

ZÁPADOČESKÁ UNIVERZITA V PLZNI
FAKULTA ELEKTROTECHNICKÁ

KATEDRA ELEKTRONIKY A INFORMAČNÍCH TECHNOLOGIÍ

DIPOMOVÁ PRÁCE

Autonomní bezdrátová síť sensorů

vedoucí práce: Ing. Jan Mráz, Ph.D.

autor: Bc. David Ježek

2020/2021

ZÁPADOČESKÁ UNIVERZITA V PLZNI

Fakulta elektrotechnická

Akademický rok: 2020/2021

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

| | |
|-------------------|-------------------------------------------------------|
| Jméno a příjmení: | Bc. David JEŽEK |
| Osobní číslo: | E19N0061P |
| Studijní program: | N2612 Elektrotechnika a informatika |
| Studijní obor: | Elektronika a aplikovaná informatika |
| Téma práce: | Autonomní bezdrátová síť senzorů |
| Zadávací katedra: | Katedra elektroniky a informačních technologií |

Zásady pro vypracování

Poznejte fungování protokolů internetu věcí a aplikujte jej spolu se znalostmi elektroniky na návrh autonomní senzorické sítě.

1. Seznamte se s principy fungování internetu věcí, diskutujte vlastnosti protokolů LoRaWAN, Weightless, případně dalších.
2. Navrhněte senzorickou síť dle požadavků AKKA Czech Republic s.r.o. s využitím vybraného protokolu.
3. Zrealizujte síť s vybranými senzory na vybrané platformě mikrokontrolérů.
4. Připravte dokumentaci navrženého hardwarového a softwarového řešení.

Rozsah diplomové práce: **40 – 60 stran**
Rozsah grafických prací: **podle doporučení vedoucího**
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. Internet of Things for architects : architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security / Perry Lea. – Birmingham : Packt Publishing, 2018.
2. IoT fundamentals : networking technologies, protocols, and use cases for the internet of things / David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Robert Barton, Jerome Henry. – Indianapolis, Cisco Press [2017].

Vedoucí diplomové práce: **Ing. Jan Mráz, Ph.D.**
Katedra elektroniky a informačních technologií

Datum zadání diplomové práce: **9. října 2020**
Termín odevzdání diplomové práce: **27. května 2021**


Prof. Ing. Zdeněk Peroutka, Ph.D.
děkan

LS.


Doc. Ing. Jiří Hammerbauer, Ph.D.
vedoucí katedry

V Pízní dne 9. října 2020

Abstrakt

Předkládaná diplomová práce nabízí návrh autonomní bezdrátové sítě senzorů. První část shrnuje různé technologie a protokoly, které využívá internet věcí. V další části je pak rozebrané samotné hardwarové a softwarové řešení sítě. Na závěr je shrnuto splnění jednotlivých bodů zadání.

Klíčová slova

Internet věcí, LoRa, LoRaWAN, GPS, gyroskop, akcelerometr, síť, STM32, bezdrátový přenos.

Abstract

This thesis offers a design of an autonomous wireless sensor network. The first part summarizes the various technologies and protocols used by the Internet of Things. In the next section, the hardware and software solution of the network itself is dismantled. Finally, the fulfilment of the individual award points is summarised.

Key words

Internet of Things, LoRa, LoRaWAN, GPS, gyroscope, accelerometer, network, STM32, wireless transmission.

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně, s použitím odborné literatury a pramenů uvedených v seznamu, který je součástí této diplomové práce.

Dále prohlašuji, že veškerý software, použitý při řešení této bakalářské/diplomové práce, je legální.

.....

podpis

V Plzni dne 25.5.2021

David Ježek

Poděkování

Tímto bych rád poděkoval vedoucímu diplomové práce Ing. Jan Mráz, Ph.D. za cenné rady, připomínky a metodické vedení této práce.

Obsah

| | |
|------------------------------------------------------|----------------------------------------|
| OBSAH..... | 8 |
| SEZNAM SYMBOLŮ A ZKRATEK..... | 9 |
| ÚVOD..... | 10 |
| 1 INTERNET VĚCÍ..... | 11 |
| 1.1 POUŽÍVANÉ PROTOKOLY..... | 11 |
| 1.1.1 Dělení dle vzdálenosti přenosu dat..... | 11 |
| 1.1.2 Dělení dle využívané frekvenční oblasti..... | 13 |
| 1.2 TOPOLOGIE IOT SÍTÍ..... | 15 |
| 1.3 LORAWAN..... | CHYBA! ZÁLOŽKA NENÍ DEFINOVÁNA. |
| 1.3.1 Fyzická vrstva..... | 17 |
| 1.3.2 Vrstva MAC..... | 18 |
| 1.3.3 Topologie..... | 20 |
| 1.3.4 Bezpečnost..... | 20 |
| 1.4 SIGFOX..... | 21 |
| 1.4.1 Fyzická vrstva Sigfox..... | 22 |
| 1.4.2 Sigfox MAC vrstva..... | 22 |
| 1.4.3 Topologie Sigfox..... | 23 |
| 1.5 WEIGHTLESS..... | 24 |
| 1.5.1 Weightless-W..... | 24 |
| 1.5.2 Weightless-N..... | 24 |
| 1.5.3 Weightless-P..... | 25 |
| 1.5.4 Vlastnosti Weightless..... | 25 |
| 1.6 SROVNÁNÍ..... | 26 |
| 2 VLASTNÍ ŘEŠENÍ..... | 27 |
| 2.1 ZVOLENÝ HARDWARE..... | 27 |
| 2.1.1 Mikrokontroler STM32F767ZI..... | 27 |
| 2.1.2 GPS modul NEO-6M..... | 28 |
| 2.1.3 Gyroskop a akcelerometr MPU6050..... | 29 |
| 2.1.4 Modul USI WM-SG-SM-42 (I-NUCLEO-LRWANI)..... | 30 |
| 2.1.5 Brána Dragino LG01-N..... | 31 |
| 2.1.6 Propojovací modul..... | 32 |
| 2.2 PROGRAMOVÁ ČÁST..... | 33 |
| 2.2.1 Program mikrokontroleru..... | 34 |
| 2.2.2 Nastavení brány Dragino LG01-N..... | 36 |
| 2.2.3 Program pro příjem a vizualizaci dat v PC..... | 38 |
| 3 OVĚŘENÍ VÝSLEDKŮ..... | 39 |
| 4 ZÁVĚR..... | 42 |
| SEZNAM LITERATURY A INFORMAČNÍCH ZDROJŮ..... | 1 |

Seznam symbolů a zkratek

| | | |
|--------|---------------------------------------------------------------|----------------------------------------------------------|
| IoT | Internet of Things | Internet věcí |
| PAN | Personal Area Network | Osobní síť |
| HAN | Home Area Network | Domácí síť |
| NAN | Neighborhood Area Network | Sousedská síť |
| FAN | Field Area Network | Polní síť |
| LAN | Local Area Network | Lokální síť |
| RF | Radio Frequency | Rádiový kmitočet |
| WPAN | Wireless Personal Area Network | Bezdrátová osobní síť |
| LPWAN | Low-Power Wide Area Network | Nízkoenergetická síť s dlouhým dosahem |
| ISM | Industrial, Scientific and Medical | Průmyslové, vědecké a zdravotnické pásmo |
| RFD | Reduced Function Device | Zařízení s omezenou funkcí |
| FFD | Full Function Device | Zařízení s plnou funkcí |
| ADR | Adaptive Data-Rate | Adaptivní datová rychlost |
| SF | Spreading Factor | Rozptylový faktor |
| MAC | Media Access Control | Řízení přístupu k médiu |
| OTA | Over The Air | Bezdrátový přenos |
| UNB | Ultra Narrowband | Ultra úzké pásmo |
| OSSS | Orthogonal Sequence Spread Spectrum | Rozprostřené spektrum ortogonální sekvencí |
| MEMS | Micro Electro Mechanical Systems | Mikroelektromechanické systémy |
| CRC | Cyclic Redundancy Check | Cyklický redundantní součet |
| TVWS | TV Whitespace | Bílá místa v televizním spektru |
| GMSK | Gaussian Minimum Shift Keying | Gaussovo Klíčování s minimálním zdvihem |
| GFSK | Gaussian Frequency Shift Keying | Gaussovo Klíčování Frekvenčním zdvihem |
| BPSK | Binary-Phase Shift Keying | Klíčování binárním fázovým posuvem |
| DDC | Display Data Channel | Kanál pro data displeje |
| I2C | Two Wire Interface | Dvoudrátové rozhraní |
| RFTDMA | Random Frequency Time Division Multiple Access | Náhodný vícenásobný přístup s frekvenčním dělením v čase |
| EEPROM | Electrically Erasable Programmable Read-Only Memory | Elektricky Vymazatelná Paměť pouze pro čtení |
| UART | Universal asynchronous receiver-transmitter | Univerzální asynchronní přijímač-vysílač |
| USART | Universal Synchronous / Asynchronous Receiver and Transmitter | Univerzální synchronní/asynchronní přijímač-vysílač |
| SDRAM | Synchronous Dynamic Random Access Memory | Synchronní dynamická paměť s náhodným přístupem |

Úvod

V dnešní době je pojem IoT velmi často používán a tato zařízení jsou čím dál častěji implementována do každodenního života, a to hlavně díky jejich vlastnostem, jako je nízká spotřeba a velké dosahy bezdrátových sensorů. Z těchto důvodů jsou použity IoT protokoly i pro tuto práci. Tato práce je vypracována za účelem bližšího seznámení s technickým řešením bezdrátových sensorů na dlouhé dosahy. Cílem diplomové práce je vytvoření bezdrátové sítě sensorů. Především se jedná o sensor polohy, gyroskop a akcelerometr s dosahem jednotek kilometrů. Tato síť sensorů má být nezávislá na ostatních již existujících sítích. Práce se nejdříve zabývá používanými protokoly v IoT. Následuje popis použitého hardwaru a vytvořeného softwaru. Výsledky jsou shrnuty v závěru.

1 Internet věcí

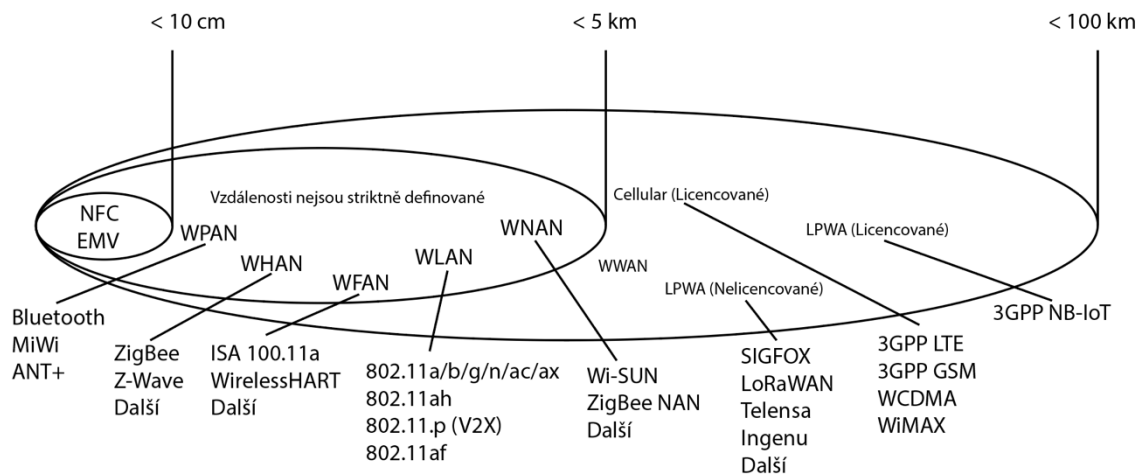
Za zrod internetu věcí se často považuje období, kdy počet připojených zařízení do internetu převýšil počet lidí na planetě. To se stalo mezi roky 2008 a 2009. Osobou, které se připisuje vymyšlení výrazu „Internet of Things“, je Kevin Ashton. Ten v roce 1999 pracoval pro společnost Procter & Gamble, a použil tuto frázi k vysvětlení nové myšlenky související s propojením dodavatelského řetězce společnosti s internetem. Cílem internetu věcí, v angličtině „Internet of Things“ (IoT) je připojit všechna běžně používaná zařízení do internetu, tak, aby spolu všechna tato zařízení mohla komunikovat a vyměňovat data. V budoucnu by se mohlo jednat například o drony s autopilotem, které by samy doručovaly zásilky a mohly by se například rozhodovat, zda je vhodné roznášet, podle dat z meteorologické stanice. Dále by se mohlo jednat o sensory v našem oblečení pro monitorování a odesílání zdravotních dat například do nemocnic. Dá se tedy říci, že hlavním cílem IoT je „připojit nepřipojené“. Tím je myšleno připojit do internetu zařízení, která zatím nejsou připojena. Připojením více zařízení, která budou schopna komunikovat s okolním světem, dalšími zařízeními a lidmi, docílíme větší propojenosti fyzického světa a počítačů. To nám dovolí zvýšení efektivity, přesnosti, automatizaci pokročilejších aplikací. Spíše než pohlížet na IoT jako na jedinou technologickou doménu je lepší se na tuto problematiku koukat jako na spojení různých koncepcí, protokolů a technologií. Co se konkrétně použije, je vždy závislé na místě a způsobu využití daného zařízení. [1]

