VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ
DEPARTMENT OF COMPUTER SYSTEMS

ZABEZPEČENÍ A STŘEŽENÍ OBJEKTŮ A PROSTOR POMOCÍ ARDUINO/SIGFOX

GUARDING AND SECURING OF OBJECTS AND AREAS BASED ON ARDUINO/SIGFOX

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **TOMÁŠ SADÍLEK**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. VÁCLAV ŠIMEK**
SUPERVISOR

BRNO 2019

Vysoké učení technické v Brně
Fakulta informačních technologií

Ústav počítačových systémů (UPSY) Akademický rok 2018/2019

Zadání bakalářské práce

Student: **Sadílek Tomáš**
Program: Informační technologie
Název: **Zabezpečení a střežení objektů a prostor pomocí Arduino/Sigfox**
Guarding and Securing of Objects and Areas Based on Arduino/Sigfox
Kategorie: Vestavěné systémy

Zadání:

1. Seznamte se s technologiemi používanými při zabezpečení a střežení vnějších a vnitřních prostor (např. kamery, čidla, světelné závory).
2. Vytvořte specifikaci a s využitím vhodně vybraných technologií z bodu 1 navrhněte blokové schéma systému pro zabezpečení a střežení zvoleného objektu a/nebo prostoru.
3. Systém specifikovaný v bodu 2 navrhněte s ohledem na následující požadavky: snadnost instalace, možnost uživatelského ovládání a změny strukury/vlastností systému, změny komponent systému, archivace a zasílání uživatelem upřesněných dat.
4. Na obvodové úrovni realizujte jednotlivé moduly navrženého systému a implementujte obslužný firmware zajišťující jejich činnost.
5. Funkčnost celého systému či jeho vybraných částí stanovených po dohodě s vedoucím prakticky ověřte. Diskutujte dosažené výsledky a zvažte případná rozšíření či vylepšení.

Literatura:

- Dle pokynů vedoucího.

Pro udělení zápočtu za první semestr je požadováno:

- Splnění bodů 1 a 2 zadání.

Podrobné závazné pokyny pro vypracování práce viz http://www.fit.vutbr.cz/info/szz/

Vedoucí práce: **Šimek Václav, Ing.**
Vedoucí ústavu: Sekanina Lukáš, prof. Ing., Ph.D.
Datum zadání: 1. listopadu 2018
Datum odevzdání: 15. května 2019
Datum schválení: 31. října 2018

Abstrakt

Cílem této bakalářské práce je navržení a postavení zabezpečovacího systému využívajícího komunikačního protokolu Internetu věcí. Systém je tvořen vývojovou deskou Arduino Nano, komunikačním modulem pro síť Sigfox a senzory pro zabezpečení prostor. Naměřená data jsou odesílána na server, po zpracování a vyhodnocení jsou uložena do databáze MySQL. Při spuštění alarmu je uživatel informován. Na webovém serveru jsou tyto informace přístupné uživateli.

Abstract

The aim of this bachelor thesis is to design and build a guarding system using Internet of Things communication protocol. The system is based on the Arduino Nano developement board, the Sigfox communication module, and security sensors. The measured data are sent to the server, processed, evaluated and stored in MySQL database. When the alarm is triggered, the user is notified. The information is accessible to users on the web server.

Klíčová slova

Zabezpečení a střežení objektů, Internet věcí, Sigfox, LoRaWAN, Arduino Nano, LoPy, MicroPython

Keywords

Guarding and securing of objects, Internet of Things, Sigfox, LoRaWAN, Arduino Nano, LoPy, MicroPython

Citace

SADÍLEK, Tomáš. *Zabezpečení a střežení objektů a prostor pomocí Arduino/Sigfox*. Brno, 2019. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Ing. Václav Šimek

Zabezpečení a střežení objektů a prostor pomocí Arduino/Sigfox

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením pana Ing. Václava Šimka. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

.....

Tomáš Sadílek

16. května 2019

Obsah

Seznam obrázků

Kapitola 1

Úvod

Cílem práce je navrhnout zabezpečení objektu pomocí vývojové desky Arduino a technologie Sigfox, jako alternativu k běžně dostupným zabezpečovacím systémům používajícím mobilní technologie GSM.

Předložená práce se zabývá návrhem zabezpečovacího systému komunikujícího s využitím technologií používaných v rámci sítě pro Internet věcí. Konkrétně byly zvoleny sítě Sigfox a LoRaWAN.

V kapitole 3 (Hardware) je popsán hardware potřebný pro sestavení základního testovacího obvodu navrhovaného zabezpečovacího systému, jsou to senzory pro detekci pohybu, akustický bzučák a anténa pro komunikaci se sítí Sigfox. Jako srdce systému jsou navrženy dvě vývojové desky Arduino a Lopy (Pycom).

Kapitola 4 (Zabezpečovací modul) se zabývá vlastním návrhem zabezpečovacího systému, popisem a implementace jeho jednotlivých částí.

Kapitola 2

Internet věcí

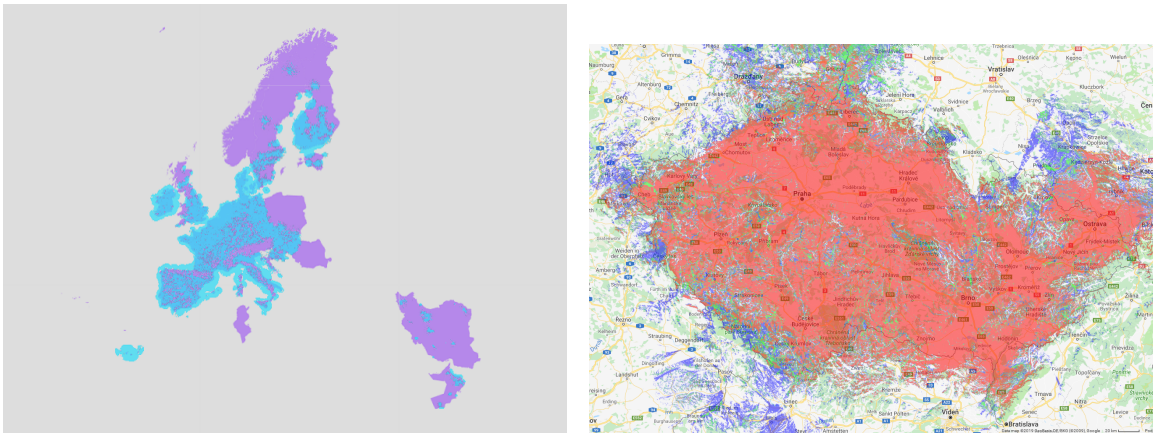
Internet věcí, z anglického názvu Internet of Things (IoT), je v informatice označení pro globální síť fyzických zařízení, vozidel a domácích spotřebičů vybavených síťovou konektivitou pro výměnu dat. Pro komunikaci se využívá bezdrátových, satelitních, kabelových či optických technologií. Výměna dat probíhá bez aktivní účasti člověka, jedná se tedy o komunikaci „machine to machine (M2M)“. Zařízení v síti IoT mohou pro komunikaci využívat různé bezdrátové technologie, např. LPWAN, WIFI, Bluetooth, NFC, a komunikační protokoly, např. LoRa, ZigBee, atd. IoT síť není používána pouze pro „Chytré domácnosti“, ale lze se s ní setkat i v průmyslu, zemědělství, energetice, dopravě a ve zdravotnictví. Za minulý rok vzrostl počet zařízení v IoT síti o 31 %. V roce 2017 bylo v síti více než 8,4 mld. aktivních zařízení a pro rok 2020 se odhaduje počet aktivních zařízení na více než 20 miliard. Další milník IoT by měl nastat po masovém rozšíření 5G sítí, které díky nízké latenci a vyšší přenosové kapacitě umožní nasazení těchto technologií například v oblasti řízení autonomních automobilů.

