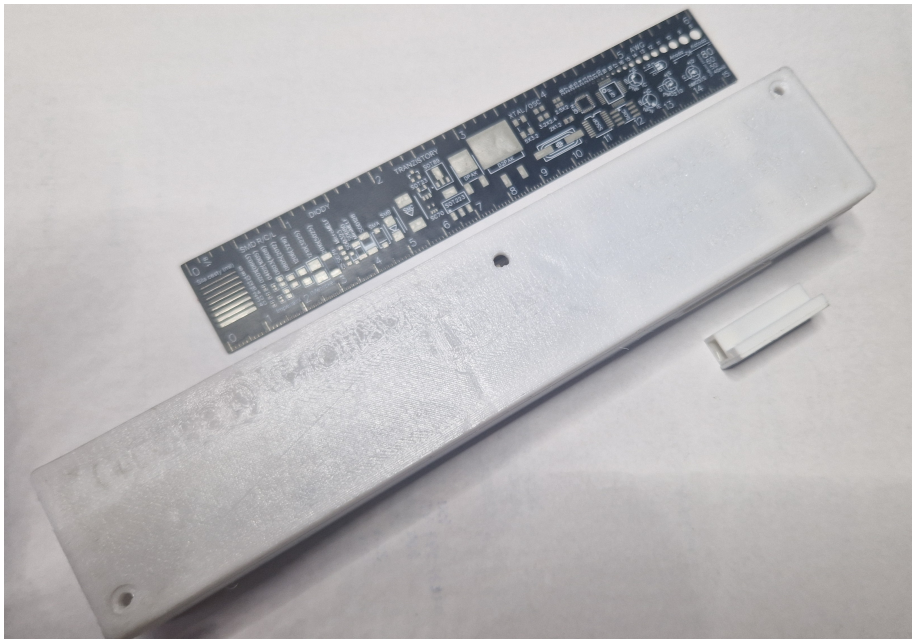
Obr. 3.7: Spodný kryt s NC/NO spínačmi

Uvedenie modulu do prevádzky

Pre uvedenie skompletizovaného modulu do prevádzky je potrebné mať všetky kontakty v pokojovom stave pred pripojením akumulátora. T.j. magnetický rozpínací kontakt musí byť zopnutý a rozpínacie kontakty narušenia - zapojené v sérii musia byť takisto zopnuté. V opačnom prípade budú po zapnutí tieto kontakty deaktivované a zariadenie nebude generovať udalosti na základe týchto kontaktov. Pre upevnenie na rám okna alebo dverí by bolo možné použiť obojstrannú lepiacu pásku. To však nie je vhodné z dôvodu, že by takto pripevnený modul mohol po čase odpadnúť. Pre spoľahlivé uchytenie sa odporúča použiť skrutky do dreva 3x40mm. Na vrchnej strane krytu je otvor, cez ktorý vidieť na indikačnú zelenú LED pre potreby diagnostiky.



Obr. 3.8: Spodný kryt s elektronikou



Obr. 3.9: Skompletizované zariadenie

4 Softvérová časť

Skompletizovaný modul tvorí kľúčovú jednotku systému. Nezaobídeme sa však bez nastavenia siete LoRaWAN. Komunikácia zachytená bránami siete LoRaWAN sa odosiela na príslušný LNS (LoRaWAN Network Server) a to na základe DevEUI a AppEUI. Nakoľko LoRaWAN siete a zvlášť sieť Helium umožňujú prevádzkovanie LNS serverov tretím stranám[10], je potrebné sa s prevádzkovateľom dohodnúť, ktoré DevEUI a AppEUI adresy bude spracovávať príslušný LNS. Táto väzba prebieha pomocou DevAddrs a NwkAddr s Device EUI a App EUI. Smerovaniine prostredníctvom adries DevAddrs a NwkAddr je obdobou smerovacích tabuliek v sieťových prepínačoch alebo smerovačoch. Ako v sieti TTN tak aj Helium je postup užívateľsky pomerne dobre spracovaný. Detailne je popísaný v dokumentácii siete Helium.

4.1 Integrácia v sieti Helium LoRaWAN

Na prístup do konzoly siete Helium je potrebné zaregistrovať účet. Na stránke Helium Console je potrebné zadať e-mailovú adresu alebo prihlásiť sa kontom Google. Ide o testovací balík max 10 zariadení s plnou funkcionalitou.

Počas registrácie konzola žiada o zadanie názvu organizácie. Názov organizácie môže byť ľubovoľný. Viac informácií o organizáciách je možné nájsť na sieti Helium v Dokumentácii.

Pokračujeme nastavením MAC vrstvy 4.1.1 a aplikačnej vrstvy **??**, 4.1.3.

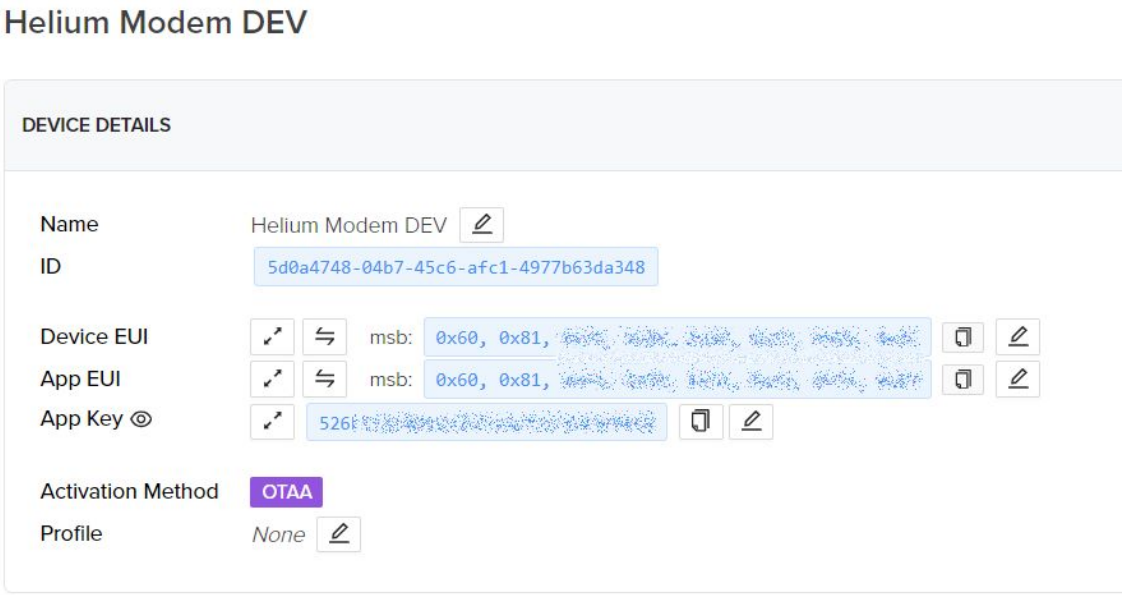
4.1.1 Konzola siete Helium - Pridanie zariadenia

Pridanie zariadenia do MAC vrstvy pozostáva z pridania zariadenia v konzole - Add Device. Ide o zaregistrovanie Device EUI a App EUI, ktoré sa v sieti spárujú s adresou z rozsahu DevAddrs priradenou zariadeniu a organizácii, ktorá prevádzkuje LNS server. Device EUI ani App EUI nemusia byť pre každé zariadenie jedinečné[10].