1.1 Používané protokoly

Existuje přímý vztah mezi technologií IoT sítě a typem topologie sítě, kterou tato technologie umožňuje. Každá z těchto komunikačních technologií byla navržena na určitý typ použití. Rozhodující otázky jsou, co připojit, kde připojit, kolik dat v jakém intervalu budeme přenášet a na jakou vzdálenost je budeme přenášet. Tyto otázky a podmínky určily nejvhodnější frekvenční pásmo a strukturu rámce dat pro daný případ použití. [1]

1.1.1 Dělení dle vzdálenosti přenosu dat

Klíčovým parametrem při volbě technologie přenosu je vzdálenost mezi senzorem a bránou, která data přijímá a zpracovává. Obrázek 1 uvádí některé přístupové technologie vzhledem k přenosové vzdálenosti, se kterými se můžeme v IoT setkat. [1]



Obrázek 1 - Závislost přístupové technologie na vzdálenosti přenosu podle zdroje [1]

Rozsahy na obrázku 1 jsou inkuzivní. Například mobilní data jsou znázorněna na vzdálenost nad 5 km, ale fungují i na vzdálenost 100 m. Oproti tomu ZigBee bude efektivní na vzdálenost několik desítek metrů, ale nebude fungovat na vzdálenost jednotek kilometrů. Odhady vzdáleností jsou seskupeny podle názvů kategorií sítě, které ilustrují prostředí, kde se očekává přenos dat. [1]

- PAN (Personal Area Network neboli osobní síť) – Jedná se o osobní prostor kolem člověka s dosahem několik metrů. Běžnou bezdrátovou technologií pro tuto síť je Bluetooth.
- HAN (Home Area Network neboli domácí síť) – Dosah několika desítek metrů. Běžnou IoT technologií pro tuto síť je ZigBee a Bluetooth Low Energy.
- NAN (Neighborhood Area Network neboli sousedská síť) – Dosah několika stovek metrů. Termín NAN se často používá k označení sítě HAN jednotek, ze kterých jsou shromažďována data.
- FAN (Field Area Network neboli polní síť) – Dosah od desítek do stovek metrů. Jedná se o otevřený prostor, někdy je vnímán jako skupina NAN sítí.
- LAN (Local Area Network neboli místní síť) – Dosah až 100 metrů. Pro tuto síť je běžné použití Ethernetu nebo IEEE 802.11.

Před každý typ sítě se dá v IoT přidat písmeno „W“, které značí bezdrátovou technologii pro přenos dat. Každý protokol využívá specifický formát rámce dat a techniku přenosu na určité frekvenci nebo frekvenčním pásmu. Každý z protokolů má také jinou závislost

vzdálenosti a datové propustnosti. S rostoucí vzdáleností klesá datová propustnost každého protokolu jiným způsobem. U některého klesá s velkou strmostí a u jiného lze pozorovat mírný pokles datové propustnosti vzhledem ke vzdálenosti. Zvýšením dosahu a datové propustnosti zvyšujeme i spotřebu energie. [1]

Dále můžeme přístupové technologie kategorizovat dle rozsahu takto. Krátký dosah, tento rozsah se pohybuje v desítkách metrů maximální vzdálenosti mezi dvěma zařízeními. Příklady bezdrátových technologií krátkého dosahu jsou IEEE 802.15.1 Bluetooth a IEEE 802.15.7 Visible Light Communications (VLC). Tyto komunikační metody krátkého dosahu se nacházejí pouze u menšiny instalací IoT. [1] [2]

Střední dosah, tento rozsah je jednou z často využívaných kategorií přístupových technologií IoT. V rozsahu desítek až stovek metrů je k dispozici mnoho specifikací a implementací. Maximální vzdálenost mezi dvěma zařízeními je obvykle menší než 1 kilometr. Mezi příklady bezdrátových technologií středního dosahu patří IEEE 802.11 Wi-Fi, IEEE 802.15.4 a 802.15.4 g WPAN. [1]

Dlouhý dosah, vzdálenost mezi dvěma zařízeními, která je větší než 1 kilometr, vyžaduje technologie dlouhého dosahu. Příkladem bezdrátového připojení jsou mobilní sítě (2G, 3G, 4G) a některé aplikace venkovních technologií IEEE 802.11 Wi-Fi a Low-Power Wide-Area (LPWA). Komunikace LPWA má schopnost komunikovat na velké ploše bez velké spotřeby energie. Tyto technologie jsou proto ideální pro senzory IoT napájené z baterie. [1]

1.1.2 Dělení dle využívané frekvenční oblasti

Rádiové spektrum je regulováno zeměmi a organizacemi. Tyto skupiny definují předpisy a požadavky na přenos pro různá frekvenční pásma. Například části spektra jsou přiděleny telekomunikacím, jako je rozhlas, televize, armáda atd. Zaměřením na přístupové technologie IoT jsou frekvenční pásma rozdělena mezi licencovaná a nelicencovaná pásma.

Licencované spektrum je obecně použitelné pro IoT technologie s dlouhým dosahem a přidělení komunikačních spekter řídí poskytovatelé služeb, veřejné služby jako zdravotnictví a armáda. Důležitým hlediskem pro IoT infrastruktury, které chtějí využívat licencované spektrum, je to, že uživatelé si musí před připojením svých zařízení předplatit využívání

těchto spekter. To zvyšuje složitost a cenu nasazení velkého počtu senzorů a dalších zařízení IoT, ale výměnou za to může provozovatel sítě zaručit exkluzivitu využití frekvence v cílové oblasti, a proto může nabízet lepší záruku služeb. [1] [2]

Telekomunikační společnosti také definují nelicencované spektrum pro průmyslové, vědecké a lékařské využití, jedná se o ISM pásma. Tyto frekvence se používají v mnoha komunikačních technologiích pro zařízení krátkého dosahu. Označení „bez licence“ znamená, že v těchto pásmech nejsou poskytovány žádné záruky ani ochrany proti rušení komunikace. Pro IoT jsou to nejčastěji pásma 2,4 GHz využívané IEEE 802.11 b/g/n Wi-Fi, IEEE 802.15.1 Bluetooth a IEEE 802.15.4 WPAN. Nelicencované pásmo není neregulované. Pro každé z přidělených kmitočtových pásem existují národní a regionální předpisy stejně jako u licencovaných pásem. Tyto předpisy nařizují parametry zařízení, jako je vysílací výkon, pracovní cyklus a doba prodlevy, šířka pásma kanálu a přeskokování kanálu. Některé komunikace v pásmech ISM pracují v rozsahu pod GHz. Tato pásma používají protokoly jako IEEE 802.15.4, 802.15.4 g a 802.11ah a technologie jako LoRa a Sigfox. [1] [2]

Frekvence přenosu přímo ovlivňuje, jak se signál šíří, a jeho praktický maximální dosah. U vnitřních nebo venkovních rozmístění umožňují frekvenční pásma pod GHz větší vzdálenosti mezi zařízeními. Tato pásma mají lepší schopnost pronikat do infrastruktur budov nebo obcházet překážky, přičemž udržují nižší vysílací výkon v rámci regulace než pásmo 2,4 GHz. Nevýhodou frekvenčních pásem pod 1 GHz je jejich nižší rychlost přenosu dat ve srovnání s vyššími frekvencemi. Většina senzorů IoT však nemusí odesílat data vysokou rychlostí. Například ve většině evropských zemí je pásmo 169 MHz často považováno za nejvhodnější pro bezdrátové aplikace měření vody a plynu. To je způsobeno jeho dobrým, hlubokým pronikáním signálu do budovy. Nízká datová rychlost této frekvence navíc odpovídá malému objemu dat, která je třeba přenášet. [1] [2]

V pásmu ISM bylo definováno několik rozsahů. Nejznámější rozsahy jsou soustředěny na 169 MHz, 433 MHz, 868 MHz a 915 MHz. Většina přístupových technologií IoT má však tendenci zaměřovat se na dvě frekvenční oblasti, a to kolem 868 MHz a 915 MHz. Tato hlavní pásma se běžně vyskytují po celém světě a jsou použitelná téměř ve všech zemích. Stručně řečeno, při implementaci nebo nasazení inteligentních objektů IoT je nutné vzít v úvahu frekvence a odpovídající předpisy dané země. Zařízení běžící v nelicencovaných

pásmech lze snadno optimalizovat, pokud jde o hardware podporující dvě hlavní celosvětové frekvence, 868 MHz a 915 MHz. Parametry, jako je vysílací výkon antény však musí být řádně navrženy tak, aby vyhovovaly nastavením požadovaným předpisům jednotlivých zemí. [1] [2]

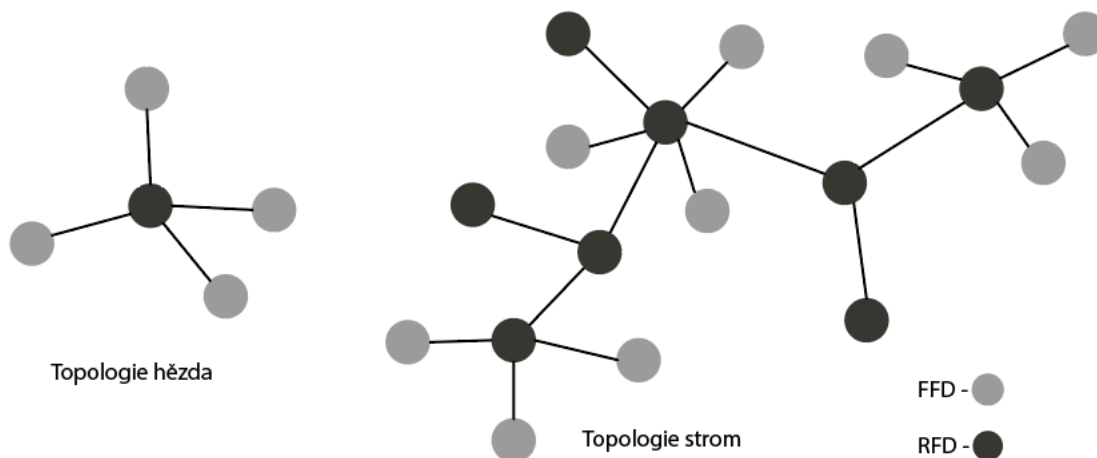
1.2 Topologie IoT sítí

Některé protokoly nabízejí flexibilní strukturu připojení pro rozšíření možností komunikace. Point-to-point topologie umožňuje jednomu bodu komunikovat s jiným bodem. Tato topologie v nejpřísnějším smyslu, tedy pouze dvě zařízení se v IoT nevyužívá jelikož by to znamenalo, že by jeden objekt mohl komunikovat pouze s jedním jiným objektem. Několik technologií se však označuje jako point-to-point, každý objekt vytvoří individuální relaci s bránou. Koncept point-to-point v takovém případě odkazuje spíše na komunikační strukturu než na fyzickou topologii sítě. [1] [2]

Topologie typu point-to-multipoint umožňuje jednomu bodu komunikovat s více než jedním dalším bodem sítě. Většina IoT technologií, funguje tak, že jedna nebo více bran komunikuje s více inteligentními sensory. Zvláštností v IoT sítích je, že některé uzly, například sensory, podporují jak funkce příjmu dat, tak odesílání, ale jiné sensory pouze odesílání. Jiné uzly, třeba brány, mohou shromažďovat data, ale někdy mohou také zaslat požadavek na sensor a vytvářet rozhraní s jinými typy sítí nebo dalšími bránami. Z toho důvodu některé technologie kategorizují uzly na základě funkcí, které implementují. [1] [2]

Příkladem takové technologie, která kategorizuje uzly na základě jejich funkcí, je IEEE 802.15.4. V takové konfiguraci může mít centrální bod na starost celkovou koordinaci sítě, starat se o přenosy dat a připojení ke každému sensoru. Ve standardu IEEE 802.15.4 se centrální bod nazývá koordinátor. U tohoto typu nasazení není každý sensor určen k tomu, aby dělal něco jiného, než komunikoval s koordinátorem ve vztahu typu master/slave. Takové zařízení se nazývá zařízení se sníženou funkcí (RFD). RFD nemůže být koordinátorem, také nemůže implementovat přímou komunikaci s jiným RFD. Koordinátor, který implementuje plné síťové funkce, se naopak nazývá plně funkční zařízení (FFD). FFD může komunikovat přímo s jedním nebo více jinými FFD a vytvářet tak připojení peer-to-peer. Topologie, kde každá FFD má jedinečnou cestu k jiné FFD, se nazývají topologie

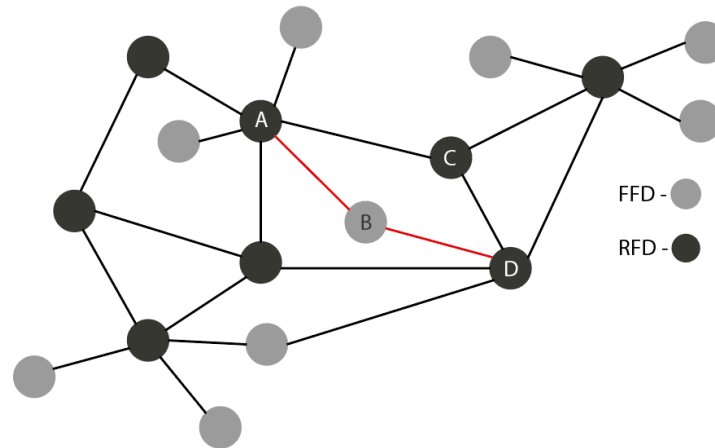
hvězda. FFD ve hvězdě mohou mít RFD, což má za následek topologii strom. Obrázek 2 ilustruje tyto topologie. [1] [2]