V této kapitole jsou popsány jednotlivé technologie patřící mezi „Low-Power Wide-Area Network“ (LPWAN), použité v této práci. LPWAN je typ bezdrátové komunikace speciálně vytvořený pro použití na dlouhé vzdálenosti, s velmi malými objemy dat, vyšší latencí, s vysokou škálovatelností a nízkou spotřebou. Výhodou je nižší cena koncového zařízení. Mezi tyto sítě patří například LoRaWAN, Sigfox, Weightless, Nwave nebo NB-Fi Protocol.

Další části práce se zabývají pouze sítě Sigfox a LoRaWAN. Tyto sítě vysílají v bezlicenčním frekvenčním pásmu 868 MHz. Toto pásmo spravuje Český telekomunikační úřad (ČTÚ) ve všeobecném oprávnění (VO) číslo VO-R/10/12.2017-10. VO specifikuje maximální celkový vyzářený výkon, který je nutné vyzářit dipólovou anténou, hodnotou 25 mW. Dále specifikuje klíčový poměr, který udává podíl času, během kterého může zařízení aktivně vysílat v rámci jedné hodiny. Pro frekvenční pásmo 868–868,6 MHz je hodnota klíčového poměru 1 % a pro pásmo 868,7–869,2 MHz je 0,1 %. [21]

2.1 Sigfox

Sigfox je francouzská firma, založená v roce 2009, která zaštiťuje provoz stejnojmenné sítě Sigfox. V jednotlivých státech tuto firmu zastupují jednotliví lokální operátoři. V České republice je to operátor SimpleCell ve spolupráci s firmou T-mobile.



Obrázek 2.1: Mapa pokrytí Evropy a České republiky sítí Sigfox. Levá mapa zobrazuje pokrytí Evropy: modrá barva značí již pokryté oblasti a fialová plánované pokrytí. Na pravé mapě je pokrytí České republiky, kde barva udává počet základních stanic, kterými je oblast pokryta: 3 a více stanic (červená), 2 stanice (zelená) a 1 stanice (modrá). (zdroj: [9] [12])

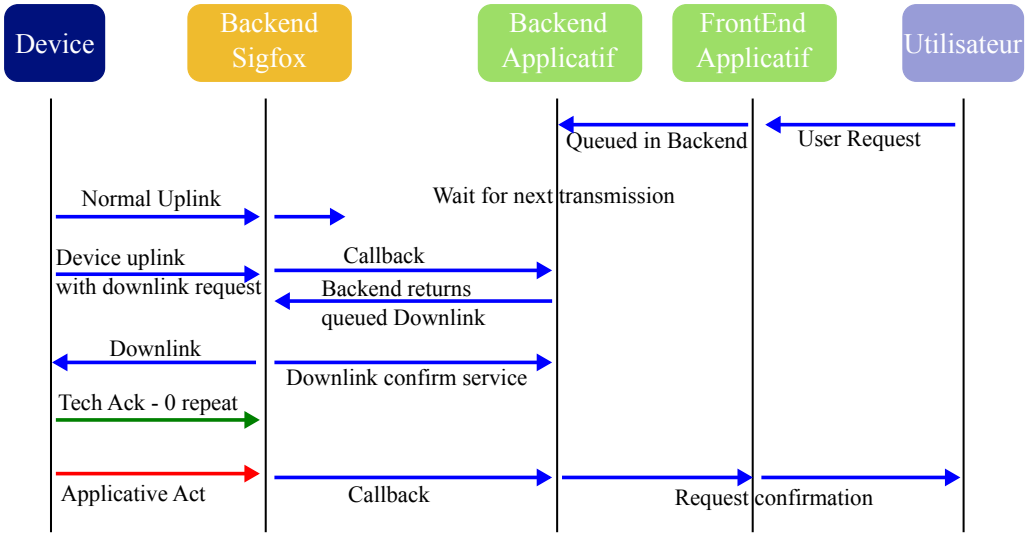
2.1.1 Pokrytí

Sítí Sigfox je v dnešní době pokryto více než 60 zemí světa, přičemž pokryta jsou především velká města a jejich okolí. V Evropě je síť rozšířena především v její západní a střední části, jak je vidět na obrázku 2.1 vlevo, kde modrá barva značí již pokryté oblasti a fialová plánované pokrytí. Pokrytí České republiky je 94 % území a 96 % populace. Jak je vidět na obrázku 2.1 vpravo, je většina území ČR pokryta třemi a více základními stanicemi (červená barva), popřípadě dvěma stanicemi (zelená barva) nebo pouze jednou stanicí (modrá barva). V oblastech, které jsou pokryty více než jednou stanicí bude síť dostupná i při výpadku některé z nich.

Základní stanice dokáže pokrýt oblast 3–10 km v zástavbě, 30–50 km ve volném prostoru a až 200 km na přímou viditelnost. Ve volném prostoru tedy umožňují lepší pokrytí než mobilní sítě. Traumabody umístěné na území bývalého újezdu Brdy jsou příkladem pokrytí rozsáhlé oblasti, kde není dostatečné pokrytí mobilním signálem. Tyto body umožňují přivolání pomoci ke konkretnímu bodu [15]. Maximální počet zpráv na jednu základní stanici je 9 milionů zpráv denně [17]. Pokud uživatel potřebuje vylepšit signál v budově, popřípadě na nepokrytém území, může si koupit Micro Base Station s cenovkou kolem 390 €, která zprostředkuje komunikaci mezi Sigfox cloudem a zařízeními [11]. Tato stanice však dokáže přijímat pouze 70 000 zpráv denně. Pro vývojáře je navíc dostupný i emulátor prostředí Sigfox SDR Dongle, který slouží pro testovaní sítě mimo pokrytí skrze USB rozhraní [10].

2.1.2 Frekvence

Vysílací frekvence je v Evropě v bezlicenčních pásmech 868 MHz a ve zbytku světa 902 MHz. To odpovídá rozsahu frekvencí pro Evropu 868 MHz až 868.2 MHz a ve zbytku světa 902 MHz až 928 MHz. Šířka jednoho kanálu je 100 Hz, což v Evropě udává potenciál mít až 2000 kanálů. Topologie sítě je typu hvězda, kdy každé zařízení je připojené k centrálnímu prvku (bráně). [3]



Obrázek 2.2: Schéma komunikace zařízení se Sigfox cloudem a koncovým serverem. (zdroj: [5])

Maximální počet zpráv je 140 odeslaných a 4 přijaté, viz tabulka 2.2. Velikost odeslané zprávy je 0–12 bajtů a rychlost odesílání může dosáhnout až 100 bit/s. Přijatá zpráva může mít maximální velikost 4 bajty. Rychlost příjmu zprávy se odvíjí od rychlosti poslední odeslané zprávy. Zprávy se odesílají vždy tak, že se odešle jeden frame na určité frekvenci a poté se pošlou další dvě repliky na různé frekvenci a v různém čase.