Informácie získané v konzole Device EUI, App EUI, App Key je potrebné skopírovať do softvéru zariadenia. Pre pridanie zariadenia je potrebné počkať asi 20 minút na propagáciu informácií zadaných v konzole. Rýchle XOR filtre v sieti budú na základe DevAddr, ktoré je asociované s DevEUI a AppEUI, smerovať prevádzku z brán k LNS. AppKey parameter je AES-128 symetrický šifrovavcí kľúč. Používa sa pri generovaní kľúčov NwkSKey a AppSKey. NwkSkey používajú zariadenia v LoRaWan sieti na šifrovanie prenášaných dát a riadiacich príkazov MAC vrstvy a

overenie integrity. AppSKey pozná len aplikačný server a zariadenie siete LoRaWAN a umožňuje zašifrovať prevádzku tak, aby nebola prístupná prevádzkovateľovi siete.[1]

Na obrázku **??** je zobrazená konzola zariadenia v sieti Helium priradená adresa AppEUI a DevEUI spoločne s kryptovacím kľúčom AppKey.

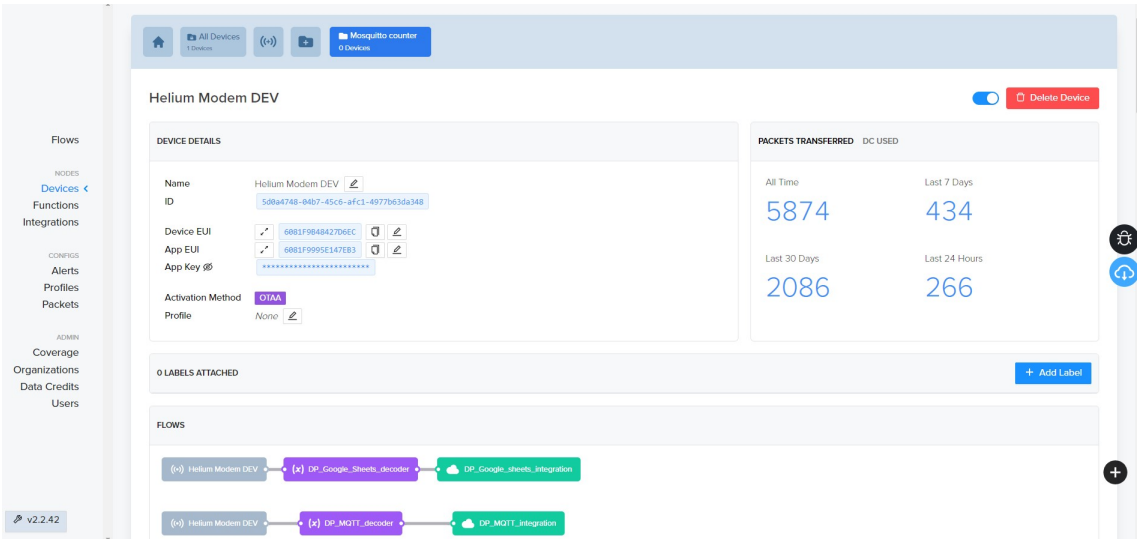


Obr. 4.1: Konzola siete Helium - pridanie zariadenia

4.1.2 Helium Console - Functions

Na prevod paketu alebo rámca siete LoRaWAN využijeme funkciu - „Functions“. Telo paketu môže obsahovať až 24 bajtov a teda 192bitov. Pokiaľ naša aplikácia prenáša známe dáta, najjednoduchším spôsobom je vyhradiť niektoré konkrétne bity resp bajty a pristupovať k nim pomocou polohy jednotlivých bajtov.

```
function Decoder(bytes, port) {
 var decoded = {};
 decoded.batt_mV = ((bytes[0]<<8 |
 (bytes[1]))/1000).toFixed(2);
 decoded.temperature = ((((bytes[2]<<8) |
 bytes[3])/100) - 273.15).toFixed(2);
 decoded.contacts = (bytes[4]);
 decoded.alarms = (bytes[5]);
 return decoded;
}
```



Obr. 4.2: Konzola siete Helium - Device

Pre teplotu bolo možné použiť aj iné možnosti, konvertovať do termodynamickej teploty je výhodné z hľadiska potrebného prenosu minimálneho počtu bitov. Za základ by sa dala použiť aj iná hodnota ako 0K, t.j. -273,15C . V tomto prípade bola však konverzia jednoduchá.