Obrázek 2 - Topologie typu hvězda a strom podle zdroje [1]

Další technologie typu point-to-multipoint umožňují uzlu mít více než jedno spojení s jiným uzlem a vytvářet topologii sítě mesh. Toho lze využít k přímé výměně informací mezi uzly nebo k rozšíření dosahu komunikačního spojení. V tomto případě prostřední uzel funguje jako převaděč komunikace mezi dvěma dalšími uzly. Rozšíření dosahu obvykle přichází za cenu pomalejší komunikace, protože mezilehlé uzly musí trávit čas předáváním zpráv jiných uzlů. Příkladem technologie, která implementuje tuto topologii sítě, je Wi-Fi síť. Další vlastností topologie typu mesh je redundance. Zmizení jednoho uzlu nemusí nutně přerušit síťovou komunikaci. Data mohou být stále přenášena přes jiné uzly k dosažení zamýšleného cíle. [1] [2]

Obrázek 3 ukazuje topologii sítě mesh. Uzly A a D jsou příliš daleko od sebe, aby mohly přímo komunikovat. V tomto případě lze komunikaci předávat přes uzly B nebo C. Uzel B lze použít jako převaděč. Ztráta uzlu B však nezabrání komunikaci mezi uzly A a D. Zde je komunikace přeměrována přes jiný uzel, třeba uzel C. [1]



Obrázek 3 - Topologie sítě typu mesh podle zdroje [1]

1.3 LoRaWAN

V posledních letech se objevila nová sada bezdrátových technologií známých jako Low-Power Wide-Area (LPWA). Technologie LPWA, obzvláště pro koncové zařízení přizpůsobené pro dlouhé dosahy a napájení z baterie, otevírají nové příležitosti poskytovatelům služeb i podnikům zvažujícím řešení IoT. Technologie pro IoT využívající LPWA v nelicencovaném pásmu je známá jako LoRaWAN. [1] [2]

Zpočátku byla LoRa pouze fyzická vrstva. Jde o modulaci, kterou vyvinula francouzská společnost Cycleo. Později Cycleo koupila společnost Semtech. Optimalizovanou pro dálkovou, obousměrnou komunikaci a nízkou spotřebu energie se vyvinula z fyzické vrstvy do širšího rozsahu vytvořením aliance LoRa. Semtech LoRa jako technologie modulace fyzické vrstvy je dostupná u více prodejců čipových sad. Aby se odlišila od modulace fyzické vrstvy známé jako LoRa, používá LoRa Alliance termín LoRaWAN k označení své architektury a jejích specifikací, které popisují end-to-end LoRaWAN komunikace a protokoly. [1]

1.3.1 Fyzická vrstva

Semtech LoRa je založena na chirp modulaci rozprostřeného spektra, která má nižší datovou rychlost, aby se výrazně zvýšil komunikační dosah. Kromě toho umožňuje demodulaci pod úrovní šumu a nabízí dobrou odolnost vůči rušení. Zařízení LoRa mohou přijímat na více kanálech paralelně. Regionální specifikace LoRaWAN 1.0.2 popisují

použití hlavních nelicencovaných frekvenčních pásem 433 MHz, 779-787 MHz, 863-870 MHz a 902-928 MHz. [1] [2]

Porozumění branám LoRa je zásadní pro porozumění systému LoRaWAN. Brána LoRa je nasazena jako centrální rozbočovač síťové topologie typu hvězda. Využívá více přenosových kanálů a může demodulovat více kanálů najednou, nebo dokonce demodulovat více signálů na stejném kanálu současně. Brány LoRa slouží jako transparentní most přenášející data mezi koncovými zařízeními. [1]

Datová rychlost v LoRaWAN se liší v závislosti na frekvenčních pásmech a adaptivní datové rychlosti (ADR). ADR je algoritmus, který spravuje rychlost přenosu dat pro každý koncový bod. Algoritmus ADR zajišťuje, že pakety jsou dodávány s nejvyšší možnou přenosovou rychlostí a že vysílací výkon zařízení je optimální vzhledem ke vzdálenosti. Koncové body v blízkosti bran s dobrými hodnotami signálu vysílají s nejvyšší datovou rychlostí a nejnižším vysílacím výkonem. Mezitím koncové body na okraji dosahu spojení komunikují s nejnižší datovou rychlostí a nejvyšším vysílacím výkonem. [1]

Důležitou vlastností LoRa je jeho schopnost zvládat různé rychlosti přenosu dat pomocí rozptylového faktoru. Zařízení s nízkým rozptylovým faktorem (SF) dosahují ve své komunikaci menší vzdálenosti, ale vysílají vyšší rychlostí, což má za následek kratší vysílací čas. Vyšší SF poskytuje pomalejší přenosové rychlosti, ale dosahuje vyšší spolehlivosti na delší vzdálenosti. Pro hodnotu SF12 a 125 kHz šířky pásma kanálu je datová rychlost 250 b/s. Nicméně když se SF sníží na hodnotu 7, datová rychlost se zvýší na 5470 b/s. Hodnoty šířky pásma kanálu jsou 125 kHz, 250 kHz a 500 kHz. Hodnoty SF jsou 7, 8, 9, 10,11 a 12. [1] [2]

1.3.2 Vrstva MAC

Vrstva MAC je definována ve specifikaci LoRaWAN. Tato vrstva využívá fyzickou vrstvu LoRa a klasifikuje koncové body LoRaWAN k optimalizaci jejich životnosti baterie a zajištění následné komunikace. Specifikace LoRaWAN dokumentuje tři třídy zařízení LoRaWAN. Síť LoRaWAN jsou nejprve spojeny jako třída A s možností změny třídy během provozu. [2]

Třída A optimalizuje nastavení výkonu pomocí různých zpoždění příjmu během přenosu. Koncový bod začíná odesláním paketu dat na bránu. Zařízení po přenosu přejde do režimu spánku, dokud nevyprší časovač zpoždění příjmu. Když vyprší časovač, koncový bod se probudí a otevře přijímací slot a po určitou dobu čeká na přenos. Poté znovu přejde do režimu spánku. Zařízení opustí režim spánku, jakmile vyprší jiný časovač. To znamená, že veškerá přijímací komunikace probíhá během krátké doby poté, co zařízení odešle paket. [2]

Zařízení třídy B vyvažují výkon a latenci. Tento typ zařízení se spoléhá na signál odesílaný bránou v pravidelných intervalech. Signál synchronizuje všechny koncové body v síti. Když zařízení přijme signál, vytvoří ping okno, což je krátké přijímací okno. Během tohoto okna lze zprávy odesílat a přijímat. Jinak je zařízení v režimu spánku. V zásadě se jedná o relaci iniciovanou bránou a založenou na metodě časových oken. [2]

Koncová zařízení třídy C používají nejvíce energie, ale mají nejkratší latenci. Tato zařízení otvírají dvě přijímací okna třídy A, která jsou nepřetržitě otevřená. Zařízení třídy C jsou obvykle stále napájená zařízení. Neexistuje žádná latence pro přenos. Zařízení třídy C nemohou implementovat třídu B. [2]

Zprávy LoRaWAN, mají formát složený z hlavičky MAC, užitečného zatížení (dat) s proměnou velikostí a kódu integrity zprávy o délce 4 bajty. Velikost užitečného zatížení MAC závisí na frekvenčním pásmu a datové rychlosti, v rozmezí od 59 do 230 bajtů pro pásmo 863-870 MHz a 19 až 250 bajtů pro pásmo 902-928 MHz. [2]

Ve verzi 1.0.x používá LoRaWAN šest typů zpráv MAC. Zařízení LoRaWAN používají žádost o připojení a přijímají zprávy pro bezdrátovou aktivaci (OTA) a připojení k síti. Ostatní typy zpráv jsou nepotvrzená a potvrzená data. Potvrzená zpráva je ta, kterou je třeba potvrdit, a nepotvrzená znamená, že koncové zařízení nemusí potvrdit přijetí zprávy. [1]

Koncové zařízení LoRaWAN jsou jedinečně adresovatelné pomocí různých metod. Například globální ID zařízení, DevEUI a AppEUI reprezentované jako IEEE Adresa EUI-64, které jednoznačně identifikuje poskytovatele aplikace, vlastníka a koncové zařízení. V síti LoRaWAN jsou koncová zařízení rozlišena také podle adresy koncového zařízení, známé jako DevAddr, což je 32bitová adresa. Zde je 7 nejvýznamnějších bitů

identifikátorem sítě (NwkID), který identifikuje síť LoRaWAN. 25 zbylých bitů se používá jako síťová adresa (NwkAddr) k identifikaci koncového bodu v síti. [1]

1.3.3 Topologie

LoRaWAN je založen na topologii sítě typu hvězda, ale lze říci, že podporuje topologii stromu. Spíše než model s jedním paprskem může LoRaWAN předpokládat více paprsků. Uzel může být přidružen k více než jedné bráně. Kritickou součástí LoRaWAN, která ji odlišuje od většiny přenosů, je skutečnost, že uživatelská data budou přenášena z koncového uzlu do brány přes protokol LoRaWAN. V tomto okamžiku bude brána LoRaWAN předávat paket přes nějaké zpětné připojení, například 4G-LTE, Ethernet nebo Wi-Fi na vyhrazenou síťovou službu LoRaWAN v cloudu. [1] [2]

Pokud je uzel mobilní a pohybuje se od antény k anténě, síťové služby zachytí více identických paketů z různých cest. Tyto cloudové, síťové služby umožňují systémům LoRaWAN zvolit nejlepší trasu a zdroj informací, když je koncový uzel přidružen k více než jedné bráně. Mezi odpovědnosti síťových služeb patří odstranění duplicitních paketů, bezpečnostní služby, směrování a řízení potvrzovací zprávy. [1] [2]

1.3.4 Bezpečnost

Zabezpečení v LoRaWAN se vztahuje na různé komponenty architektury. Koncové body LoRaWAN musí implementovat dvě vrstvy zabezpečení, které chrání komunikaci a ochranu dat v celé síti. První vrstva je použita ve vrstvě MAC, zaručuje autentizaci koncových bodů síťovým serverem LoRaWAN. Také chrání LoRaWAN pakety provedením šifrování na základě AES. Každé koncové zařízení implementuje klíč síťové relace (NwkSKey), který používá jak sám koncový bod, tak i síťový server LoRaWAN. NwkSKey zajišťuje integritu dat pomocí výpočtu a kontroly každé datové zprávy a šifrováním a dešifrováním datových zpráv. [1]

Druhá vrstva je klíč aplikační relace (AppSKey), který provádí funkce šifrování a dešifrování mezi koncovým bodem a jeho aplikačním serverem. Dále vypočítává a kontroluje integritu dat na úrovni aplikace, pokud je jeho součástí. Tím je zajištěno, že poskytovatel služeb LoRaWAN nemá přístup k užitečnému obsahu aplikace, pokud mu tento přístup není povolen. [1]

Koncové body připojené k síti LoRaWAN se musí zaregistrovat a ověřit. Toho lze dosáhnout pomocí jednoho ze dvou mechanismů spojení:

- Aktivace pomocí personalizace (ABP). Koncové body nemusí spouštět proceduru spojení. Klíče jako DevAddr a NwkSKey a AppSKey jsou před konfigurovány a uloženy v koncovém zařízení. A stejné informace jsou registrovány také na síťovém serveru LoRaWAN. [1]

- Over-the-air activation (OTAA): Koncové body se mohou dynamicky připojit ke konkrétní síti LoRaWAN až po úspěšném provedení procedury připojení. Procedura spojení musí být provedena pokaždé, když je obnovena relace. Během procesu připojení, který zahrnuje odesílání a přijímání žádostí o připojení uzlu se síťovým serverem LoRaWAN, si vymění své globálně jedinečné DevEUI, AppEUI a AppKey. AppKey se poté používá k odvození klíčů relace NwkSKey a AppSKey. [1]

1.4 Sigfox

Sigfox je úzkopásmový protokol LPWAN vyvinutý v roce 2009 v Toulouse ve Francii. Sigfox má některé vlastnosti, které výrazně zužují jeho užitečnost, a to konkrétně limitace odeslaných zpráv na 140 denně, velikost užitečného obsahu 12 bajtů pro odeslanou zprávu a 8 bajtů pro přijatou zprávu ze strany sensoru, propustnost až 100 b/s pro odesílání a 600 b/s pro přijímání. [2]

Původně byl Sigfox jednosměrný a zamýšlený jako čistá síť senzorů. To znamená, že bylo podporováno pouze odesílání. Dnes je k dispozici i přijímání. [2]

Sigfox je patentovaná a uzavřená technologie, zatímco hardware je otevřený. Mezi hardwarové partnery Sigfox patří Atmel, TI, Silicon Labs a další. Sigfox buduje svou síťovou infrastrukturu podobnou uspořádání LTE nosičů. Jedná se o velmi odlišný model než je LoRaWAN. LoRaWAN vyžaduje ve své síti použít proprietární hardware, zatímco Sigfox používá několik prodejců hardwaru, ale jednu spravovanou síťovou infrastrukturu. Sigfox vypočítává sazby podle počtu zařízení, která jsou připojena k síti předplacené zákazníkem. [2]