2.1.3 Komunikace

Komunikační protokol umožňuje dva způsoby komunikace, a to jednosměrnou a obousměrnou, viz obrázek 2.2. Role zařízení je aktivní, tzn. zařízení inicializuje komunikaci se sítí Sigfox. Role serveru (aplikace) je pasivní, server musí pouze čekat na zařízení až inicializuje spojení. Komunikace probíhá bez záruky doručování zpráv (podobně jako u internetového protokolu UDP), tedy nedozvíme se, zda zpráva byla nebo nebyla doručena do Sigfox cloudu. Zařízení není spárované s žádnou základní stanicí, a tak musí v Sigfox cloudu probíhat i odstraňování duplicitních zpráv.

Při jednosměrné komunikaci se zařízení cyklicky probouzí z režimu spánku, následně odesílá získaná data a přechází zpět do režimu spánku.

Pro obousměrnou komunikaci je potřeba nastavit v hlavičce zprávy příslušný flag, viz datagram v oddíle 2.1.4. Zařízení čeká 20 s od odeslání první části zprávy, zda mu nepřijde odpověď. Tato doba je pevně určená přenosovou rychlostí a dobou, po kterou Sigfox cloud komunikuje s koncovým serverem. Jakmile Sigfox cloud přijme zprávu vyvolá callback pro stáhnutí příslušné zprávy a pokud je zpráva ve správném formátu přepošle ji do koncového zařízení.

Pokud zařízení posílá zprávu s požadavkem na odpověď a daný server neodpovídá nebo vrátí chybný tvar odpovědi, potom se do sítě Sigfox žádná odpověď nepošle a nepočítá se ani do maximálního počtu přijatých zpráv. Tímto způsobem se dá při každém odeslání zprávy dotázat serveru, zda na něm není dostupná nějaká zpráva. Nevýhodou je delší doba běhu zařízení, a tedy i vyšší spotřeba energie. Po úspěšném přijetí stahované zprávy pošle zařízení nazpět tzv. ACK neboli acknowledgement code, čímž zařízení potvrdí, že přijalo zprávu

v pořádku. Součástí této zprávy jsou i informace o zařízení, jako je teplota, síla signálu základní stanice, napětí během odesílání a po odeslání zprávy. Síť Sigfox také umožňuje posílání „keep-alive“ zpráv. Můžou být buď prázdné, nebo mohou obsahovat informace o teplotě, kontrolní hodnotu a stav napětí během odesílaní a po odeslání zprávy.

Zabezpečení přenášených dat Sigfox standard nedefinuje, ale může být prováděno end-to-end šifrování na aplikační úrovni. Přenos dat je zabezpečen pomocí hashe z privátního klíče uloženého v nepřepisovatelné paměti tak, aby nešlo zprávu podvrhnout jiným zařízením.

Znemožnit zařízení odesílání zpráv lze jen velmi těžko. Útočník by musel zarušit celé pásmo, jelikož zařízení pošle jednu zprávu na 3 různých frekvencích. Navíc toto pásmo je neustále monitorováno jak firmou SimpleCell, tak i ČTÚ.

2.1.4 Datagram

Velikost datagramu pro síť Sigfox je minimálně 23 bajtů a maximálně 35 bajtů. Hlavní výhodou speciálně vytvořeného datagramu je menší velikost zpráv než například u protokolu IPv6, který má minimální velikost zprávy 40 bajtů.

Uplink datagram

Pr	FT	LI	BF	REP	MC	ID	Payload	AUTH	CRC
19 b	13 b	2 b	1 b	1 b	12 b	32 b	0–12 B	2–5 B	2 B

Downlink Datagram

Pr	FT	ECC	ID	MC	Payload	ID	AUTH	CRC
91 b	13 b	4 B	4 B	2 B	0–8 B	4 B	2–5 B	1 B

Tabulka 2.1: Sigfox Datagram pro downlink a uplink. (zdroj: [13])

Pr *Preamble* je bitové pole, které slouží k synchronizaci příjmu zprávy.

FT *Frame type* je bitové pole obsahující specifickou hodnotu podle velikosti zprávy a pořadové číslo opakování odeslané zprávy specifické pro uplink a downlink.

LI *Lenght Indicator* určuje délku zprávy podle velikosti paylodu.

BF *Bidirectional Frag* indikuje jakým směrem půjde komunikace: 0 pro odesílaní a 1 pro obousměrnou komunikaci.

REP *Repeated Flag* je automaticky nastaven na 0.

MC *Message Counter* je počítadlo odeslaných zpráv na straně zařízení. Všechny opakované zprávy mají stejnou hodnotu počitadla (podle toho se dá poznat zda na základní stanici přišla stejná zpráva nebo už nová).

ID *Identifier* je jednoznačné identifikační číslo zařízení ukládané jako little-endian, tedy od nejméně významného bitu po nejvíce významný bit.

Payload Uživatelská zpráva.

AUTH *Authentication* je hash, vypočítaný z privátního klíče, zapsaný v nepřepisovatelné paměti.

CRC *Error detection field* obsahuje kontrolní součet zprávy, který určuje zda zpráva přišla neporušená. Používá se polynomiální generátor, kterému je předána celá zpráva. Výsledek je nakonec s hodnotou 0xFFFF proveden s funkcí XOR.

ECC *Downlink error correction* je cyklický samoopravný kód využívající algoritmus BCH15-11, který dokáže opravit chybu při příjmu zprávy.

2.1.5 Aktivace zařízení

Při koupi zařízení dostává uživatel také jeho unikátní identifikátor Device ID (obdoba MAC adresy u IP datagramu) a PAC (Portability Access Code) kód, kterým se prokazuje při aktivaci služby, případně převodu zařízení na jiného vlastníka. Tyto údaje zadá uživatel na adrese Sigfox cloudu[1] spolu s přihlašovacími údaji. Tím uživatel získá přístup do webového rozhraní služby Sigfox.

2.1.6 Rozhraní s cloudem

Všechna příchozí data a logy k jednotlivým callbackům jsou na stránkách Sigfox cloudu uložena po dobu jednoho roku. Data lze procházet ve webovém rozhraní, lze je stáhnout ve formátu CSV, případně je lze přeposílat na server zákazníka pomocí callbacků.

Sigfox cloud má několik předdefinovaných callbacků například pro Microsoft Azure, Amazon cloud nebo IBM Watson. Pro přeposílání dat na vlastní server je možné vytvořit vlastní callbacky. Vlastní callbacky lze posílat pomocí HTTP, HTTPS nebo SMTP protokolu. U HTTP/S callbacků lze vybírat z metod POST, GET nebo PUT. Data odesílaná pomocí jednotlivých callbacků si lze jednoduše definovat. Lze posílat Device ID, čas zaznamenání zprávy, ID základních stanic, které zprávu přijaly, sílu signálu při příjmu zprávy nebo zpoždění atd. Uživatel může mít nastaveno více callbacků pro určitou skupinu zařízení. Chce-li uživatel odesílat data ze serveru do zařízení vybere jeden z callbacků, který při obdržení zprávy ve správném formátu ji přepošle k jednotlivým zařízením. Uživatel si může nastavit kdy se zprávy odesílají buď při příjmu dat, nebo při nějaké chybě.