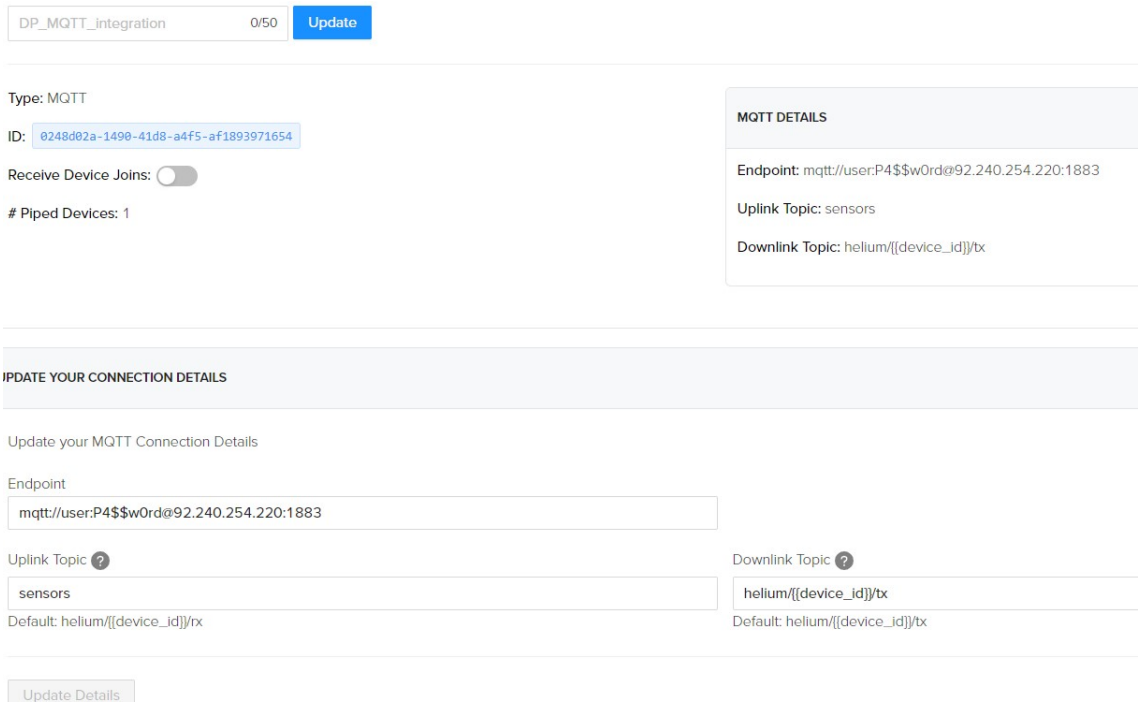
4.1.3 Helium Console - Integrations

Na obrázku 4.2 v spodnej časti je zobrazený tzv. flow. Zobrazuje schému priebehu LoRaWan rámca od zariadenia cez funkciu až po integračné rozhranie. Prvé dva kroky sú popísané vyššie, t.j. device a function. Tretí krok je tzv. integrácia, t.j. informácia o tom čo sa má s dekódovanými JSON dátami urobiť ďalej.

Pre potreby realizácie zabezpečovacieho zariadenia použijeme reťazec pre MQTT integráciu: *mqtt://user:*******@92.240.254.220:1883* Podľa obrázka 4.3, kde namiesto hviezdičiek je potrebné použiť heslo. Takisto Uplink topic, v tomto prípade *Sensors*. Téma(topic) pre downlink nie je využitá.

4.2 Softvér modulu

Kód pre aplikáciu je písaný v jazyku C++/Arduino vo vývojovom prostredí Platformio.



Obr. 4.3: Helium Integrácia MQTT

4.2.1 Voľba siete LoRaWAN

Pre kompiláciu je potrebné zvoliť direktívu `-d HELIUM` alebo `-d TTN` podľa zvolenej siete.

```
#if defined(HELIUM)
static uint8_t devEui[] = { 0x60, 0x81, 0xF9, 0xB4, 0x84, 0x27, 0xD6, 0xEC };
static uint8_t appEui[] = { 0x60, 0x81, 0xF9, 0x99, 0x5E, 0x14, 0x7E, 0xB3 };
static uint8_t appKey[] = { ********************************************** };
#elif(TTN)
static uint8_t devEui[] = { 0x70, 0xB3, 0xD5, 0x7E, 0xD0, 0x04, 0x17, 0x7B };
static uint8_t appEui[] = { 0x70, 0xB3, 0xD5, 0x7E, 0xD0, 0x04, 0x17, 0x7B };
static uint8_t appKey[] = { ********************************************** };
#endif
```

4.2.2 Návrh softvéru pre modul

Softvér pre modul zabezpečuje odosielanie udalostí:

1. Informácie o poplachu - aktivity (či došlo k spojeniu alebo rozpojeniu) v prípade aktivity (zmeny stavu) mechanického spínacieho senzoru
2. Napätie batérie

3. Teplotu
4. Silu signálu pri príjme z predchádzajúcej správy
5. Stav mechanického kontaktu (spojené/rozpojené/aktívny/neaktívny)

4.2.3 Spojenie cez sieť LoraWAN - Helium

Pri programovaní modulu som použil knižnicu Heltec LoraWanMinimal. Pomocou nej a cez LoRa HTCC-AB02A komunikuje cez LoRaWAN sieť Helium s tým, že odosielané dáta pomocou integračnej funkcie konzoly sa zapisujú do časovej databázy influxDB. Popis programu je v prílohe E, pričom jednotlivé sekcie sú okomentované. Okrem toho sú v nasledujúcich odstavcoch popísané hlavné funkcie.

4.2.4 Popis funkcie softvéru

Po zapnutí zariadenia sa aktivuje:

- napájanie periférií Vext
- sériové rozhranie
- zistenie stavov jednotlivých NC kontaktov - neaktívne sa vypnú
- meranie teploty pre odoslanie úvodného uplinku
- sekvencia na pripojenie k sieti LoRaWan, tzv. „JOIN“

Následne sa zapne časovač pre režim hlbokého spánku a nastavia sa povolené prerušenia, ktoré môžu zariadenie „zobudiť“, viď. 3.1.

Hlboký spánok zariadenia prebieha v 60-minútových cykloch. Po uplynutí časovača (3600s) zariadenie:

- zapne napájanie modulu teplomera DS18B20
- odčíta hodnotu teplomera
- odčíta napätie batérie
- pripraví rámec siete LoRaWan
- odošle rámec
- zariadenie sa uvedie do hlbokého spánku

Alarmové kontakty sú riešené ako inicializácia prerušenia a na ich základe sa zavolá funkcia programu pre vybavenie takéhoto prerušenia. V prípade, že v priebehu posledných 10 minút už došlo k narušeniu softvér len inkrementuje počítadlo a pri najbližšom odoslaní LoRaWan paketu odošle aj počet narušení. Po ukončení funkcie sa zariadenie uvedie do režimu hlbokého spánku.

4.2.5 Serverové Aplikácie

V tejto podkapitole sú popísané jednotlivé aplikácie, ktoré boli použité pri príprave riešenia. Všetky aplikácie bežia na virtuálnom stroji s parametrami:

- Vendor ID: GenuineIntel
- 2300MHz / 1 jadro
- 4590 bogomips
- 4GB RAM
- 10GB storage

VPS je Linuxový stroj hostovaný v slovenskom hostingu Exohosting s operačným systémom Ubuntu. VPS a VM sa môžu v tomto texte vyskytovať v ekvivalentnom význame. Na stroji sú nainštalované nasledovné balíky:

- Docker
- MQTT broker
- NodeRED
- InfluxDB
- Grafana
- OpenHAB (docker container)

Pre prístup k VPS je vhodné používať zabezpečené spojenie. Keďže server využíva autor aj na iné účely, je prístup zabezpečený prostredníctvom VPN WireGuard. To umožňuje využívať služby VPS bez potreby aktivovať pre každú službu zvlášť TLS. Nastaveniu VPN sa v tejto práci nebudeme venovať.