1.4.1 Fyzická vrstva Sigfox

Sigfox je Ultra Narrow Band (UNB). Jak název napovídá, přenos používá pro komunikaci velmi úzký kanál. Jsou tato pásma: 868 MHz pro Evropu (předpisy ETSI 300-200) a 902 MHz pro Severní Ameriku (předpisy FCC část 15). Některé oblasti, jako je Japonsko, mají přísná omezení spektrální hustoty, což v současné době ztěžuje zavedení ultra úzkopásmového připojení. [2]

Pásmo má šířku 100 Hz, pro odesílání využívá spektrum rozprostřené ortogonální sekvencí (OSSS) a 600 Hz pomocí Gaussova klíčování frekvenčním zdvihem (GFSK) pro příjem. Sigfox odešle krátký paket na náhodný kanál s náhodným časovým zpožděním, konkrétně 500 až 525 ms. Tento typ kódování se nazývá RFTDMA (Random Frequency and Time Division Multiple Access). Obousměrná komunikace v Sigfoxu neumožňuje žádný pasivní režim příjmu, což znamená, že centrální stanice nemůže kdykoli jednoduše odeslat zprávu koncovému zařízení. Přijímací okno se otevře až po dokončení přenosových oken. Přijímací okno se otevře až po 20 sekundách od odeslání první zprávy uzlem. Okno zůstane otevřené po dobu 25 sekund, což umožňuje příjem krátké zprávy z centrální stanice. U Sigfoxu je použito 333 kanálů o šířce 100 Hz. Citlivost přijímače je -120 dBm / -142 dBm. Přeskakování kmitočtů je podporováno pomocí pseudonáhodné metody 3 z 333 kanálů. [2]

1.4.2 Sigfox MAC vrstva

Každé zařízení v síti Sigfox má jedinečné ID Sigfox. ID se používá pro směrování a identifikaci zpráv a ověření zařízení Sigfox. Další charakteristikou komunikace Sigfox je, že používá princip odeslání a zapomenutí. Přijímač zprávy nepotvrzuje. Zpráva je odeslána třikrát na třech různých frekvencích ve třech různých časech. To pomáhá zajistit integritu přenosu zprávy. Model Odešli a zapomeň nemá žádný způsob, jak zajistit, aby byla zpráva skutečně přijata, takže je na vysílači, aby udělal co nejvíce pro zajištění správného přenosu. [2]

| Sigfox MAC rámec odeslaných zpráv | | | | | | |
|-----------------------------------|---------|-----------------------|-------------|----------------|----------------|-------------|
| 32 bitů | 16 bitů | 32 bitů | 0 - 96 bitů | proměnná délka | 16 bitů | |
| Preamble | Sync | ID koncového zařízení | Data | Autentizace | FCS | |
| Sigfox MAC rámec přijatých zpráv | | | | | | |
| 32 bitů | 13 bitů | 2 bity | 8 bitů | 16 bitů | Proměnná délka | 0 - 64 bitů |
| Preamble | Sync | Flags | FCS | Autentizace | Chybové kódy | Data |

Obrázek 4 - Rámec zpráv protokolu Sigfox podle zdroje [1]

Na obrázku 4 je znázorněn rámec zpráv pro Sigfox protokol. Rámce zprávy obsahují preambuli předdefinovaných symbolů používaných pro synchronizaci při přenosu. Pole synchronizace rámců určuje typ rámců, které budou přenášeny. FCS je sekvence kontroly rámce používaná pro detekci chyb. [2]

Zásobník protokolů je podobný ostatním zásobníkům podle modelu OSI. Existují tři úrovně. Fyzická vrstva syntetizuje a moduluje signály pomocí BPSK ve směru odesílání a GFSK ve směru přijímání. Vrstva MAC přidá pole pro identifikaci / autentizaci zařízení a kód pro opravu chyb (CRC). Vrstva rámců generuje rádiový rámec z dat aplikace. Rovněž systematicky připojuje pořadové číslo k rámečku. [2]

Z hlediska bezpečnosti nejsou zprávy nikde v zásobníku protokolu Sigfox šifrovány. Je na uživateli, aby k datům užitečného zatížení poskytl šifrovací schéma. V síti Sigfox se nevyměňují žádné klíče, každá zpráva je však kvůli identifikaci podepsána klíčem jedinečným pro zařízení. [2]

1.4.3 Topologie Sigfox

Síť Sigfox může být velmi hustá, například až 1 milion uzlů na jednu centrální stanici. Všechny uzly, které se připojují k základnové stanici, vytvoří síť typu hvězda. [2]

Všechna data jsou spravována prostřednictvím sítě Sigfox. Všechny zprávy ze základní stanice Sigfox musí dorazit na server prostřednictvím IP připojení. Backfox cloudová služba Sigfox je cílem každého paketu. Server uloží a odešle zprávu klientovi po ověření, že neexistují žádné duplikáty. Pokud je třeba data přenést do uzlu koncového bodu, server vybere bránu s nejlepším připojením ke koncovému bodu a předá data. Server již identifikoval zařízení pomocí ID paketu a předchozí zřízení vynutí, aby byla data odeslána

do cílového zařízení. V architektuře Sigfox nelze k zařízením přistupovat přímo. Server Sigfox je také správa, licencování a poskytování služeb zákazníkům. Cloud Sigfox směřuje data do cíle, který si zákazník vybral. [2]

1.5 Weightless

Weightless je jedním z mnoha protokolů v prostoru s nízkou spotřebou a dlouhým dosahem (LPWAN). Speciální skupina Weightless nabízí tři různé protokoly, a to Weightless-N, Weightless-W a Weightless-P, které podporují různé způsoby a případy použití. [10]

1.5.1 Weightless-W

Tento otevřený standard Weightless-W je navržen pro provoz ve spektru bílých míst televizního spektra (TVWS). Použití TVWS je zajímavé, protože využívá výhod ultra vysokofrekvenčního spektra, které se jinak nevyužívá. V praxi to však může být docela obtížné. Pravidla a předpisy pro používání TVWS pro IoT se liší a nejsou k dispozici všude. Koncové uzly jsou také obvykle navrženy tak, aby fungovaly pouze v malé části spektra, protože je nemožné postavit malou anténu, která může fungovat kdekoli od 400 MHz do 800 MHz. V jednom městě může být k dispozici kanál 500 MHz, zatímco v jiném může být k dispozici kanál 700 MHz a systém se nedokáže přizpůsobit tak, aby vyhovoval oběma z nich. [10]

Skupina Weightless používá vcelku sofistikované modulace pro standard Weightless-W, včetně kvadraturní amplitudové modulace, s rozšiřujícími se kódy. Tyto modulace poskytují vrstvu služeb se skutečně vysokými datovými rychlostmi. Weightless-W je ideální pro použití v inteligentním ropném a plynárenském sektoru. [10]

1.5.2 Weightless-N

Weightless-N je ultra úzkopásmový systém, který je velmi podobný Sigfoxu. Můžeme si ho představit jako verzi Sigfoxu založenou na LoRaWAN. Místo toho, aby se jednalo o úplně uzavřený systém, je tvořen sítí partnerů. Používá stejný typ modulace, diferenciální BPSK v úzkých frekvenčních kanálech a je určen pro přenos dat ze senzorů. N-wave je vývojář hardwaru a softwaru IoT. Mezi nevýhody N-wave oproti například systému založenému na LoRa patří požadavek na teplotně kompenzovaný krystalový oscilátor a

relativně nevyvážené zatížení linky. To může být problematické, protože při cestě k centrální stanici získáváte mnohem vyšší citlivost než směrem ke koncovému zařízení. Tento typ systémů se obecně musí spoléhat na jednodušší modulaci FSK pro přijímané zprávy. Weightless-N je ideální pro senzorové sítě, měření teploty, monitorování hladiny nádrže a další. [10]

1.5.3 Weightless-P

Weightless-P je nejnovější technologií Weightless. Nabízí obousměrnou komunikaci. Pokud jde o základní technologii, je to relativně úzkopásmový kanál 12,5 kHz. Weightless používá Gaussovo klíčování s frekvenčním zdvihem, což je standardnější modulace, a kvadrurní klíčování s fázovým posunem, které je mnohem pokročilejší. Na rozdíl od Weightless-N a W Weightless-P nevyžaduje teplotně kompenzovaný krystalový oscilátor kvůli širšímu pásmu. [10]

Společnost ubiik se stala lídrem ve vývoji Weightless-P. Dosah Weightless-P je uváděn na zhruba dvou kilometrech a na rozdíl od Weightless-N pravděpodobně nebude vhodný pro síť s dlouhým dosahem. Důvodem je, že citlivost přijímače kanálu 12 kHz s minimálním posunem klíčování nebude nikdy tak blízko tomu, co získáváme v úzkém kanálu BPSK. Weightless-P je ideální pro soukromé sítě, sofistikovanější případy použití a věci, kde jsou důležitá jak data odesílaná, tak přijímaná. [10]

1.5.4 Vlastnosti Weightless

Centrální stanice pro úzkopásmové signály je v protokolech Weightless složitější, protože je založena na hardwaru definovaném softwarovým rádiem. To vytváří stovky až tisíce kanálů malého klíčování s binárním fázovým posunem. To nám umožní dostat z architektury velkou kapacitu, ale vytvoří se dražší centrální stanice. [10]

Koncové uzly Weightless-N mohou být také dražší, protože mohou vyžadovat teplotně kompenzovaný krystalový oscilátor namísto jednoduchého krystalu. LoRa, na druhou stranu, je velmi shovívavý vůči špatným oscilátorům (nebo krystalům s velkým driftem). [10]

Dosahy Weightless-N a Weightless-W se pohybují kolem pěti kilometrů v městském prostředí. Weightless-P nabídne dosah kolem dvou kilometrů. [10]

1.6 Srovnání

WEIGHTLESS-N VS. SIGFOX

Weightless-N a Sigfox jsou si podobné z technologického hlediska, ale z pohledu marketingu se velmi liší. Weightless je standard, takže je na jiné společnosti, aby kolem toho vytvořila řešení IoT. (Jak bylo zmíněno, N-Wave je lídrem v tomto prostoru a prodává spoustu hardwaru pro Weightless-N společnostem, které se snaží vytvořit síť Weightless.) Na druhou stranu Sigfox nabízí kompletní řešení. [10]

WEIGHTLESS VS. LORA & LORAWAN

Weightless a LoRa nabízejí z technologického hlediska velmi odlišné způsoby. Ale funkčně jsou LoRaWAN a Weightless-N velmi podobné, zejména proto, že oba jsou systémy zaměřeným na odesílání dat více než na příjem. Pokud LoRa není pro uživatele atraktivní, protože hardware pochází výhradně od společnosti Semtech, je Weightless dobrou alternativou založenou na dostupném standardu. [10]

2 Vlastní řešení

V rámci této práce měl vzniknout návrh autonomní bezdrátové sítě senzorů. Návrh se týká především programového řešení a přenosu dat do počítače pro následovné zpracování, ale také volby vyhovujícího hardwaru autonomní bezdrátové sítě senzorů.

Mezi požadavky AKKA Czech Republic s.r.o. na tuto síť patří například dosah od brány k modulu v řádech jednotek kilometrů, možnost kontroly a analýzy pozice a natočení každého z modulů. Síť by byla použitelná například pro monitorování osob v lese při honu a tím předejití úrazu. Základní myšlenkou autonomní sítě byla možnost snadné manipulace a použití na libovolném místě, bez podmínky již existující sítě a pokrytí.

2.1 Zvolený hardware

Pro vlastní realizaci byl použita vývojová deska s mikrokontrolerem STM32F767ZI. Mikrokontroler se stará o sběr dat z jednotlivých senzorů a odesílání dat pomocí LoRa do brány. Technologie LoRa byla zvolena kvůli možnosti odesílat neomezené množství zpráv. Dalším důvodem byl fakt, že technologie Sigfox neumožňuje sestavit privátní síť. Co se týká technologie Weightless zde je problém s dostupností vývojových modulů. Mezi výhody LoRa technologie patří i přímá podpora Semtech modulů firmou STMicroelectronics. Pro určení GPS souřadnic byl použit modul NEO-6M od U-blox, dále pro měření natočení a přetížení byl použit 3osý gyroskop a akcelerometr MPU 6050 jako modul GY-521. Pro komunikaci pomocí LoRa technologie byl použit modul od USI WM-SG-SM-42 a brána od Dragino LG01-N.

2.1.1 Mikrokontroler STM32F767ZI

Jedná se o 32bitový mikrokontroler od firmy STMicroelectronics s ARM Cortex M7 architekturou, 2 MB FLASH paměť pro uložení vlastního programu, 512 kB SRAM paměť, 16MHz vnitřní oscilátor a mnoho dalších vnitřních obvodů, které zde nebudou všechny uváděny. Zmíním pouze ty, které jsou využité pro tuto aplikaci.