2.1.7 Cena

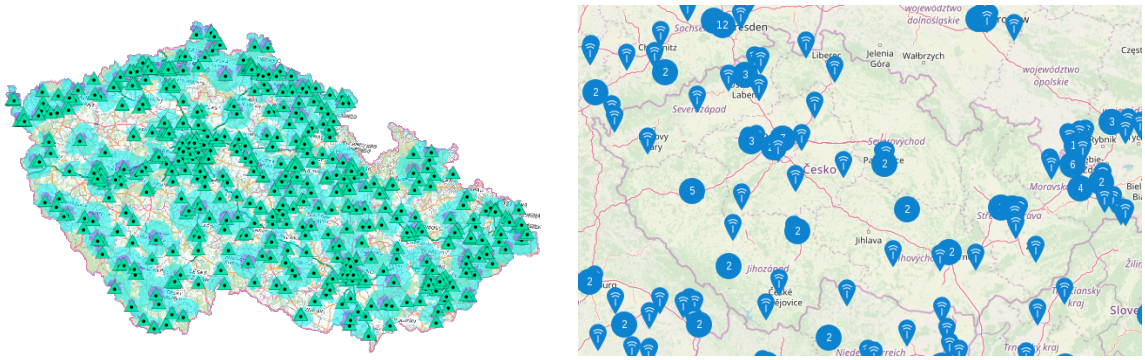
Při koupi všech certifikovaných devkitů získá uživatel licenci Platinum na rok zdarma. Pro nákup licencí má Sigfox čtyři úrovně předplatného, které platí po dobu jednoho roku, viz tabulka 2.2. V každé zemi se o distribuci licencí stará lokální operátor, u nás například SimpleCell. Cena v tabulce 2.2 je orientační a záleží na požadavcích jednotlivých firem. Po vypršení roční licence pro testovaní, výuku či pilotní projekt nabízí SimpleCell reaktivaci zdarma [16]. V síti Sigfox neplatí žádný roaming, tedy čidlo se může připojit u jakéhokoliv operátora bez dodatečných poplatků.

Cena jednoho senzoru je mezi 5–10 USD a ceny antén se pohybují podle jejich kvality v rozmezí 3–15 USD. Dokumentaci k protokolu poskytuje Sigfox zcela zdarma. Výrobci, kteří splní certifikační podmínky, mohou bez omezení vyrábět zařízení připojující se do sítě Sigfox. Jsou tři úrovně certifikace, kterou nabízí například český SimpleCell. Certifikace P1 slouží pro certifikaci modemů či modulů a stojí jednorázově 7500 €. Certifikace P2 je certifikace pro koncová zařízení a testuje zda zařízení vysílá správně do všech směrů a stojí jednorázově 2500 €. Certifikace P3 slouží pro certifikaci univerzální IoT platformy, kdy zařízení je přidáno do katalogu podporovaných modulů a stojí jednorázově 1500 €. [16]

[1] ADRESA SIGFOX CLOUDU

Úroveň předplatného	max uplink	max downlink	cena <1000	cena/zprava
Platinum	140	4	193	1.37
Gold	100	2	151	1.51
Silver	50	1	124	2.48
One	2	0	83	41.5

Tabulka 2.2: Cena licencí služby Sigfox (cena v Kč/rok pro méně než tisíc licencí)(zdroj: [14])



Obrázek 2.3: Mapa pokrytí České republiky sítí LoRaWAN[3]. Vlevo jsou zobrazeny jednotlivé vysílací stanice provozované Českými Radiokomunikacemi a modré plochy znázorňují oblast, kterou tyto stanice dokážou pokrýt. Na mapě vpravo je vidět pokrytí stanice komunitní sítí The Thing Network, kterou jsou pokryta především krajská města.

2.2 LoRaWAN

LoRa (Long Range) je patentovaná bezdrátová komunikace nyní vlastněná firmou Semtech. Používá rádiovou modulaci pro vytváření spojení na dlouhé vzdálenosti. LoRa má několik standardů, jedním z nich je síť pro IoT jménem LoRaWAN definující komunikační protokol a síťovou architekturu. V České republice provozují tuto síť České Radiokomunikace (CRA) nebo The Things Network (TTN) jako komunitní síť. Síť TTN je komunitní, otevřená, nízkonákladová a decentralizovaná infrastruktura pro IoT, vlastněná a provozovaná uživateli. Společnost vznikla v roce 2015 jako iniciativa. Pro pokrytí jednoho města stačí kolem 10 základních stanic. Jednotlivé standardy schvaluje asociace LoRa Alliance, která sdružuje kolem 100 operátorů ve více než 50 zemích po celém světě, viz obrázek A.1.

2.2.1 Pokrytí

LoRaWAN od Českých Radiokomunikací pokrývá 70–75 % obyvatel České republiky. Síť pokrývá především hustě obydlené oblasti, jak je vidět na obrázku 2.3 vlevo, kde jednotlivé body jsou vysílací stanice a modrá plocha znázorňuje oblast pokrytou těmito stanicemi. Je vidět, že pokrytí venkova nebo neobydlených oblastí je buď žádné, nebo velmi slabé. Komunitní síť TTN tvořená stanicemi uživatelů má pokrytí po celém světe, jak je vidět na obrázku A.2. V ČR je pokrytí velmi slabé a pokryta jsou převážně krajská města, jak je vidět na obrázku 2.3 vpravo. Za pokrytím většiny území stojí komunita (např. Praha),

[3] https://www.cra.cz/ – je nutné být přihlášen

jednotlivci, případně města (např. v roce 2018 touto technologií pokrylo své území Nové Město na Moravě).

Jelikož LoRaWAN není proprietární řešení, typy a vlastnosti základních stanic se můžou značně lišit. Obecně se dá ale říct, že dosah sítě je v husté městské zástavbě 3–5 km a ve volném prostoru kolem 20 km. Za vhodných podmínek a při přímé viditelnosti vysílače, například za pomoci výškového balonu, lze docílit dosahu ve stovkách kilometrů [18]. Pokud uživatel chce rozšířit nebo si udělat svoji soukromou síť LoRaWAN, může si koupit buď základní stanici s cenovkou kolem 1500 USD nebo z jednoho vysílače udělat přijímač, případně lze použít jeden vysílač jako opakovač, a tím pokrýt i větší území.

2.2.2 Frekvence

Frekvence vymezená pro provoz sítě je v Evropě 868 MHz, v Severní Americe 915 MHz a v Asii 433 MHz. Rozsahu frekvencí v Evropě je od 867 MHz až 869 MHz. Šířka jednoho kanálu je 125 kHz až 250 kHz. V Evropě je definováno 10 kanálů, z toho 8 s vícenásobnou rychlostí, jeden vysokorychlostní a jeden samostatný FSK kanál (klíčování frekvenčním posuvem). Topologie sítě je typu hvězda, případně několik do sebe zanořených architektur typu hvězda [6].

Maximální počet odeslaných a přijatých zpráv je prakticky neomezený, záleží samozřejmě na samotném operátorovi, jaký ceník a omezení si nastaví. Typicky se počet odeslaných zpráv pohybuje v řádu stovek zpráv za den a počet přijatých v řádu desítek zpráv denně. Maximální velikost odeslané a přijaté zprávy je 243 bajtů, rychlost odesílání se pohybuje v rozmezí od 300 bit/s do 50 kbit/s.