Služby vymenované vyššie sú prístupné prostredníctvom web rozhrania nasledovne:

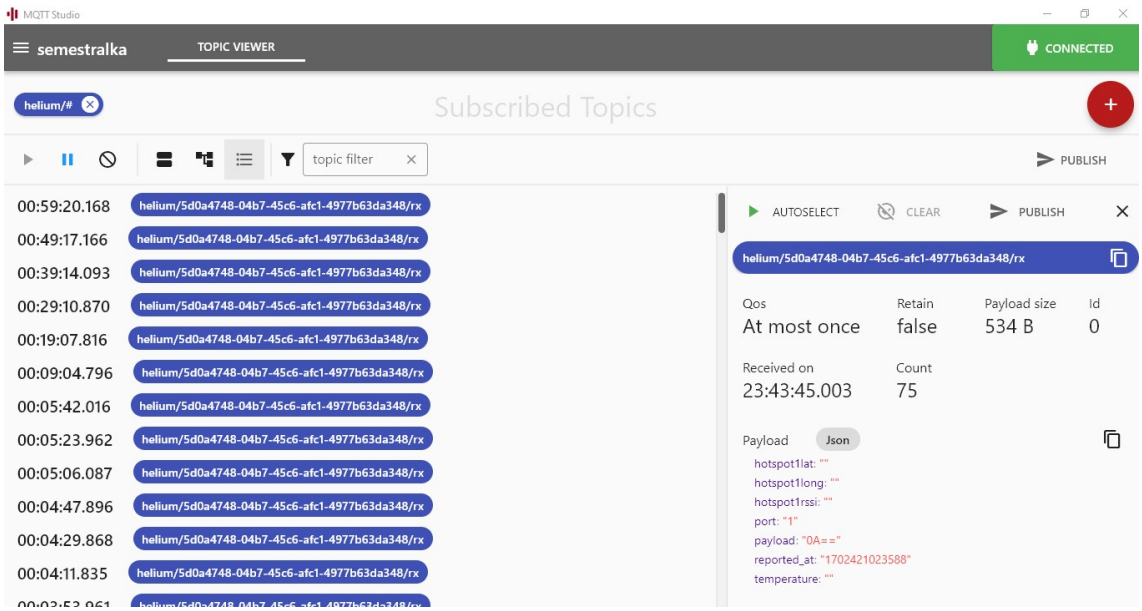
MQTT

MQTT je jednoduchý sieťový protokol na publikovanie a získavanie tém (topics) pre obsluhu front správ. Je navrhnutý pre spojenia so vzdialenými miestami, ktoré majú zariadenia s obmedzenými zdrojmi alebo obmedzenou šírkou pásma siete, ako napríklad IOT senzory. Dáta sú zo siete preposielané pomocou MQTT protokolu do MQTT brokera umiestneného na VPS (Virtual Private Server). V sieti TTN je MQTT broker súčasťou poskytovaného riešenia. V sieti Helium je potrebné nastaviť MQTT integráciu a publikovanie MQTT topics smerovať na samostatný MQTT broker bežiaci na VPS. Viď odstavec Helium Console - Integrations v kapitole 4.1.3

Pre účely testovania sa osvedčil MQTT klient „MQTT Studio“ na zobrazovanie jednotlivých tém. Viď obrázok 4.4.

Príklad správy formátovanej ako JSON z MQTT relácie:

```
{
"devEUI":"6081F9B48427D6EC",
"temp":23.81,
"battery":3.76,
"alarms":0,
```



Obr. 4.4: MQTT Studio

```
"rssi":-115,
"contacts":0,
"rxTime":"12:25:54",
"rxDate":"20. 5.2024",
"rxTs":1716200752325,
"latency":2096,
"topic":
"data",
"timestamp":1716200754421
}
```

Inštalácia MQTT brokera pomocou manažéra balíkov *apt*:

```
$ sudo apt update -y && sudo apt install mosquitto mosquitto-clients -y
```

Po inštalácii preveríme stav v systemctl, najmä či je **loaded** a **active**:

```
$ sudo systemctl status mosquitto
mosquitto.service - Mosquitto MQTT v3.1/v3.1.1 Broker
   Loaded: loaded (/lib/systemd/system/mosquitto.service; enabled;
   vendor preset: enabled)
   Active: active (running) since Mon 2023-10-11 21:59:09 CET; 36min ago
     Docs: man:mosquitto.conf(5)
           man:mosquitto(8)
    ...
```

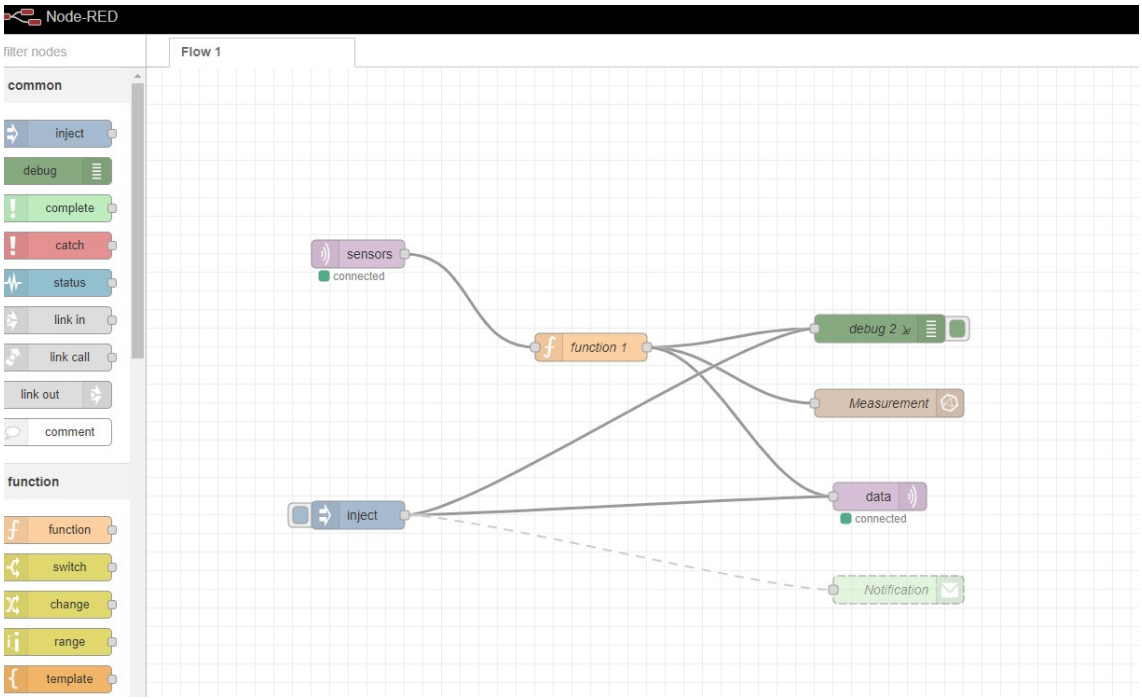
NodeRed

Node-RED je otvorený webový programovací nástroj, ktorý na programovanie aplikácií využíva tzv. flow-based prístup. Ten je založený na tzv. uzloch (nodes), z ktorých každý plní špecifickú funkciu, podľa ktorej spracováva prichádzajúce dáta a odosiela ich do ďalšieho uzla v poradí. Samotné správanie aplikácie potom užívateľ tvorí jednoduchým umiestňovaním a prepojovaním uzlov do tzv. toku (flow). Okrem užívateľskej prívetivosti tento prístup ponúka aj prehľadnosť programov a výrazne uľahčuje riešenie prípadných problémov.