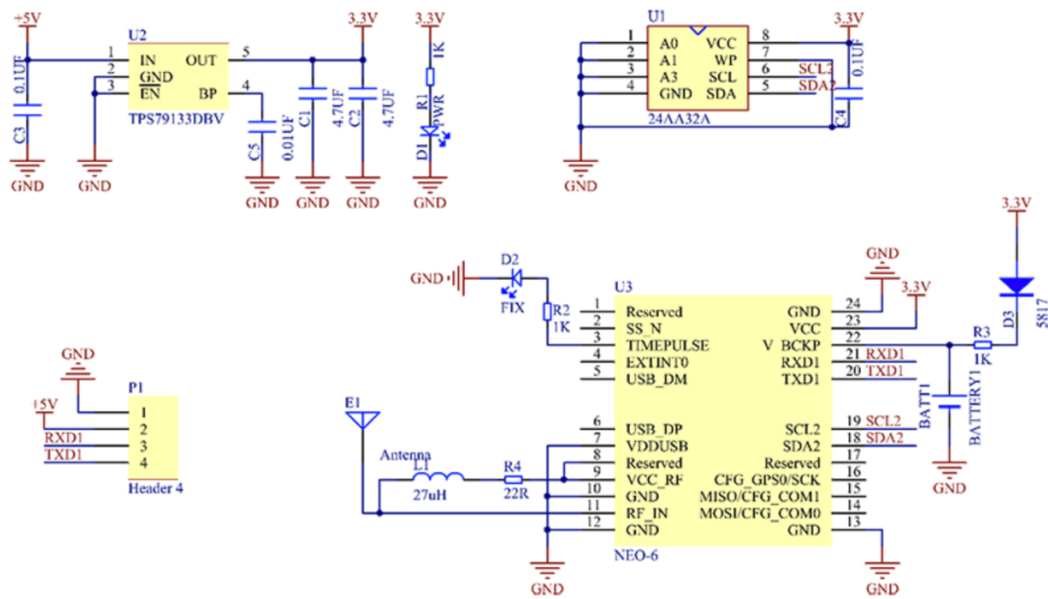
- USART (pro komunikaci s USI LoRa a GPS modulem)
- I2C (pro komunikaci s akcelerometrem a gyroskopem MPU 6050)

2.1.2 GPS modul NEO-6M

Jedná se o modul, který obsahuje samotný NEO-6M, LED pro indikaci napájení a signálu, EEPROM pro uložení konfiguračních dat a záložní baterii pro data v případě ztráty napájení. Možností komunikace s NEO-6M je více, ale pro vyčítání dat se primárně využívá UART s předdefinovanou rychlostí 9600 b/s. Další možností pro připojení s modulem je SPI, které umožňuje připojení sériových externích zařízení, jako je například FLASH paměť pro ukládání konfiguračních dat. Dále je zde rozhraní Display Data Channel (DDC), toto rozhraní je kompatibilní s I2C a může sloužit k připojení EEPROM pro dlouhodobé uložení konfiguračních dat, například pro UART komunikaci. Toho je využito i v modulu, který je v této práci využit. Tento modul dokáže při takzvaném studeném startu určit polohu přibližně za 27 s, tato prodleva není pro tuto práci limitující. A při Hot startu je čas na určení polohy okolo 1 s. [3] [4]

V porovnání s ostatními moduly, které jsou k dostání, nepatří tento modul mezi nejlepší. Například v porovnání s Adafruit Ultimate GPS, který dokáže sledovat satelity až na 66 kanálech NEO-6M pouze na 50 kanálech. Dále dokáže lépe zachytit GPS signál v budovách, s čímž má NEO-6M problém. Další moduly, jako jsou například SIM800L, Goouu Tech Mini IOT-GA6 a SIM7000E, obsahují i slot na SIM kartu, která pro tuto aplikaci není potřeba. Tudíž z důvodu ceny a absence slotu na SIM kartu byl zvolen modul NEO-6M.

Na schématu zapojení (obr. 5) je vidět lineární napěťový regulátor TPS79133DBV od Texas Instruments a I2C EEPROM paměť 24AA32A s velikostí 32 kB od firmy Microchip. Dále je zde znázorněno zapojení samotného modulu NEO-6M, kde je patrné zapojení statusové LED diody D2, zapojení záložní baterie BATT1 a zapojení antény. [4]



Obrázek 5 - Zapojení modulu U-blox NEO 6-M [4]

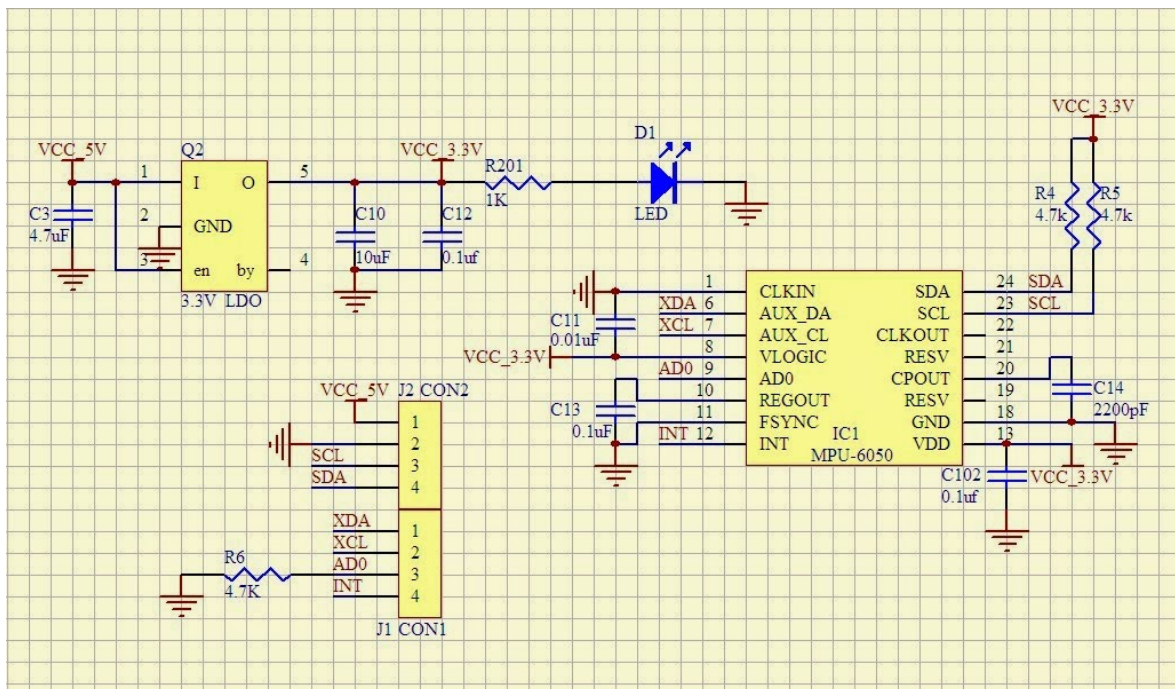
2.1.3 Gyroskop a akcelerometr MPU6050

MPU-60X0 je zařízení, které má v sobě integrovaný 3osý gyroskop a 3osý akcelerometr. Tato řada obsahuje také kalibrační firmware, který je schopný kalibrovat zařízení za běhu. Disponuje třemi 16bitovými ADC převodníky pro digitalizaci dat z gyroskopu a třemi pro akcelerometr. Vyrovňovací FIFO paměť s velikostí 1024 bajtů pomáhá snižovat spotřebu energie tím, že data se vyčítají nárazově a poté přechází sensor do low-power režimu. Komunikace se všemi registry sensoru se provádí v případě MPU-6050 jen pomocí I2C na 400kHz. Mezi další funkce patří zabudovaný teplotní sensor a oscilátor s odchylkou $\pm 1\%$. [5]

Gyroskop typu MEMS má digitální výstup s uživatelsky programovatelným, plným rozsahem ± 250 , ± 500 , ± 1000 a $\pm 2000^\circ/\text{s}$. Provozní proud gyroskopu je 3,6mA a pohotovostní je 5µA. MEMS akcelerometr má také digitální výstup s uživatelsky programovatelným, plným rozsahem $\pm 2\text{ g}$, $\pm 4\text{ g}$, $\pm 8\text{ g}$ a $\pm 16\text{ g}$. Provozní proud je 500 µA a v Low-power modu 10 µA při 1,25 Hz, 20 µA při 5 Hz, 60 µA při 20 Hz, 110 µA při 40 Hz. [5]

Došlo k porovnání třeba s novější řadou MPU 9000, která obsahuje navíc magnetometr, ale rozsahy a způsob komunikace jsou totožné. Tudíž z důvodu ceny, vlastností a rozšíření

tohoto senzoru byl zvolen MPU 6050. Zapojení modulu GY-521 je znázorněno na obrázku 6. Zde je vidět, že modul obsahuje lineární napěťový stabilizátor Q2 s indikační diodou D1. Zapojení samotného modulu MPU-6050 je identické s doporučeným zapojením v datasheetu modulu MPU6050.

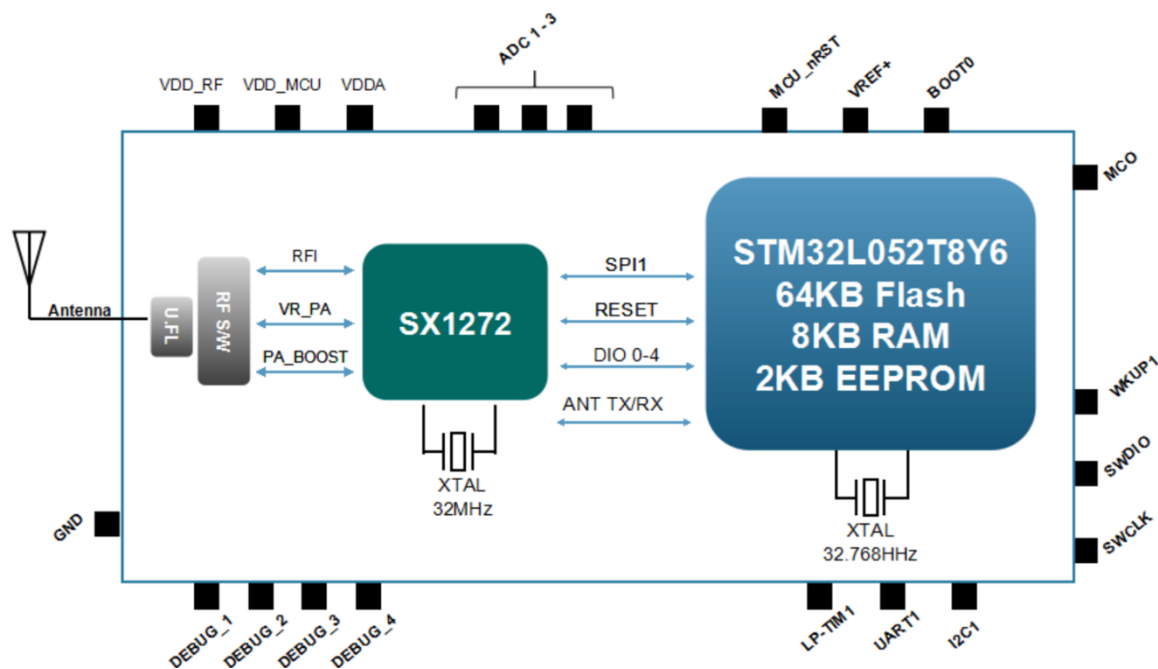


Obrázek 6 - Schéma zapojení GY-521 [6]

2.1.4 Modul USI WM-SG-SM-42 (I-NUCLEO-LRWAN1)

Tento modul je sestaven z čipu Semtech SX1272 a mikroprocesoru STM32L052. Semtech SX1272 obstarává komunikaci LoRa s vysokou citlivostí -137 dBm a podporou Low-power modu. Podporuje LoRa, FSK, GFSK, MSK, GMSK a OOK modulaci. Ultra-Low-Power STM32L052 je 32bitový ARM procesor Cortex-M0+ s frekvencí až 32 MHz, integrovanou 8 kB SDRAM, 2 kB EEPROM a 64 kB FLASH pamětí. Na obrázku 7 je znázorněn blokový diagram modulu. Komunikace mezi SX1272 a STM32L052 probíhá pomocí SPI a komunikace modulu s nadřazeným mikroprocesorem nebo počítačem pomocí UART s předdefinovanou rychlostí 115 200 b/s. Komunikace probíhá na standartu LoRa modulace. Frekvenční rozsah modulu je 860 MHz až 1020 MHz s šířkou pásma 125 kHz, 250 kHz a 500 kHz. Frekvenční tolerance je ± 25 ppm a vysílací výkon až 20 dBm. [7]

Modul I-NUCLEO-LRWAN1 dále obsahuje akcelerometr a magnetometr (LSM303AGR), relativní sensor tlaku a teploty (HTS221) a sensor tlaku (LPS22HB). Modul také disponuje arduino patičí a konektorem pro 50 Ω anténu. [8]