2.2.3 Komunikace

Standard LoRaWAN definuje tři třídy komunikace mezi zařízeními a základními stanicemi. Třída A je určena pro zařízení s omezenou spotřebou elektrické energie a pro posílaní krátkých zpráv. Pokud zařízení pouze odesílá data, tak je odešle a následně se uspí do dalšího odesílání zprávy. Při obousměrné komunikaci zařízení odešle zprávu a potom čeká dvě časová období na příjem zprávy. Následně musí vydržet, dokud mu zařízení nepošle zprávu, a až potom může zařízení přeposlat daná data ve frontě.

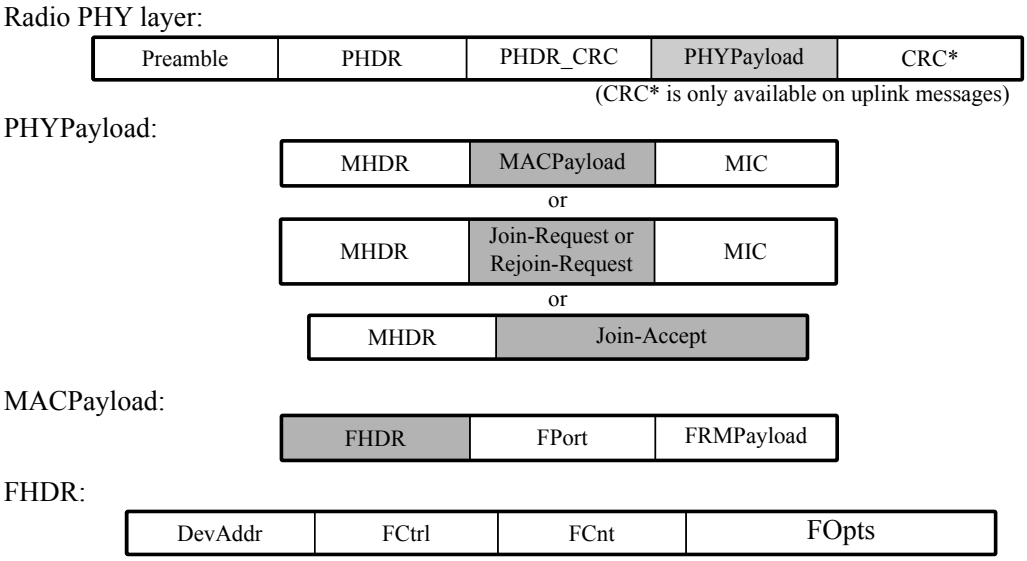
Třída B je podobná jako třída A s tím rozdílem, že zařízení se navíc probouzí v plánovaných časech, které jsou synchronizované se základní stanicí. Zařízení po probuzení čeká dvě časová období a poté se znovu uspí.

Třída C je pro zařízení s připojením do elektrické sítě nebo s dostatečným napájecím zdrojem. Zařízení se neuspává a tak přijímá zprávy po celou dobu. Příjem zpráv je vypnut pouze při odesílání zpráv. [7]

Na šifrovaní je u LoRaWANu kladen velký důraz a je prováděno na dvou vrstvách: na síťové i na aplikační. Síťová vrstva zabezpečuje nepodvrženost zprávy. Na aplikační vrstvě jsou data šifrována pomocí šifry AES (Advanced Encryption Standard) a 128b klíče.

2.2.4 Aktivace zařízení

Aktivovat zařízení je možné dvěma způsoby aktivace: OTAA a ABP. OTAA (Over-The-Air Activation) aktivace probíhá na bázi „handshaku“ mezi zařízením a sítí. Zařízení potřebuje pro připojení do sítě DevEUI, AppEUI a AppKey. Po obdržení join requestu server vygeneruje pomocí AppKey session key a ten následně vrací v join response s hodnotami NwkSKey a AppSKey. Tento klíč si zapamatuje a pro každé další spojení ho používá. Uživatel si může



Obrázek 2.4: Datagram sítě LoRaWAN pro Uplink a Downlink. (zdroj: [2])

zvolit expiraci tohoto klíče buď po určité době, nebo po určitém počtu poslaných zpráv. Pokud tento klíč ztratí nebo uběhla doba expirace, musí znovu proběhnout handshake. Výhoda tohoto způsobu je, že session key nemůže být odcizen ještě před aktivací a pokud by byl přesto odcizen, bude po expiraci vygenerován nový. Nevýhodou je, že ne všechna zařízení tuto aktivaci podporují, a také vyšší spotřeba energie.

ABP (Activation By Personalisation) neprovádí „handshake“ a hodnoty NwkSKey a AppSKey se nastavují na konstantní hodnotu. Výhoda je, že zařízení nepotřebuje znát funkce na provádění handshaku, ušetří se čas a energie pro odeslání a příjem zpráv. Nevýhoda je, že tento session key může být kdykoliv odcizen jak před spuštěním čidla, tak během fungování. Uživatel musí potom tento klíč na všech zařízeních změnit ručně. [19]

2.2.5 Datagram

Datagram pro komunikační protokol LoRaWAN [1] se skládá ze tří vrstev: fyzické, MAC a aplikační vrstvy. Datagram je graficky znázorněný na obrázku 2.4. Fyzická vrstva (Radio PHY layer) se skládá z těchto částí:

- *Preambule*, která většinou obsahuje 8 znaků a slouží pro kontrolu, zda je vysílací pásmo volné, a také pro synchronizaci komunikace. Aby se povedla synchronizace, potřebuje přijmout alespoň 5 znaků. Konec preambule je signalizován obráceným signálem, který říká vysílači, že je zahájeno vysílání.
- *Physical header* (PHDR), který má velikost 2 bajty a obsahuje velikost užitečné informace.
- *Physical header cyclic redundancy check* (PHDR_CRC) je kontrolní součet PHDR o velikosti 4 bity.
- CRC má velikost 2 bajty a je odesílán pouze při příjmu zpráv.

MAC vrstvu (PHYPayload) tvoří:

- *MAC header* (MHDR), který má velikost 1 bajt a obsahuje informace o verzi komunikačního protokolu a typu spojení (uplink, dowlink). Dále uvádí, zda se jedná o datový nebo řídící rámec.
- *Message Integrity Code* (MIC) je hash části MHDR a MACPayload vypočítaný pomocí klíče NwkSKey a slouží jako ověření proti padělání zprávy. Pro aktivaci metodou OTAA se join request posílá místo MAC Payload části. V případě potvrzení aktivace (Join-Accept) se vrací MIC v zašifrované podobě společně s NwkSkey a AppSKey.

Aplikační vrstva (MACPayload) obsahuje:

- *frame header* (FHDR), který se skládá z:
  - *Device address* (DevAddr) o velikosti 4 bajty. DevAddr obsahuje dvě části: prvních 8 bitů identifikuje síť a zbylé bity jsou automaticky přiřazeny pro identifikaci zařízení v síti.
  - *Frame control* (FCtrl) o velikosti 1 bajt obsahuje informace o řízení sítě (datová rychlost, potvrzení předchozí zprávy, více zpráv pro spojení).
  - *Frame counter* (FCnt) o velikosti 2 bajty udává pořadí odeslané zprávy.
  - *Frame options* (FOpts) o velikosti 0–15 bajtů obsahuje informace pro vylepšení následujících přenosů.
- *Frame Port* (FPort) o velikosti 1 bajt informuje o typu aplikace.
- *Frame payload* (FRMPayload) obsahuje užitečnou informaci šifrovanou algoritmem Advanced Encryption Standard (AES) s aplikačním klíčem (AppKey) o délce 128 bitů.