Pred inštaláciou z príkazového riadku je potrebné overiť a prípadne doinštalovať balíky:

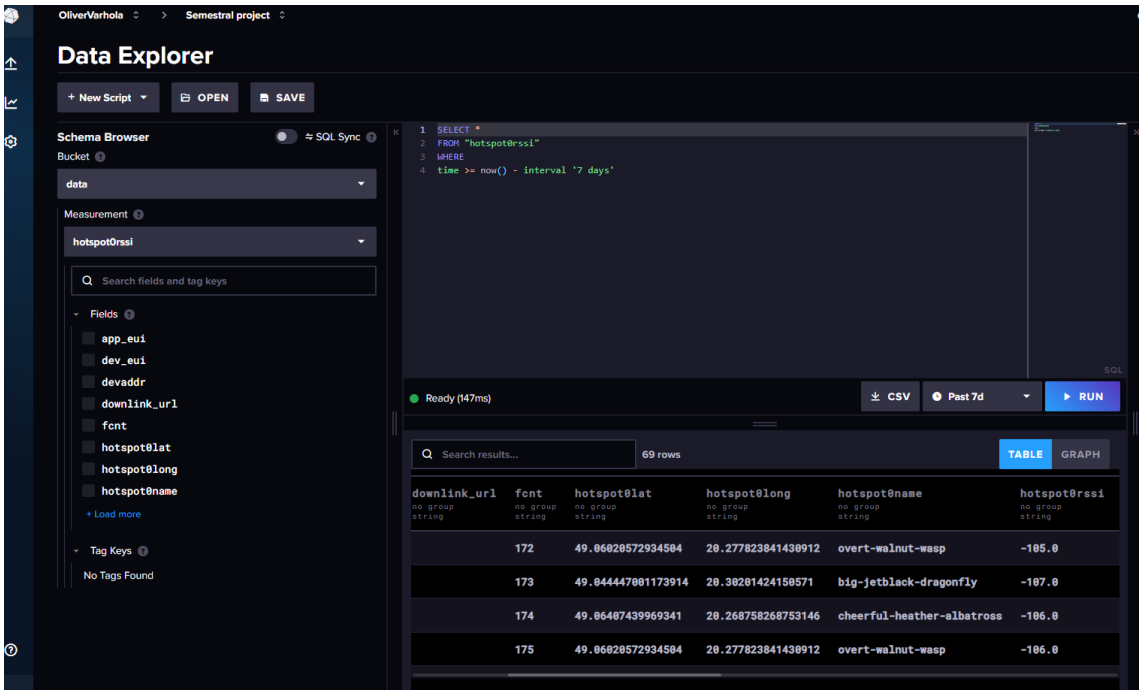
```
$ sudo apt install build-essential git curl
```

Dalej pokračujeme v prehliadači, otvoríme URL: *http://<hostname>:1880/*



Obr. 4.5: NodeRed

NodeRed flow sa skladá z jednotlivých uzlov (nodov), ktoré podľa svojho účelu vykonávajú príslušné akcie. Pre základnú funkcionalitu zostavíme jednoduchý tok (flow) tvorený MQTT, InfluxDB a debug uzlami. Tie medzi sebou poprepájame ako je zobrazené na obrázku 4.5. NodeRed zo senzoru prijíma dáta o teplote, stave batérie a poplachu, ďalej smeruje jednotlivé toky, ukladá dáta do InfluxDB, preposiela do OpenHab-u.



Obr. 4.6: InfluxDB

Prijaté dáta MQTT brokerom sú pomocou Node-Red jednak uložené do InfluxDB 2.0 databázy, tzv "bucket". Ďalej sú tieto dáta zobrazované ako užívateľské grafy pomocou programu Grafana a OpenHAB. Systémy Grafana aj OpenHAB umožňujú zobraziť jednak verejné dáta – teplotu, po zadaní hesla aj ďalšie dáta – stav batérie, stav čidiel, aktivácia/deaktivácia jednotlivých senzorových vstupov.

Nastavenia celého toku sú v elektronickej prílohe J.

Pre nakonfigurovanie uzla InfluxDB je potrebné mať vytvorenú organizáciu v InfluxDB, zásobník (bucket) a API token, čo je poísané v ďalšom odstavci.

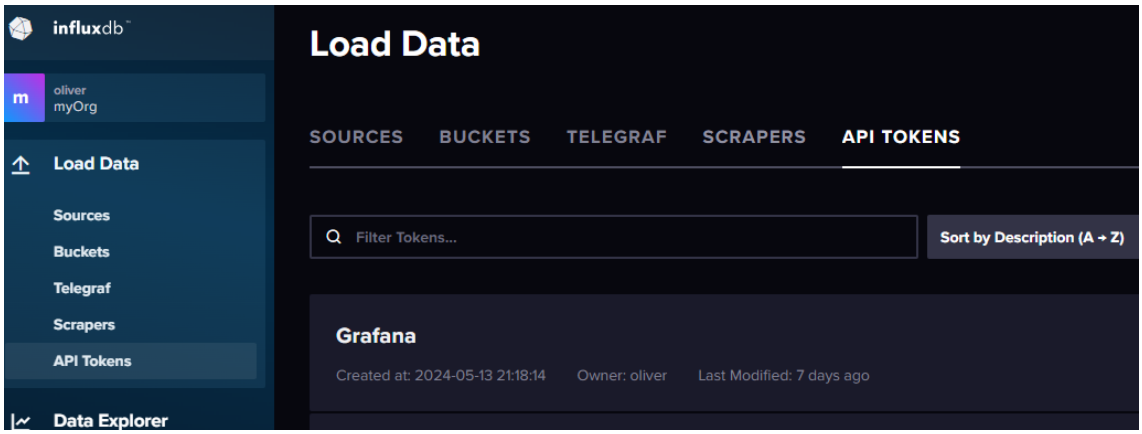
InfluxDB

InfluxDB 4.6 zaznamená dáta odoslané senzorom v konkrétnom momente spolu s časovou značkou. Obrázok nižšie napríklad zobrazuje zaznamenanú silu signálu:

Okrem požadovaných parametrov sú v databáze uložené aj iné premenné. Výhodou Influx databázy napr. Oproti MySQL je, že nie je neyhnutne potrebné nastavovanie jednotlivých tabuliek. Takto napríklad zberáme údaje o latencii, t.j. rozdiele medzi časovými značkammi prijatého paketu zo siete a časovou značkou z NodeRED. InfluxDB zaznamenáva údaje v databáze, ktorej syntax jazyka je obdobný ako pri SQL avšak vždy je informácia o potrebných dátach doplnená časovým obdobím.

Postup pri inštalácii je popísaný v prílohe G.

V InfluxDB je potrebné vygenerovať API tokeny pre jednotlivé aplikácie pristupujúce k dátam a to najmä pre NodeRed, Grafana a OpenHab. Postup je zobrazený



Obr. 4.7: Vygenerovanie API tokenu v InfluxDB

na obrázku 4.8. Pre prístup k zásobníku *sensors* vygenerujeme read-write token pre NodeRed a read-only pre Grafanu.