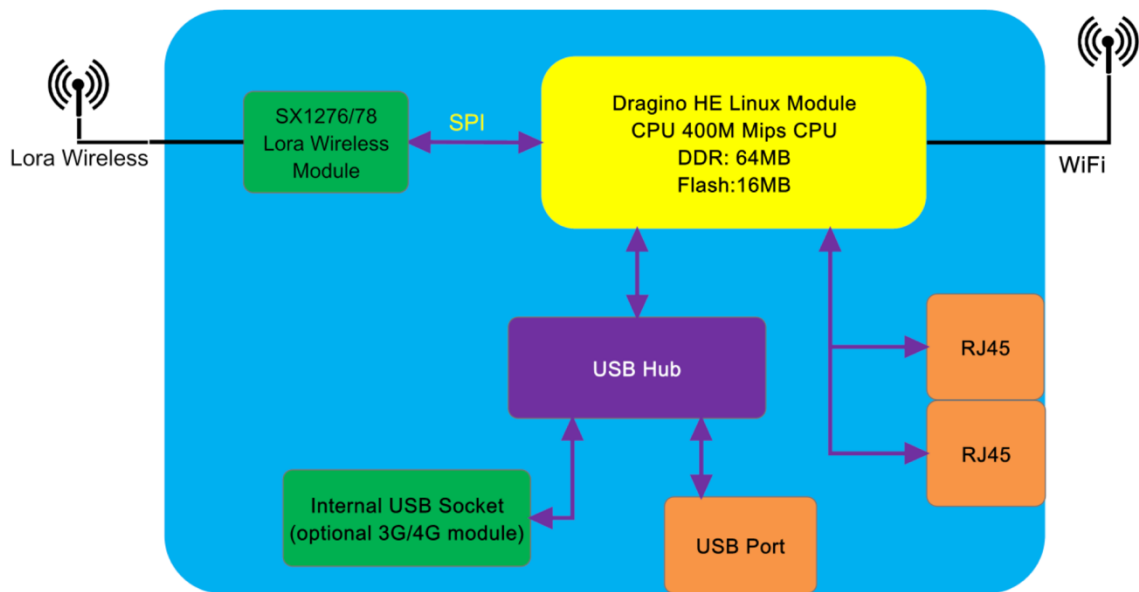
Obrázek 7 - Blokový diagram USI WM-SG-SM-42 [7]

Další moduly s oficiální podporou ST jsou například P-NUCLEO-LORAWAN1 a 2. Tento modul také využívá SX1272, avšak řídicí STM32L0x již není součástí modulu, ale je dodáván jako NUCLEO deska od ST. Modul B-L072Z-LRWAN1 využívá řešení vše v jednom stejně jako I-NUCLEO-LRWAN1, ale tento je od firmy Murata. Disponuje SX1276 a STM32L072CZ. Jelikož parametry všech modulů jsou víceméně totožné, [8] rozhodnutí probíhalo na základě toho, že již bylo k dispozici výše zmíněné NUCLEO STM32F767ZI, tudíž nebylo potřeba kupovat set P-NUCLEO-LORAWAN1 nebo 2, který také obsahuje desku NUCLEO. Volba mezi B-L072Z-LRWAN1 a I-NUCLEO-LRWAN1, tudíž mezi řešením od USI nebo Murata, byla již pouze na základě ceny a konečné rozhodnutí bylo pro modul USI.

2.1.5 Brána Dragino LG01-N

Jedná se o jednokanálovou open source LoRa bránu, která umožňuje přemostit bezdrátovou LoRa síť do IP sítě. Možnosti, jak bránu připojit, jsou Wi-Fi, Ethernet, 3G a 4G mobilních dat. Tato brána není určena pro LoRaWAN síť, ale pro soukromé LoRa síť, ta

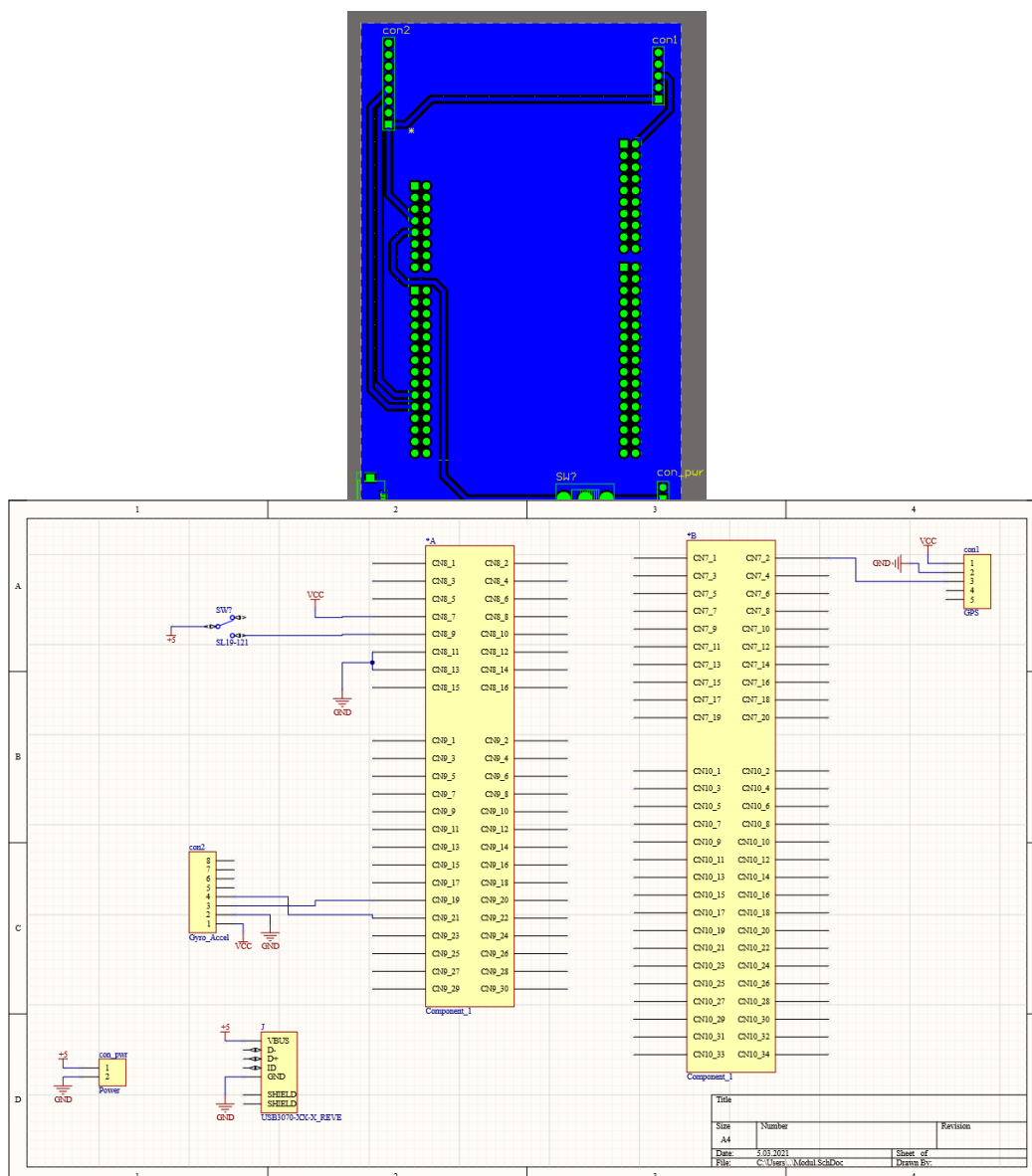
je využita i v této práci. Brána dokáže pokrýt až 100 senzorových uzlů. Systém brány využívá procesor AR9331, 64 MB RAM, 17 MB FLASH a funguje na operačním systému Linux. Frekvenční rozsah LoRa sítě je 862-1020 MHz a 410-528 MHz a citlivost je -148 dBm. Brána primárně odesílá pomocí TCP IP klient nebo MQTT módu. V této práci je využita možnost TCP IP klienta a odesílání na PC. Na obrázku 8 je znázorněn blokový diagram brány LG01-N. [9]



Obrázek 8 - Blokový diagram brány Dragino LG01-N [9]

2.1.6 Propojovací modul

Dále byla navržena jednoduchá propojovací deska, hlavně z důvodu zvýšení mobility modulu pro testování dosahu. Propojovací deska slouží k propojení modulů GPS, gyroskopu, akcelerometru a LoRa. Na desce se dále nachází konektor a mikro USB pro napájení modulů a desky NUCLEO pomocí 5 V. Je zde i vypínač pro odpojení napájení všech modulů a desky NUCLEO. Obrázek 9 dole zobrazuje schéma zapojení propojovací desky a horní obrázek znázorňuje vzhled DPS.



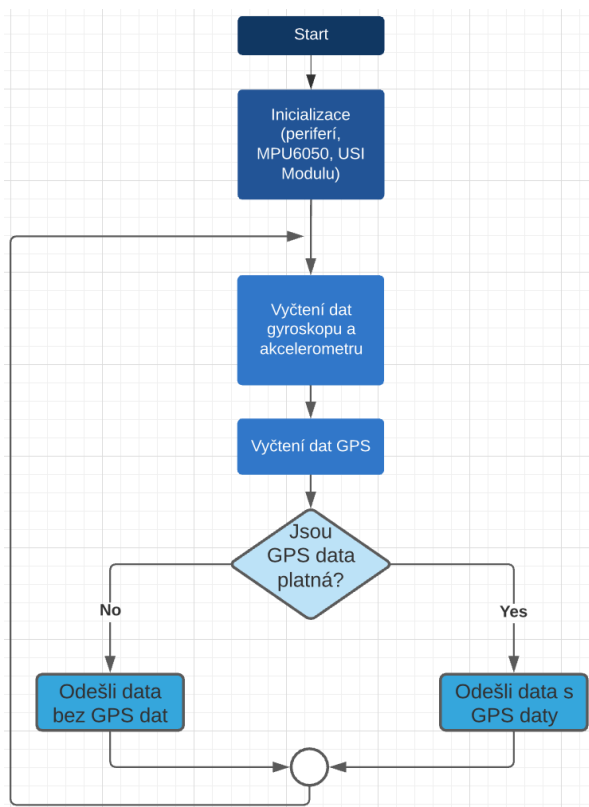
Obrázek 9 - Schéma zapojení a vzhled propojovací desky

2.2 Programová část

Program mikrokontroleru pro zpracování dat ze senzorů a odesílání přes LoRa je psán ve vývojovém prostředí STM32CubeIDE v jazyce C. Pro počítačovou vizualizaci dat přijímaných z LoRa brány bylo zvoleno Visual studio od Microsoftu. Dále bude v této kapitole popsáno nastavení LoRa brány.

2.2.1 Program mikrokontroleru

Jak bylo zmíněno výše, program je psán ve vývojovém prostředí od ST STM32CubeIDE v jazyce C. Zde vysvětlím podrobně pouze hlavní části programu. Celý program naleznete v příloze. Zde ve složce /Program STM32Cube/Lora_Modul_1 nebo 2 /Core/Src lze nalézt soubor main.c a lora_modul.c. V souboru main.c je inicializace periférií, nastavení hodin a hlavní smyčka programu. Soubor lora_modul.c obsahuje všechny mnou vytvořené funkce, které jsou použity v hlavní smyčce programu. Na obrázku 10 je znázorněn vývojový diagram programu. Program začíná inicializací všech periférií, jako je UART, I2C a hodin. Inicializace USART3 slouží pro komunikaci s PC a debugu.



Obrázek 10 - Vývojový diagram programu pro STM32F767

Při inicializaci MPU6050 se nejprve pošle dotaz pomocí I2C na adresu registru 0x75, kde je uložena adresa zařízení. Základní adresa je 0xD0, pokud adresa při odpovědi souhlasí, pokračuje se s probuzením MPU6050, nastavením vzorkovací frekvence na 1kHz, nastavením rozsahu gyroskopu na ± 250 °/s a nastavením rozsahu akcelerometru na ± 2 g.

Dále se inicializuje USI LoRa modul. Tento modul se ovládá a nastavuje přes UART s rychlostí 115200 b/s pomocí AT příkazů. Příklad takového příkazu je například

„AT+RF=20,867100000,7,0,1,0,500,0,0“, který provede nastavení vysílacího výkonu, přenosové frekvence a dalších parametrů rádiové komunikace. Těchto příkazů je celá řada a jsou k dohledání na GitHubu viz [7]. Před samotným použitím byla provedena aktualizace modulu na poslední firmware pomocí programátoru ST-Link V2 a převodníku z UART na USB připojených na konkrétní piny dle návodu na GitHubu. V programu jsou nastaveny parametry rádiové komunikace, rychlost přenosu dat a maska kanálů, na které bude modul vysílat.