2.2.6 Rozhraní s cloudem

Rozhraní služby CRA umožňuje zatím použít pouze dvě rozhraní pro komunikaci. První je metoda REST neboli přeposílání příchozích zpráv na server zákazníka (endpoint). Zpráva je ve formátu JSON a obsahuje jak informace přijaté od čidla, tak seznam základních stanic, které tento signál přijaly. V dnešní době je možné zadat adresu koncového bodu pouze se zabezpečeným přenosem informací přes HTTPS. Toto rozhraní nepodporuje všechny možné znaky, které může obsahovat url adresa (např: ∼, !, . . .).

Druhá metoda je přes API, kdy jsou všechna data uložena na serveru CRA. Uživatel si vygeneruje autentizační klíč (token), s jehož využitím následně komunikuje metodou POST s rozhraním databáze. Komunikace probíhá ve formátu JSON a umožňuje i obousměrnou komunikaci se zařízením.

Data přijatá na server CRA můžou být skladována po neomezenou dobu (podle smlouvy). Webové rozhraní umožňuje export do formátu CSV.

Rozhraní služby TTN funguje na bázi modulů, které vytváří sama komunita. Nabízí například rozhraní komunikující přes HTTP nebo různá rozhraní API pro IoT platformy (Ubidots). Rozhraní přes HTTP probíhá metodou POST ve formátu JSON a umožňuje jak přijímaní, tak i odesílání zpráv. Data jsou na serveru TTN uložena po dobu sedmi dnů, v případě potřeby lze tuto dobu za určitý poplatek prodloužit.

2.2.7 Cena

Cena přístupu do sítě LoRaWAN CRA je závislá na objemu a počtu přenesených zpráv. Platí se měsíční paušál za každé zařízení, které odeslalo alespoň jednu zprávu do sítě. Pro

studijní nebo testovací účely je možné objednat službu Freemium, čímž zákazník získá přístup do sítě na měsíc zdarma s možností si vyzkoušet rozhraní pro IoT s limitem 360 odchozích zpráv a 36 příchozích zpráv za den. Přístup do komunitní sítě TTN je zdarma pro malé množství koncových zařízení a základních stanic. Pro připojení většího množství zařízení a stanic je tato služba zpoplatněna. V rámci poplatku získá uživatel nástroje pro správu velkého počtu zařízení a delší dobu archivace přijatých zpráv na serveru.

Cena základní stanice je různá v závislosti na jejích parametrech (kvalita signálu, umístění, počet zařízení). Dříve se cena pohybovala v řadu 1000 € za základní stanici. Díky TTN, která žádala na serveru Kickstarter[4] o skupinové financování (crowdfunding) na vývoj základní stanice s pětinovou cenou, se dnešní ceny základních stanic pohybují kolem 100 €, případně lze vytvořit základní stanici z koncového zařízení se základními deskami z rodiny Raspberry Pi. Ceny koncových zařízení se pohybují mezi 10–30 €. Cena se odvíjí od kvality modulů a podpory jednotlivých standardů.

[4] https://www.kickstarter.com/

Kapitola 3

Hardware

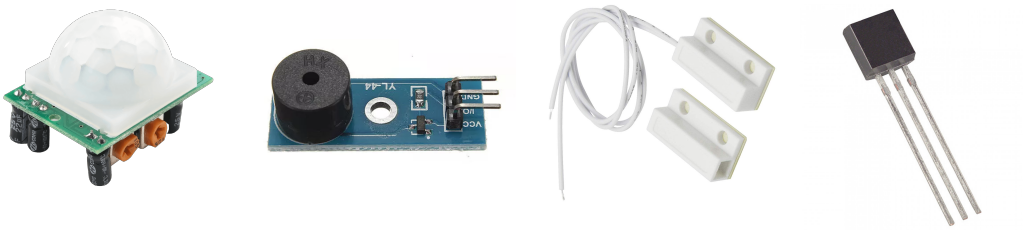
V kapitole je popsán hardware použitý pro stavbu zabezpečovacího systému. Jedná se o senzory detekující pohyb s minimální spotřebou. Jsou zde popsané vývojové desky a jejich nejznámější zástupci.

3.1 PIR detektor

PIR – pasivní infračervený detektor (HC-SR501, obr. 3.1) funguje na principu pyroelektrického jevu. Na čidlu je optika, která směřuje jednotlivé infračervené paprsky do PIR elementu. PIR element je polovodičová součástka z lithia a tantalu, která po ozáření infračerveným zářením generuje elektrický náboj. PIR senzor je citlivý ve velkém vlnovém rozsahu, proto je aplikován filtr na rozsah 8 µm až 10 µm, přičemž lidské tělo vydává 9,4 µm. Senzor se připojuje na 3 piny: 5 V, GND a výstupní pin. Výstup se může pomocí přepínače na desce upravit tak, aby se zapínal buď po každé hraně, nebo pouze při změně hrany. Na modulu jsou dva potenciometry, kterými lze upravit práh detekce a délku zpoždění čidla na výstupu. [4]

3.2 Magnetický snímač s jazýčkovým kontaktem

Jazýčkový kontakt je mechanický spínač ovládaný magnetickým polem pomocí permanentního magnetu (obr. 3.1). Jazýčkový kontakt obsahuje dva feromagnetické plíšky (jazýčky), které jsou od sebe vzdáleny jen několik setin milimetru a jsou hermeticky uzavřeny ve skleněné trubičce. Pokud se dostane jazýčkový kontakt do magnetického pole, feromagnetický



Obrázek 3.1: Na obrázku jsou zleva: PIR detektor HC-SR501, akustický bzučák YL-44 a magnetický snímač s jazýčkovým kontaktem, teplotní čidlo DS18B20.

materiál jazýčku zesílí účinnost magnetického pole, čímž dojde k vytvoření dvou magnetů, které se protikladnými póly přitahují, a vznikne tak vodivé spojení [20].

3.3 Akustický bzučák

Aktivní akustický bzučák (YL-44, obr. 3.1 uprostřed) obsahuje spínací NPN tranzistor a samotný bzučák. Aktivní bzučák znamená, že vydává jednotný tón okolo 2 kHz při logické 1. Tudíž se nemusí generovat signál na vstup bzučáku. Bzučák má 3 piny VCC (3.3-5 V), GND a ovládací pin, který zapíná tranzistor. [8]

3.4 Komunikační modul IOT LPWAN SigFox

Komunikační modul, IOT LPWAN SigFoxK zprostředkovává komunikací se sítí Sigfox. Modul má 6 pinů: jeden slouží k připojení externí antény, RX a TX pro sériovou komunikaci přes rozhraní UART, dva pro napájení GND a VCC (3.3 V) a poslední pin slouží k probouzení modulu z režimu spánku (deep sleep).