Grafana

Grafana je open-source platforma, ktorej hlavným účelom je vizualizácia a monitorovanie dát. Ponúka širokú škálu vizualizácií, ako sú grafy, diagramy, tabuľky a iné. V administrátorskom rozhraní aplikácie Grafana je potrebné pridať zdroj dát - Data Sources. Dôležité parametre sú *Organization* - zhoduje sa s údajom v InfluxDB pre daný zásobník (bucket), ku ktorému chceme pristupovať a API Token, ktorý získame postupom uvedeným v predošlej podkapitole a zobrazenom na obrázku **??**.

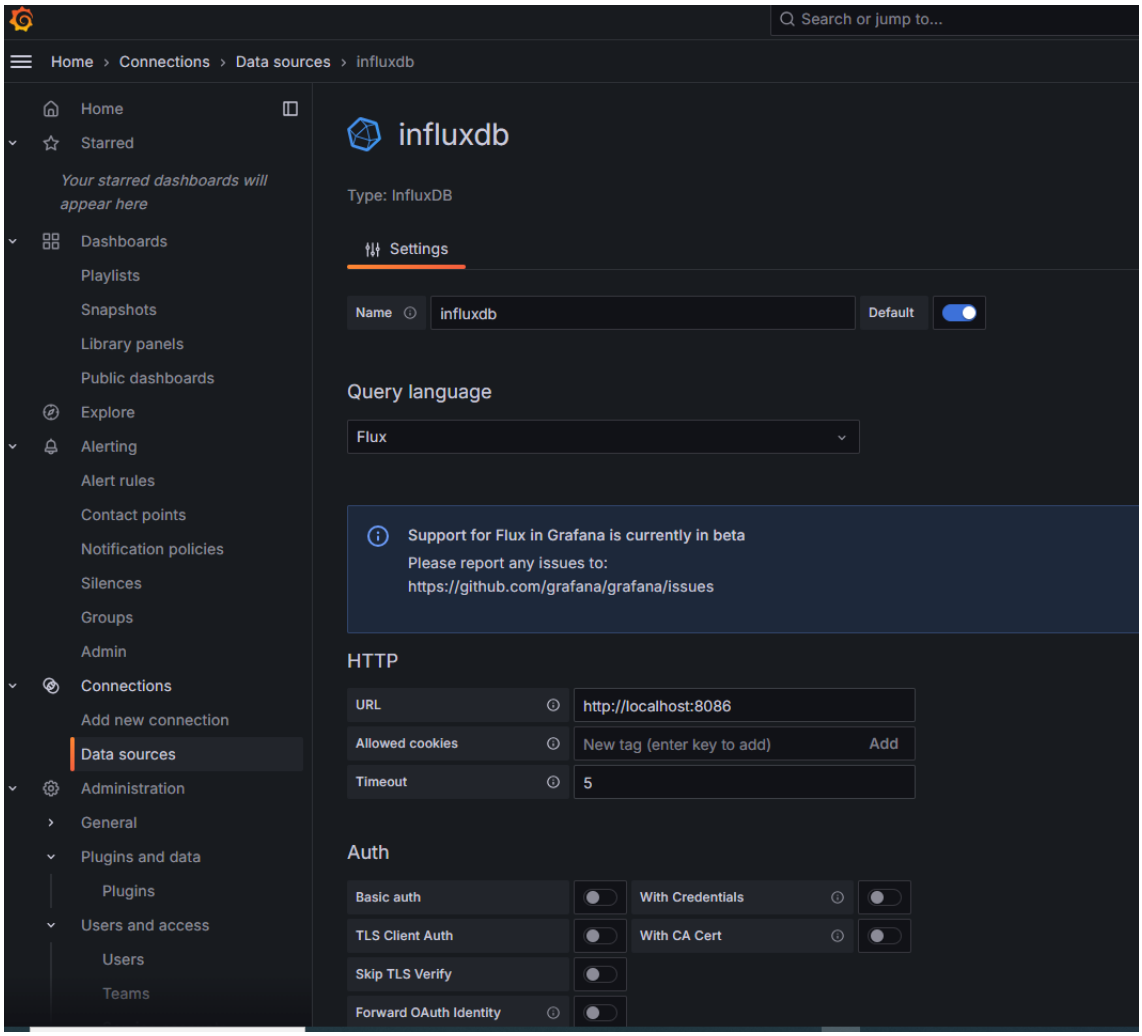
OpenHAB

OpenHAB (**open** **H**ome **A**utomation **B**us) je nástroj na centralizovanú prevádzku inteligentných domov.

openHAB Umožňuje Integrovať ďalšie zariadenia a systémy. Zahŕňa systémy domácej automatizácie, inteligentné zariadenia a ďalšie technológie do jedného riešenia. Poskytuje jednotné používateľské rozhranie a spoločný prístup k pravidlám automatizácie v rámci celého systému bez ohľadu na počet zapojených výrobcov a podsystémov.

OpenHAB využijeme najmä pre potreby notifikácií. Napríklad, notifikácia o vybitej batérii sa odošle na e-mail prostredníctvom skriptu:

```
script: >
        val mailActions = getActions("mail","mail:smtp:5635545a84")
        val success = mailActions.sendMail("xvarho00@vutbr.cz",
        "Battery: " + Security_device_battery.state + "V", "Battery:
```



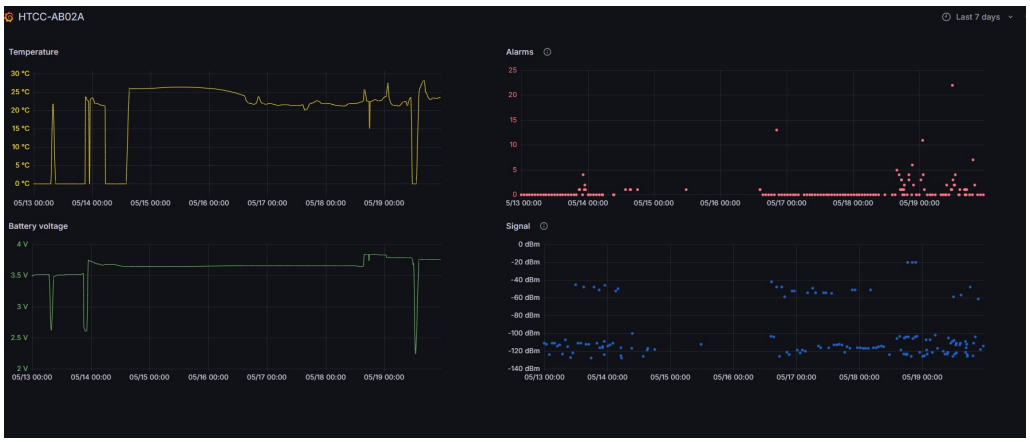
Obr. 4.8: Pridanie Data Source do Grafany

```
    " + Security_device_battery.state + "V")
type: script.ScriptAction
```