V hlavní smyčce programu je vytvořeno pomocí SysTicku časování odesílání a čtení dat z gyroskopu na 1500 ms. Vyčtení dat z MPU6050 se provádí pomocí I2C a čtení daného registru. v případě gyroskopu je to adresa 0x43 až 0x48 a pro akcelerometr je to adresa od 0x3B do 0x40. Pro každou osu jsou tedy 2 bajty pro akcelerometr a 2 bajty pro gyroskop. Poté se přečtený řetězec rozdělí na hodnoty pro jednotlivé osy. Příklad vyčtení dat gyroskopu je vidět na obrázku 11.

```
void MPU_6050_Read_Gyro(void){
    uint8_t recv[6];

    HAL_I2C_Mem_Read (&hi2c2, MPU_ADDR, 0x43, 1, recv, 6, 1000); // Read 6 BYTES of data starting from GYRO_XOUT_H register to GYRO_ZOUT_L

    gyro_x = (int16_t)(recv[0] << 8 | recv [1]);
    gyro_y = (int16_t)(recv[2] << 8 | recv [3]);
    gyro_z = (int16_t)(recv[4] << 8 | recv [5]);

    /** convert the RAW values into dps (°/s)
    we have to divide according to the Full scale value set in FS_SEL
    I have configured FS_SEL = 0. So I am dividing by 131.0
    for more details check GYRO_CONFIG Register          *****/

    Gx = gyro_x/131.0;
    Gy = gyro_y/131.0;
    Gz = gyro_z/131.0;
}
```

Obrázek 11 - Kód pro vyčtení dat gyroskopu MPU6050

Data GPS NEO-6M se vyčítají pomocí UART. Pro zachycení všech dat, která modul posílá, je využito DMA s velikostí bufferu 255 B. NEO-6M odesílá neustále řetězce dat, které mají definovaný formát. Při hledání signálu modul odesílá dané řádky, ale bez dat, jak je vidět na obrázku 12 vlevo, řádka obsahuje vesměs pouze čárky. Po zachycení začne modul odesílat řádky naplněné daty tak, jak je vidět na obrázku 12 vpravo. Z těchto řádků nás zajímá řádek začínající \$GPGLL, kde je uvedena zeměpisná šířka a délka. Tudíž v programu po naplnění DMA bufferu je celý buffer programem procházen a hledá se takto začínající řádka. Zároveň se kontroluje, zda délka řádky je větší než 49, tím se zamezí zpracování

prázdných řádek. Dále se řádek zpracuje a data zeměpisné šířky se přepočítají z formátu stupňů a minut na stupně a desetinné číslo pro vizualizaci na mapě.

```

$GPVTG,,,,,,,,,N*30
$GPGGA,014122.00,,,,,0,00,99.99,,,,,*62
$GPGSA,A,1,,,,,,,,,99.99,99.99,99.99*30
$GPGSV,1,1,02,21,29,321,,24,35,166,10*73
$GPGLL,,,,,014122.00,V,N*4E
$GPRMC,014123.00,V,,,,,060314,,,N*78
$GPVTG,,,,,,,,,N*30
$GPGGA,014123.00,,,,,0,00,99.99,,,,,*63
$GPGSA,A,1,,,,,,,,,99.99,99.99,99.99*30
$GPGSV,1,1,02,21,29,321,,24,35,166,26*76
$GPGLL,,,,,014123.00,V,N*4F
$GPRMC,014124.00,V,,,,,060314,,,N*7F
$GPVTG,,,,,,,,,N*30
$GPGGA,014124.00,,,,,0,00,99.99,,,,,*64
$GPGSA,A,1,,,,,,,,,99.99,99.99,99.99*30
$GPGSV,1,1,02,21,29,321,,24,35,166,*72
$GPGLL,,,,,014124.00,V,N*48
$GPGLL,2232.73995,N,11404.60273,E,030427.00,A,A*6B
$GPRMC,030428.00,A,2232.73995,N,11404.60275,E,0.037,,070314,,,A*7E
$GPVTG,,T,,M,0.037,N,0.069,K,A*28
$GPGGA,030428.00,2232.73995,N,11404.60275,E,1.07,1.17,122.5,M,-2.3,M,,*4F
$GPGSA,A,3,29,21,18,05,14,22,26,,,,,2,12,1.17,1.77*00
$GPGSV,3,1,10,05,18,096,31,12,07,154,15,14,12,248,29,15,44,025,*7B
$GPGSV,3,2,10,18,38,325,43,21,61,296,41,22,09,304,31,24,70,114,*7D
$GPGSV,3,3,10,26,10,045,16,29,16,208,35*7E
$GPGLL,2232.73995,N,11404.60275,E,030428.00,A,A*62
$GPRMC,030429.00,A,2232.73994,N,11404.60277,E,0.017,,070314,,,A*7E
$GPVTG,,T,,M,0.017,N,0.031,K,A*27
$GPGGA,030429.00,2232.73994,N,11404.60277,E,1.07,1.17,122.7,M,-2.3,M,,*4F
$GPGSA,A,3,29,21,18,05,14,22,26,,,,,2,12,1.17,1.77*00
$GPGSV,3,1,10,05,18,096,31,12,07,154,14,14,12,248,29,15,44,025,*7A
$GPGSV,3,2,10,18,38,325,43,21,61,296,41,22,09,304,31,24,70,114,21*7E
$GPGSV,3,3,10,26,10,045,14,29,16,208,35*79
$GPGLL,2232.73994,N,11404.60277,E,030429.00,A,A*60

```

Obrázek 12 - Příklad odesílaných řetězců modulu NEO-6M bez signálu(nalevo), se signálem(vpravo)

Poslední částí programu je odesílat dat. Odesílání dat probíhá pomocí AT příkazu „AT+TXT=1, OBSAH ZPRÁVY“. Obsah zprávy musí být v hexadecimálním tvaru. Tudiž program nejdříve vytvoří řetězec dat s ID daného modulu, který má následující tvar:

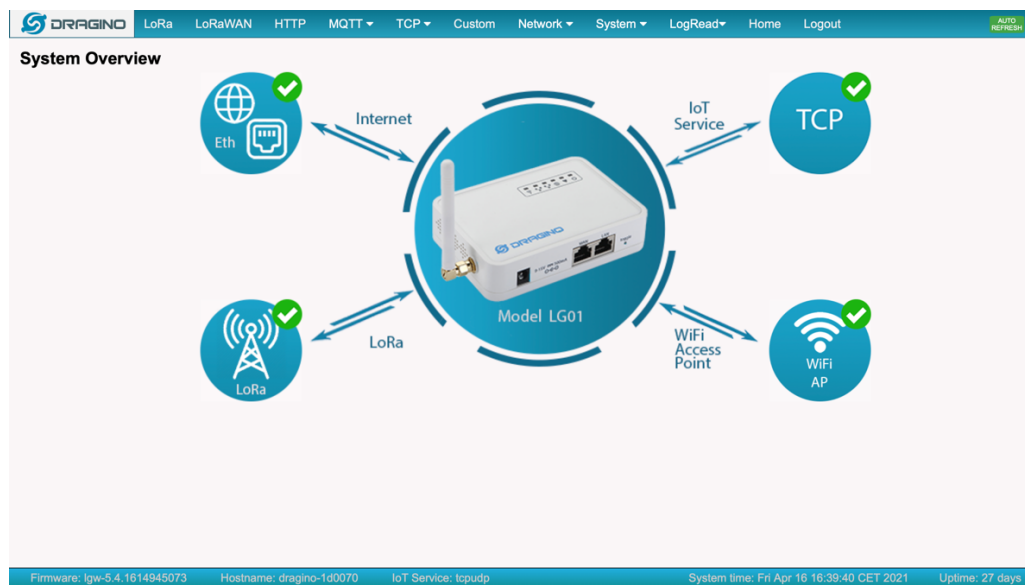
```
<1569>lat=41.54234,lon=14.23421,ax=1.03,ay=0.05,az=-1.43,gx=102,gy=32,gz=153,temp=25,53
```

Takto sestavený řetězec se převede na hexadecimální tvar pomocí vytvořené funkce. A nakonec se sestaví řetězec AT příkazu, který se odešle pomocí UART do USI modulu.

2.2.2 Nastavení brány Dragino LG01-N

Nastavení brány se provádí přes webové rozhraní brány, která je vidět na obrázku 13. Jsou dvě možnosti, jak se připojit k bráně. První je připojení se k Wi-Fi, kterou brána z továrního nastavení vysílá a heslo je k nalezení v manuálu. Druhý způsob je připojení se k bráně přes Ethernet port. Přístup do webového rozhraní je zabezpečen jménem a heslem. Jméno je „admin“ a heslo „dragino“. Nejprve byla nastavena statická adresa brány v rozsahu sítě. V tomto případě to byla adresa 192.168.1.40 a poté byl nastaven TCP IP klient. Jako adresa serveru byla použita IP adresa počítače a port, na který mají být data odesílána. Pro tento případ 192.168.1.176 a port 9999. Brána automaticky odesílá data na TCP IP server ihned po přijetí dat od některého z LoRa modulů. Na webovém rozhraní brány je možnost sledovat logy LoRa komunikace, kde jsou vidět přijímané zprávy v hexadecimálním tvaru.

Dále je zde možnost aktualizace firmwaru brány, nastavení MQTT serveru a nastavení parametrů rádiové komunikace. Konkrétní nastavení je vidět na obrázku 14. Nastavení musí být naprosto shodné s nastavením na modulu USI a po změně nastavení rádiové komunikace je nutné bránu restartovat.

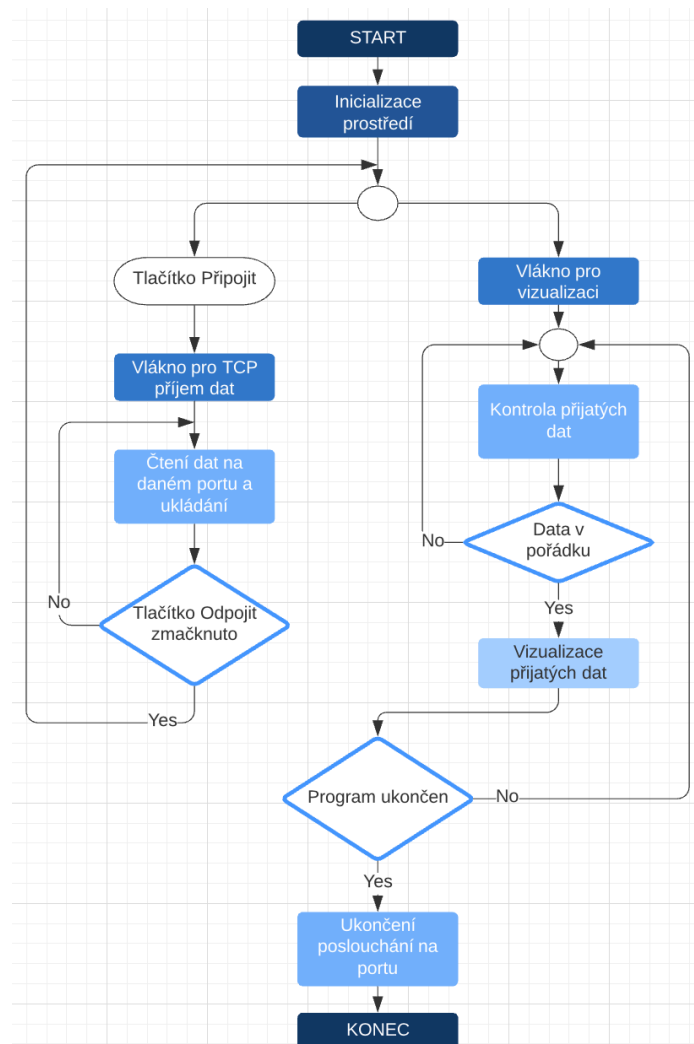


Obrázek 13 - Webové rozhraní brány Dragino LG01-N

Obrázek 14 - Nastavení LoRa komunikace na bráně

2.2.3 Program pro příjem a vizualizaci dat v PC

Pro simulaci TCP IP serveru a vizualizaci byl použit program Visual Studio, konkrétně Windows Form Application. Na obrázku 15 je znázorněn vývojový diagram programu. Spustitelný soubor programu se nachází v příloze cesta k souboru je následující „/Program Visual Studio/Vizualizace/Vizualizace/bin/Debug/Vizualizace.exe“. Při startu programu se inicializuje mapa, která slouží pro zobrazování pozice modulů. Mapa je přidána pomocí NuGet knihovny, konkrétně za pomoci GMap. Zde je nastaven poskytovatel a typ mapy, maximální a minimální zoom mapy a povolení pohybování po mapě za pomoci kurzoru myši.



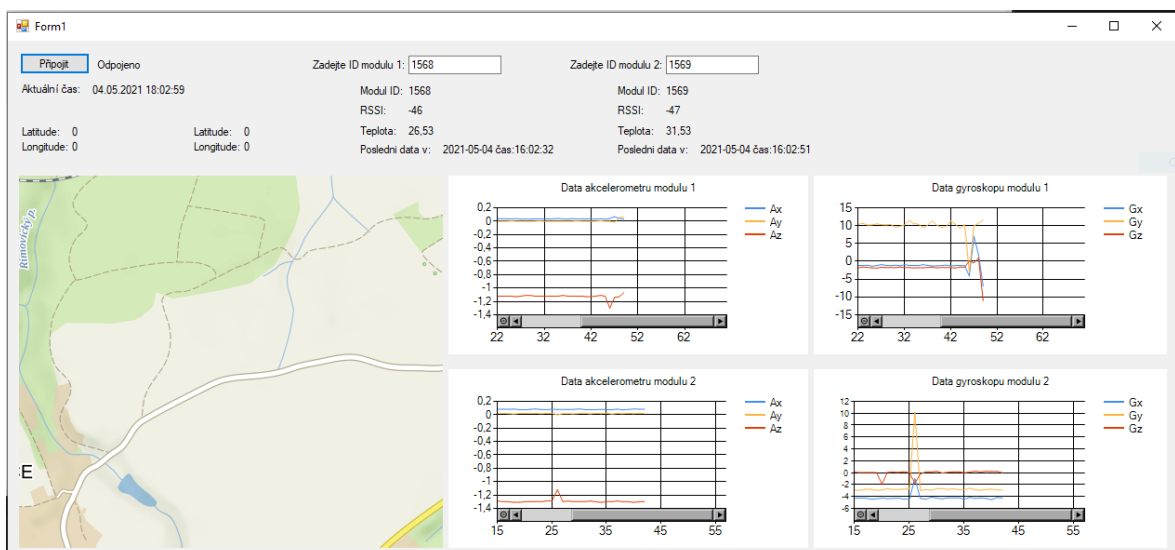
Obrázek 15 - Vývojový diagram programu pro vizualizaci dat

Dále se program dělí na dvě vlákna, a to z toho důvodu, že jedno vlákno je vyhrazeno pro čtení dat a druhé pro samotnou vizualizaci. Čtení je prováděné za pomoci vytvoření TCP IP serveru a třídy TcpListener, který je nastaven na daný port 9999. A po kliknutí na tlačítko „Připojit“ se spustí server, který začne naslouchat až do doby, kdy je server odpojen pomocí tlačítka. Ve vláknech pro vizualizaci dat je vytvořen časovač, který periodicky zkontroluje přijatá data, zda odpovídají danému formátu.

```
"1568:2021-04-17T11:34:44,-49,lat=0.000000lon=0.000000ax=0.055ay=-0.01az=-1.11gx=-1.1679gy=10.1068gz=-1.7786tmp=26.53;\r\n"
```

Následně program rozdělí řetězec na jednotlivé segmenty a převede na číselnou hodnotu, kterou dále vizualizuje do konkrétních grafů a pozic na základě ID modulu.