3.5 Teplotní čidlo DS18B20

Teplotní čidlo DS18B20 od firmy Maxim (dříve Dallas) je mezi uživateli velice oblíbené. Toto čidlo umožňuje měřit teplotu v rozmezí −55 °C až 125 °C s přesností 0,5 °C. K pinům desky se připojuje pomocí tří vodičů: VCC, GND a DATA. Čidlo lze také zapojit s využitím jen dvou vodičů. Kladné napětí je přivedeno pullup rezistorem o velikosti 4,7 kΩ na datový pin a na ostatní piny je přivedena zem. Toto zařízení komunikuje přes rozhraní 1-wire, které umožňuje připojit až stovky čidel na jeden port.

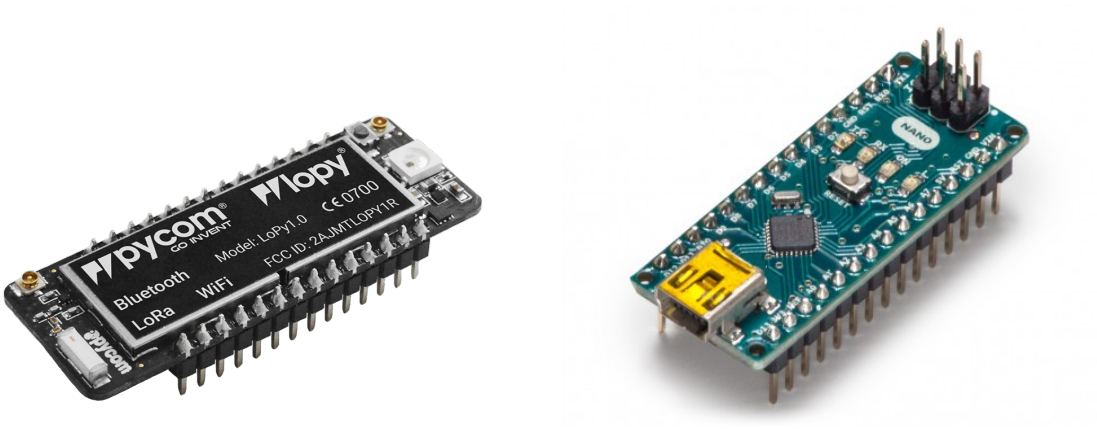
3.6 Arduino

Arduino je otevřená (open-source) vývojová platforma (obr. 3.2 vpravo), jejíž základem jsou jednodeskové počítače založené na mikrokontrolerech ATmega od firmy Atmel. Oficiálních moduly se vyrábí v mnoha variantách:

- Arduino Uno,
- Arduino Mega,
- Arduino LilyPad,
- Arduino Nano,
- a další.

Liší se velikostí, typem mikrokontroleru, výstupními porty, velikostí pamětí a dalšími parametry. Mimo tyto moduly existují i „klony“, kdy jedna ze základních součástek je nahrazena jinou.

Funkce Arduino desky lze rozšiřovat pomocí „shieldů“. Mezi nejznámější patří například shield pro připojení k internetu, k wifi, pro ovládání stejnosměrných motorů nebo pro získání aktualní polohy modulem GPS.



Obrázek 3.2: Vývojové desky LoPy (vlevo) a Arduino Nano (vpravo).

Naprogramovat desku Arduino lze pomocí jazyků C nebo C++. Ve vývojovém prostředí Arduino IDE je dostupný otevřený programovací framework Wiring, se syntaxí podobnou C++. Wiring umožňuje tvorbu programů běžících na různých mikrokontrolerech (cross-platform).

Arduino Nano je malá vývojová deska s rozměry 18×45 mm. Tato vývojová deska je osazena procesorem ATmega328P běžícím na frekvenci 16 Mhz s logickou úrovní 5 V. Obsahuje SRAM paměť s velikostí 2 kB, EEPROM o velikosti 1 kB a flash paměť o velikosti 32 kB. Pro připojení k počítači obsahuje konektor mini-USB s čipem FTDI FT232RL pro převod USB rozhraní na sériovou linku. Deska je osazena 30 piny, z toho je 14 vstupně-výstupních digitálních pinů, 8 analogových, 1 sériová linka, resetovací tlačítko a napájecí piny s regulátorem napětí pro napájecí napětí 7–12 V.

3.7 LoPy

V srpnu 2015 vznikla firma Pycom, která přišla s modulem WiPy na portál skupinového financování (crowdfunding) Kickstarter. Tento modul byl velice úspěšný a získal podporu od více než 1500 sponzorů. Jak už napovídá název firmy „Py“ jako MicroPython, který je hlavním programovacím jazykem, „com“ jako communication, což napovídá podporu různých komunikačních standardů od Bluetooth až po technologie používané pro IoT.

Základem všech desek je čip ESP32 vyvíjený pro Arduino. Je to nástupce čipu ESP8266, který už nedostačoval výkonem ani konektivitou. Čip obsahuje dvě výpočetní jádra taktovaná na 160 MHz, 512 kB SRAM paměti a 16 MB flash paměti.

V dnešní době firma prodává pět desek – WiPY, SiPy, LoPy (obr. 3.2 vlevo), GPy a FiPy. Jednotlivé desky se od sebe liší hlavně komunikační konektivitou. Například FiPy (five) podporuje 5 IoT standardů (LoRa, Sigfox, Bluetooth, NBIoT a CAT M1). Hlavní programovací jazyk na tvorbu programů pro tyto desky je MicroPython. MicroPython je interpretovaný programovací jazyk odvozený od Python 3. Je napsaný v jazyce C99 a je optimalizovaný pro běh na mikrokontrolerech. Kód lze interaktivně zadávat také do konzole, ke které se lze připojit buď přes sériovou linku, nebo přes internetový protokol Telnet. Nahrávaní zdrojových souborů do paměti zařízení je možné provádět přes sériovou komunikaci přes USB nebo při připojení přes WIFI lze využít FTP server.

K těmto deskám lze také dokoupit řadu rozšiřujících desek. Například deska Pytrack rozšiřuje funkcionalitu o hledaní polohy jak za pomocí GPS, tak pomocí evropské sítě Galileo. Deska Expansion Board přidá rozhraní pro microUSB, slot pro microSD kartu, umožňuje připojení a nabíjení baterie a další.

Kapitola 4

Zabezpečovací modul

Existuje nepřeberné množství zabezpečovacích systémů využívajících mobilní technologie GSM, které mají spotřebu v řádu několika wattů. Při připojení do elektrické sítě tato spotřeba není nijak významná, naproti tomu dlouhodobý provoz takovéhoto zařízení na akumulátor by byl nereálný.

Je možné využít síť typu LPWAN pro vytvoření zabezpečovacího systému? Ano. Tuto technologii s dlouhým dosahem a nízkou spotřebou je možné použít pro střežení objektů na odlehlých místech. Na podzim bývají zprávy o tom, že jsou vykrádány chalupy a zahrádkářské kolonie. Zde by se tato technologie dala použít, protože většina chalupářů na zimu vypíná elektřinu ve svých chalupách a někteří ji ani nemají přivedenou. Také pokrytí těchto oblastí mobilním signálem nebývá dostatečné. Dalším rozhodovacím parametrem by mohla být také cena.