4.2.6 Jednotlivé linky pre prístup ku komponentom

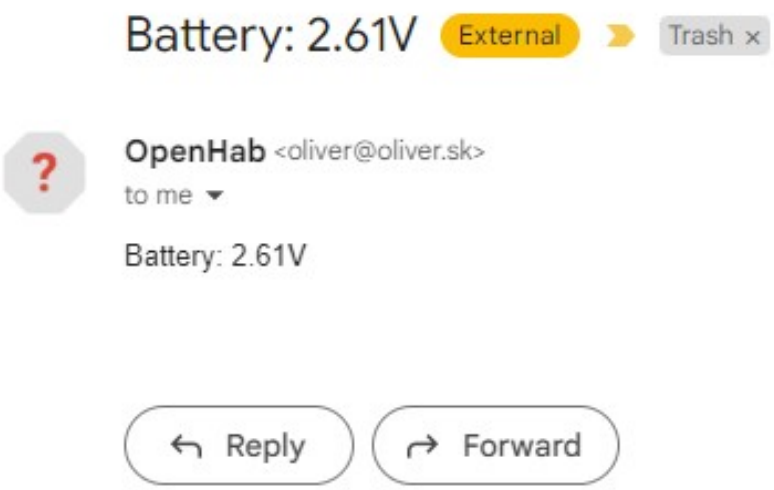
V tejto časti uvádzam všetky linky (URL) na server *dp.oliver.sk*, ktoré sú užívateľskými rozhraniami k jednotlivým aplikáciám. Linky vysádzané hrubým písmom nevyžadujú prihlásenie.

- NodeRed http://dp.oliver.sk:1880/
- InfluxDB http://dp.oliver.sk:8086/
- Grafana (1) http://dp.oliver.sk:3000/
- **Grafana (2) http://dp.oliver.sk:3000/**
- **OpenHab http://dp.oliver.sk:8080/**



Obr. 4.9: Grafana

Obr. 4.10: OpenHAB



Obr. 4.11: E-mail upozorňujúci na nízke napätie batérie

Záver

V záverečnej práci som realizoval praktické zapojenie zabezpečovacieho zariadenia LoRaWAN a spojenie prostredníctvom siete Helium ako aj riešenie aplikačného rozhrania.

Ciele práce boli splnené a zariadenie je plne funkčné. Zariadenie reaguje na alarmové stavy, zaznamenáva ako teplotu tak aj napätie batérie a úroveň signálu posledného prijatého LoRaWAN rámca. V prípade narušenia systém zašle e-mail na nastavenú adresu.

V základnom režime, za predpokladu, že nebude dochádzať k častým narušeniam by kapacita navrhnutej batérie mala postačovať najmenej na 5 rokov. Je potrebné mať na zreteli, že každý alarmový stav je energeticky náročný. Aj s ohľadom na túto vlastnosť je zasielanie správ povolené najčastejšie každých 10 minúut.

V záverečnej práci išlo o navrhnutie koncepcie a neriešil som napríklad hromadné pridávanie zariadení do siete LoRaWAN ani kvalitu používateľskej skúsenosti. Napríklad v prostredí OpenHab by mohol používateľ nastaviť svoju e-mailovú adresu v užívateľsky prívetivom dialógu, kým momentálne je nastavovanie e-mailovej adresy možné len v skripte v časti Settings->Rules. Pre prístup z verejnej siete Internet by bolo vhodné tiež zabezpečiť komunikáciu prostredníctvom TLS s použitím verejnej certifikačnej infraštruktúry.

Prevedenie elektronickej časti obsahuje rozhrania 2 NC a 2 NO kontakty. Na NC kontakty je pripojený magnetický kontakt detegujúci otvorenie dverí a dva mikrospínače detegujúce narušenie krytu senzora, rozhranie pre zabudované teplotné čidlo s protokolom OneWire a ochrana proti prepólovaniu batérie.

V aplikačnej a komunikačnej časti som riešil komplexné nastavenie niekoľkých služieb, ktoré sú potrebné pre realizáciu požiadaviek zadania. Podarilo sa prepojiť a zasielať dáta zo senzora cez LNS server siete Helium na MQTT broker. MQTT broker zabezpečuje distribúciu prijatých dát takmer neobmedzenému počtu klientov z ktorých som realizoval najmä spojenie na NodeRed a odtiaľ do InfluxDB. Spojenie medzi MQTT brokerom, NodeRed a InfluxDB nie je abezpečené protokolom TLS, čo však nevadí, lebo všetky služby bežia na jednom serveri.

Upozornenia a notifikácie sa jednak posielajú cez e-mail a potom aj prostredníctvom OpenHab cloudového riešenia ako push notifikácie na smartfón.

Komunikačná a aplikačná časť je pomerne obsiahla a okrem šiestich kľúčových systémov (Konzola siete Helium, MQTT broker, NodeRed, InfluxDb, Grafana a OpenHab) by bolo možné vymenovať ešte množstvo ďalších, s ktorými systém komunikuje ako napríklad e-mailový systém. Tu by sme samozrejme mohli zájsť do problematiky zabezpečeného odosielania e-mailových správ, autentifikácia prostredníctvom OAUTH, ak by používateľ zamýšľal napríklad využívať službu Gmail pre

odosielanie mailov. Sú to určite nezanedbateľné časti systému avšak bolo nevyhnutné vyriešiť aj mechanickú časť - najmä uchytenie a montáž senzora. Toto som vyriešil návrhom škatuľky v modelovacom 3D programe Fusion 360 a vytlačil na 3D tlačiarni. Vzhľad krabičky má určité rezervy, dôraz som však dával na funkčnosť.

Zariadenie je použiteľné a nasaditeľné všade tam, kde je pokrytie signálom siete LoRaWan a tam kde sú požiadavky používateľa odosielanie stavu magnetického kontaktu a teploty. S malými úpravami môže zabezpečovacie zariadenie slúžiť ako detektor zaplavenia, zadymenia, prípadne je ho možné pripojiť na PIR senzor pre detekciu pohybu. Ide hlavne o aplikácie, ktoré generujú stavový výstup logickej 1 a logickej 0 s napätím 3,3V.

Nespornou výhodou nasadenia zariadenia sú nízke ekonomické náklady. V sieti Helium stojí odoslanie jednej správy za hodinu 1 DC (dátový kredit) $0.00001 USD. V prípade prevádzky bez alarmových stavov je ročný prevádzkový náklad 0,08$, t.j. približne 0,07€ a teda približne dve české koruny ročne. V prípade ak by došlo k alarmu často a zariadenie by vysielalo alarmové stavy každých 10 minút, tak by sa táto suma zvýšila šesťnásobne a predstavovala by 12 Kč ročne.