Na obrázku 16 je vidět okno programu. Program vizualizuje data gyroskopu a akcelerometru do dvou samostatných grafů pro každý modul. Dále jsou zde základní informace o každém z modulů, a to konkrétně indikátor síly přijímaného signálu RSSI, teplota okolního prostředí, kde se modul nachází, čas posledního příjmu dat a číselná hodnota zeměpisné délky a šířky pro každý z modulů.

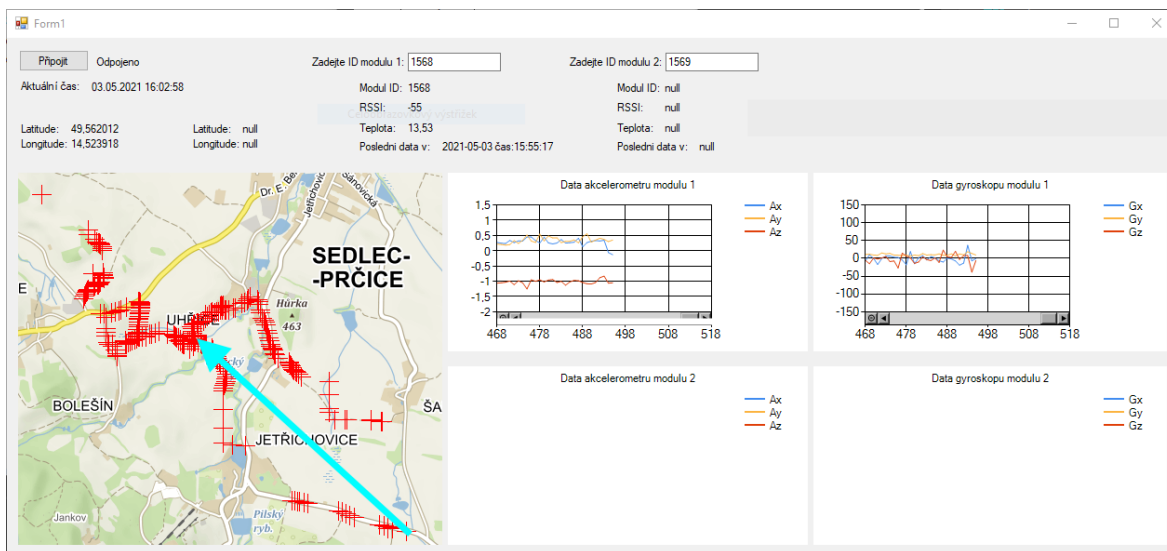


Obrázek 16 - Okno programu pro vizualizaci dat

3 Ověření výsledků

Testování dosahu modulu od brány bylo prováděno dvakrát, a to s nastavením SF 7 a SF 9 pro šířku pásma 125 kHz. Pro SF7 byla dosažená vzdálenost okolo 2 km od brány. A

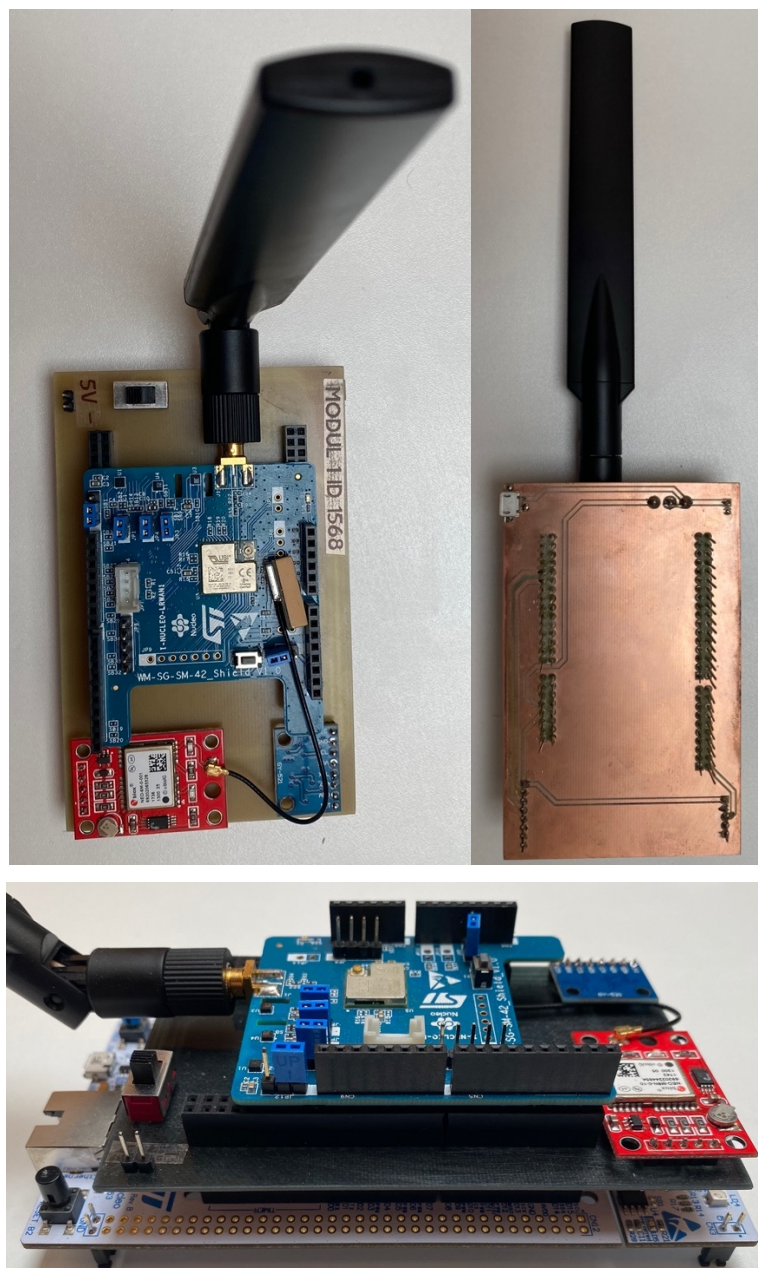
po nastavení SF na hodnotu 9 byl schopný modul odesílat data na vzdálenost až necelých 3 kilometrů. Obrázek 17 zobrazuje mapu s nejdelší dosaženou vzdáleností. Světle modrá šipka naznačuje vzdálenost od brány a odpovídá vzdálenosti 2,8 km. Dále je na obrázku patrné, že v případě trasy mezi modulem a bránou bez horizontu bylo odesílání pravidelné a husté. Při rostoucí vzdálenosti a větší komplikovanosti terénu se hustota dat zmenšovala. Při ideálních podmínkách věřím, že by modul a brána byla schopna přenosu na větší vzdálenost, ale největším problémem pro signál je terén. Dle testů stačí, aby se brána vůči modulu ocitla za horizontem a přenos již není možný. Jelikož umístění brány v době testování bylo v údolí, bylo testování na větší vzdálenost s ideálními podmínkami nemožné. Pro lepší pokrytí oblasti by bylo lepší, aby byla brána umístěna na nejvyšším místě v dané oblasti.



Obrázek 17 - Okno programu s maximálním dosahem

Modul MPU6050 fungoval vždy bez problémů a podle očekávání. U modulu NEO 6M byl občas problém se zachycením signálu a určením polohy. V některých případech zachycení trvalo i 2 minuty a občas bylo nutné modul restartovat pomocí odebrání napájení. Avšak po zachycení modul fungoval dle očekávání a problém například se ztrátou signálu nenastal. Co se týká modulu LoRa od USI, zde k nějakým závažnějším problémům také nedošlo a modul po aktualizaci firmwaru fungoval dle očekávání. Jediný problém byl při aktualizaci firmwaru. Z neznámého důvodu nešlo vytvořit zálohu dle návodu, a tudíž nebyla možná aktualizace. Tento problém pomohla vyřešit podpora na GitHubu, která podle ID modulu zaslala soubor se zálohou pro daný modul. Tento problém dle GitHubu mělo více uživatelů, a tudíž toto považuji za problém LoRa modulu. S bránou od firmy Dragino nenastal žádný problém.

Na skupině obrázků 18 je vidět finální podoba vytvořeného bezdrátového modulu.



Obrázek 18 - Finální vzhled bezdrátového modulu

4 Závěr

Cílem této diplomové práce bylo sestrojít autonomní bezdrátovou síť za použití IoT technologie s dosahem jednotek kilometrů. Na začátku této práce jsou shrnuty nalezené poznatky o používaných technologiích a protokolech v IoT. Prodiskutoval jsem zde vlastnosti protokolů LoRaWAN, Sigfox a Weightless. Pro tuto byl využit protokol LoRa.

Další částí byla volba hardwaru, který by splňoval podmínky této práce. Zde jsem zvolil snadno dostupné a cenově výhodné komponenty. Dalším krokem bylo propojení všech modulů a zachování co největší mobility, proto byla navržena jednoduchá propojovací deska. Pro oživení celého modulu byl vyvinut program v jazyce C, který sloužil pro sběr a odesílání dat na bránu. Poslední částí bylo vyvinutí programu pro vizualizaci přijímaných dat branou. Pro tento program byl využit jazyk C#.

Projekt byl zakončen testováním funkce a dosahu vytvořeného modulu. Modul byl schopný bezproblémové komunikace až do vzdálenosti jednotek kilometrů. S daty gyroskopu a akcelerometru nebyl žádný problém. Avšak příjem GPS signálu občas provázely komplikace, hlavně při spuštění modulu. Tento problém by dle mého názoru mohla vyřešit jiná GPS anténa, která by umožnila lepší příjem signálu.

Seznam literatury a informačních zdrojů

- [1] IoT fundamentals : networking technologies, protocols, and use cases for the internet of things / David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Robert Barton, Jerome Henry. -- Indianapolis, Cisco Press [2017].
- [2] Internet of Things for architects : architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security / Perry Lea. -- Birmingham : Packt Publishing, 2018.
- [3] U-blox, NEO-6 Datasheet [online] 2011 [cit. 2021-5-4] Dostupné z: [https://www.u-blox.com/sites/default/files/products/documents/NEO-6_DataSheet_\(GPS.G6-HW-09005\).pdf](https://www.u-blox.com/sites/default/files/products/documents/NEO-6_DataSheet_(GPS.G6-HW-09005).pdf)
- [4] Sunfounder, NEO-6M GPS Module [online] 2017 [cit. 2021-5-4] Dostupné z: http://wiki.sunfounder.cc/index.php?title=Ublox_NEO-6M_GPS_Module
- [5] InvenSense, MPU-6000 and MPU-6050 Product specification [online] 2012 [cit. 2021-5-4] Dostupné z: <http://www.haoyuelectronics.com/Attachment/GY-521/mpu6050.pdf>
- [6] Haoyuelectronic, Scheme MPU-6050 [online] 2016 [cit. 2021-5-4] Dostupné z: <http://www.haoyuelectronics.com/Attachment/GY-521/GY-521-SCH.jpg>
- [7] USI, USI I-NUCLEO-LRWAN1 [online] 2020 [cit. 2021-5-4] Dostupné z: https://github.com/USIWP1Module/USI_I-NUCLEO-LRWAN1
- [8] ST, I-Nucleo-LRWAN1 [online] [cit. 2021-5-4] Dostupné z: https://www.st.com/content/st_com/en/products/evaluation-tools/product-evaluation-tools/mcu-mpu-eval-tools/stm32-mcu-mpu-eval-tools/stm32-3rd-party-evaluation-tools/i-nucleo-lrwan1.html
- [9] Dragino, LoRa Gateway LG01-N [online] 2020 [cit. 2021-5-4] Dostupné z: <https://www.dragino.com/products/lora-lorawan-gateway/item/143-lg01n.html>
- [10] Brian Ray, What is Weightless? [online] 2015 [cit. 2021-5-4] Dostupné z: <https://www.link-labs.com/blog/what-is-weightless>