Uplatnenie zabezpečovacieho zariadenia je najmä v domácnostiach, firmách, školstve ale aj v priemysle a ochrane prírody. S ohľadom na prenositeľnosť zariadenia je možné ho nasadiť na miestach kde sa vyžaduje zabezpečenie priestorov alebo vstupov avšak ešte chýba potrebná infraštruktúra.

Literatúra

[1] „LoRaWAN Security“. In: *LoRaWAN Specification, v1.0.2, July 2016 LoRa-Alliance* (2016). URL: https://lora-alliance.org/wp-content/uploads/2020/11/lorawan_security_whitepaper.pdf.

[2] Massimo Ballerini et al. „NB-IoT vs. LoRaWAN: An Experimental Evaluation for Industrial Applications“. In: *IEEE Transactions on Industrial Informatics* PP (apr. 2020), s. 1–1. DOI: 10.1109/TII.2020.2987423. (Cit. 10. 11. 2023).

[3] Ningning Hou, Xianjin Xia a Yuanqing Zheng. „Jamming of LoRa PHY and Countermeasure“. In: (2021), s. 1–10. DOI: 10.1109/INFOCOM42981.2021.9488774. (Cit. 25. 11. 2023).

[4] Gabriela Morillo, Utz Roedig a Dirk Pesch. *Anomaly detection in narrowband internet of things*. 2021. URL: https://www.advance-crt.ie/wp-content/uploads/2022/10/Gabriela_Morillo_Colloquium_2022.pdf (cit. 25. 11. 2023).

[5] Ningning Hou, Xianjin Xia a Yuanqing Zheng. „Jamming of LoRa PHY and Countermeasure“. In: *ACM Trans. Sen. Netw.* 19.4 (máj 2023). ISSN: 1550-4859. DOI: 10.1145/3583137. URL: https://doi.org/10.1145/3583137 (cit. 25. 11. 2023).

[6] Gabriela Morillo, Utz Roedig a Dirk Pesch. *Detecting targeted interference in NB-IoT*. 2023.

[7] Andrew Allen. *Mapping the World with Hexagons*. URL: https://blog.helium.com/mapping-the-world-with-hexagons-49f57d8b3df5 (cit. 04. 12. 2023).

[8] Heltec Automation. *LoRa Development Board*. URL: https://resource.heltec.cn/download/CubeCell/HTCC-AB02A/AB02A.pdf (cit. 10. 12. 2023).

[9] *Helium Foundation's CEO discussed DePIN and Helium's evolution*. URL: https://cryptotvplus.com/2023/11/helium-foundations-ceo-discussed-depin-and-heliums-evolution/ (cit. 25. 11. 2023).

[10] *LoRaWAN On Helium*. URL: https://docs.helium.com/iot/lorawan-on-helium/ (cit. 04. 05. 2024).

[11] Anne-Françoise Pelé. *Why did Sigfox file for Bankruptcy protection? (02/2022)*. URL: https://www.eetimes.eu/iot-startup-sigfox-seeks-a-buyer/ (cit. 10. 11. 2023).

[12] *The Power of DePIN: Helium Network and Mycelium Testbed*. URL: https://blog.helium.com/the-power-of-depin-helium-network-and-mycelium-testbed-1d3521d8bb1f (cit. 25. 11. 2023).

Zoznam príloh

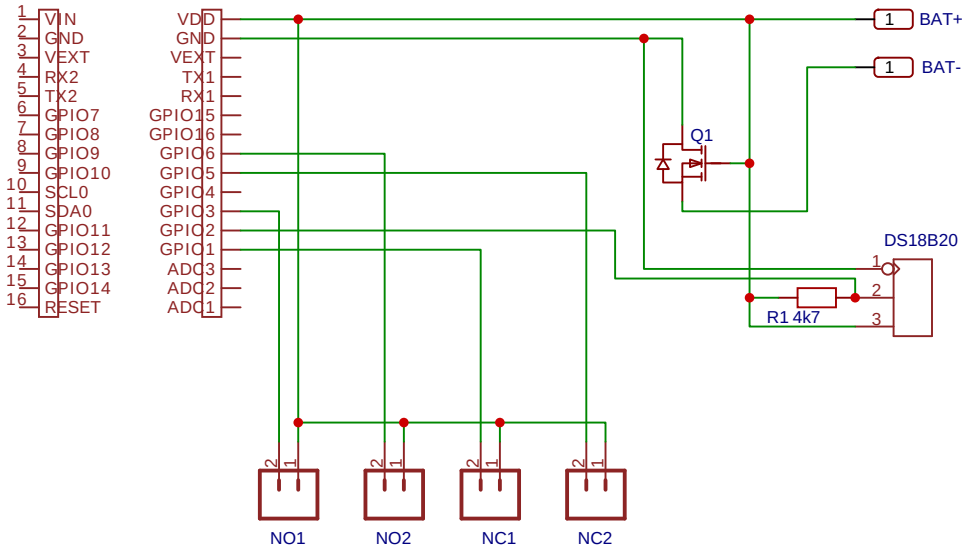
A 3D krabička

Viď elektronická príloha

B 3D tlačiareň - nastavenie

Viď elektronická príloha

C Schéma zapojenia



TITLE: Úsporné zabezpečovací za 권zení LoRaWan		REV: 1.0
EasyEDA	Company: VUT FEKT	Sheet: 1/1
	Date: 2024-05-05 Drawn By: Oliver Varhola	

D Súbory pre výrobu DPS - Gerber

Viď elektronická príloha

E Program

Viď elektronická príloha

F MQTT broker

Okrem štandardných sú podstatné tieto nastavenia:

```
per_listener_settings true

listener 1883 127.0.0.1
allow_anonymous true

listener 1883 10.10.0.1
allow_anonymous false
password_file /etc/mosquitto/pwfile

listener 1883 92.240.254.220
allow_anonymous false
password_file /etc/mosquitto/pwfile
```

Konfiguračný súbor `/etc/mosquitto/mosquitto.conf` v elektronickej prílohe.

G Inštalácia InfluxDB

Postup podľa návodu: *https://docs.influxdata.com/influxdb/v2/install/*

```
# influxdata-archive_compat.key GPG fingerprint:
#     9D53 9D90 D332 8DC7 D6C8 D3B9 D8FF 8E1F 7DF8 B07E
wget -q https://repos.influxdata.com/influxdata-archive_compat.key
echo '393e8779c89ac8d958f81f942f9ad7fb82a25e133faddaf92e15b16e6ac9ce4c␣i
echo 'deb␣[signed-by=/etc/apt/trusted.gpg.d/influxdata-archive_compat.gp

sudo apt-get update && sudo apt-get install influxdb2
```

/etc/influxdb/config.toml

```
bolt-path = "/var/lib/influxdb/influxd.bolt"
engine-path = "/var/lib/influxdb/engine"
```

H Grafana

Viď elektronická príloha

I OpenHAB (docker container)

Postup inštalácie podľa https://www.openhab.org/docs/installation/docker.html

J Node-RED flow

Viď elektronická príloha