4.1 Registrace a první komunikace

Koupí zařízení firmy PYCOM nezískají uživatelé identifikátory do sítě Sigfox ani LoRaWAN. Nejdříve je nutné zařízení aktualizovat programem, který je ke stažení na stránkách výrobce[1]. Po provedení aktualizace získá uživatel hodnoty jednotlivých identifikátorů. Tyto hodnoty jsou přístupné jako proměnné v interpretu v zařízení. Registrace do služby Sigfox je jednoduchá, stačí vyplnit všechny informace na webové stránce[2]. V Sigfox cloudu byly nastaveny tři callbacky, viz obrázek A.8. První slouží k ukládání dat příchozích od zařízení, druhý slouží pro odesílání zpráv do zařízení a třetí pro příjem chybových hlášení (chybějící zprávy, chyba při přenosu dat). Pro zasílaní zpráv je využívána metoda GET.

Zdrojový kód 4.1 v MicroPythonu ukazuje příklad základní komunikace zařízení LoPy se sítí Sigfox. Pro odeslání zprávy stačí knihovny network a socket. Pomocí knihovny network je nastavena vysílací frekvence pro Evropu. Následně je knihovnou socket vytvořen soket pro Sigfox zprávu a pomocí funkce setbloking lze nastavit, zda chce uživatel vyčkat do odeslaní zprávy. Funkcí setsockopt je nastaveno, zda chce uživatel přijmout zprávu a funkcí send je možné zprávu odeslat.

Registrace do sítě LoRa od CRA je trochu složitější. Po vytvoření uživatelského učtu může uživatel přidávat zařízení. Jsou zde obě možnosti autentizace zařízení, které byly popsány v části 2.2.4 (obrázek A.6). Zatím zde není dořešené EUI, a tak si ho uživatel volí sám (není tedy zaručena jednoznačnost, kterou definuje standard). I u metody ABP

[1] https://docs.pycom.io/gettingstarted/installation/firmwaretool.html
[2] https://buy.sigfox.com/activate

```
from network import Sigfox
import socket
sigfox = Sigfox(mode=Sigfox.SIGFOX, rcz=Sigfox.RCZ1)
s~= socket.socket(socket.AF_SIGFOX, socket.SOCK_RAW)
s.setsockopt(socket.SOL_SIGFOX, socket.SO_RX, True)
s.setblocking(True)
s.send(bytes([0x01]))
print(s.recv(32))
```

Zdrojový kód 4.1: Příklad odeslání a přijetí zprávy službou Sigfox (MicroPython)

```
$data = json_decode(file_get_contents('php://input'),true);
$data=$data["data"];
$ch = curl_init('www.stud.fit.vutbr.cz/~xsadil06/module/cra.php');
curl_setopt($ch, CURLOPT_CUSTOMREQUEST, "POST");
curl_setopt($ch, CURLOPT_POSTFIELDS, $data);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
curl_setopt($ch, CURLOPT_HTTPHEADER, array(
    'Content-Type: application/json',
    'Content-Length: ' . strlen($data))
);
curl_exec($ch);
```

Zdrojový kód 4.2: Přesměrování komunikace na školní server (PHP)

je vyžadováno zadání EUI. Následně je zařízení přidáno a je možné s ním komunikovat. Počet odeslaných a přijatých zpráv lze sledovat ve webovém rozhraní, viz obrázek A.7. Pro vytvoření koncového bodu sítě (endpoit) je nejdříve nutné vytvořit skupinu zařízení a následně je nutné zařízení do této skupiny přiřadit. U koncového bodu sítě se zadá url adresa serveru uživatele; dostupnost serveru lze otestovat pomocí funkce ping. Bohužel nelze používat v adrese URL všechny znaky, proto není možné posílat zprávy přímo na školní server. Tento problém byl vyřešen využitím hostingu u poskytovatele PHP5[3], přes který byla komunikace přesměrována. O celý proces se stará program napsaný v PHP, který nejprve přijme zprávu, následně ji dekóduje z datového formátu JSON a poté data odešle pomocí funkce curl na školní server (zdrojový kód 4.2).

Příklad komunikace se zařízením v síti LoRaWAN je ukázán ve zdrojovém kódu 4.3. Opět jsou využity knihovny network a socket. Pomocí funkce join je nastaven způsob autentizace a její parametry. Dokud neproběhne aktivace, běží smyčka **while**. Funkcí setsockopt nastavíme typ zprávy. Funkcí set_battery_level lze u zprávy nastavit stav baterie: 0 je pro zařízení připojené na stálý zdroj energie, 255 je chyba a hodnoty 1–254 určují po přepočtu nabití baterie odpovídající 0–100 %.

4.2 Pokrytí a dostupnost služeb

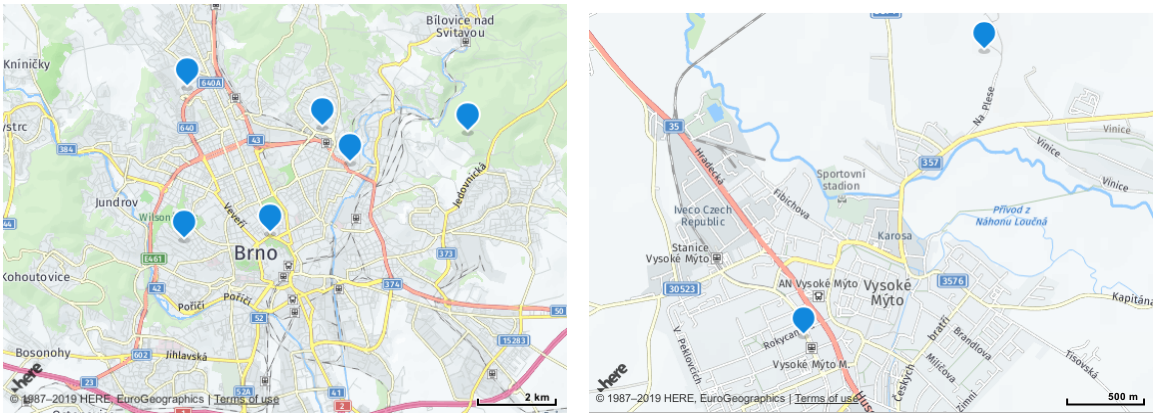
Pro testování spolehlivosti a dostupnosti testovaných sítí byl použit modul LoPy, který má společný vývod antén jak pro síť Sigfox, tak pro síť LoRaWAN. Pro sledování kvality signálu byla použita hodnota *rssi*, což je indikátor síly přijímaného signálu, který udává

[3] https://www.php5.cz/

```
from network import LoRa
import socket
lora = LoRa(mode=LoRa.LORAWAN, region=LoRa.EU868)
lora.join(activation=LoRa.OTAA, auth=(app_eui, app_key), timeout=0)
while not lora.has_joined():
    print("nepřipojeno")
s.setsockopt(socket.SOL_LORA, socket.SO_DR, 5)
lora.set_battery_level(10)
s.setblocking(True)
s.send(bytes([0x01]))
s.setblocking(False)
print(s.recv(64))
```

Zdrojový kód 4.3: Příklad odeslání a přijetí zprávy službou LoRaWAN (MicroPython)

rozdíl RSCP a Ec/lo v jednotkách dBm (decibel na miliwatt), kde RSCP (Recevived Signal Code Power) je užitečný výkon přijatého signálu a Ec/lo je poměr přijaté energie a energie přijatého šumu.

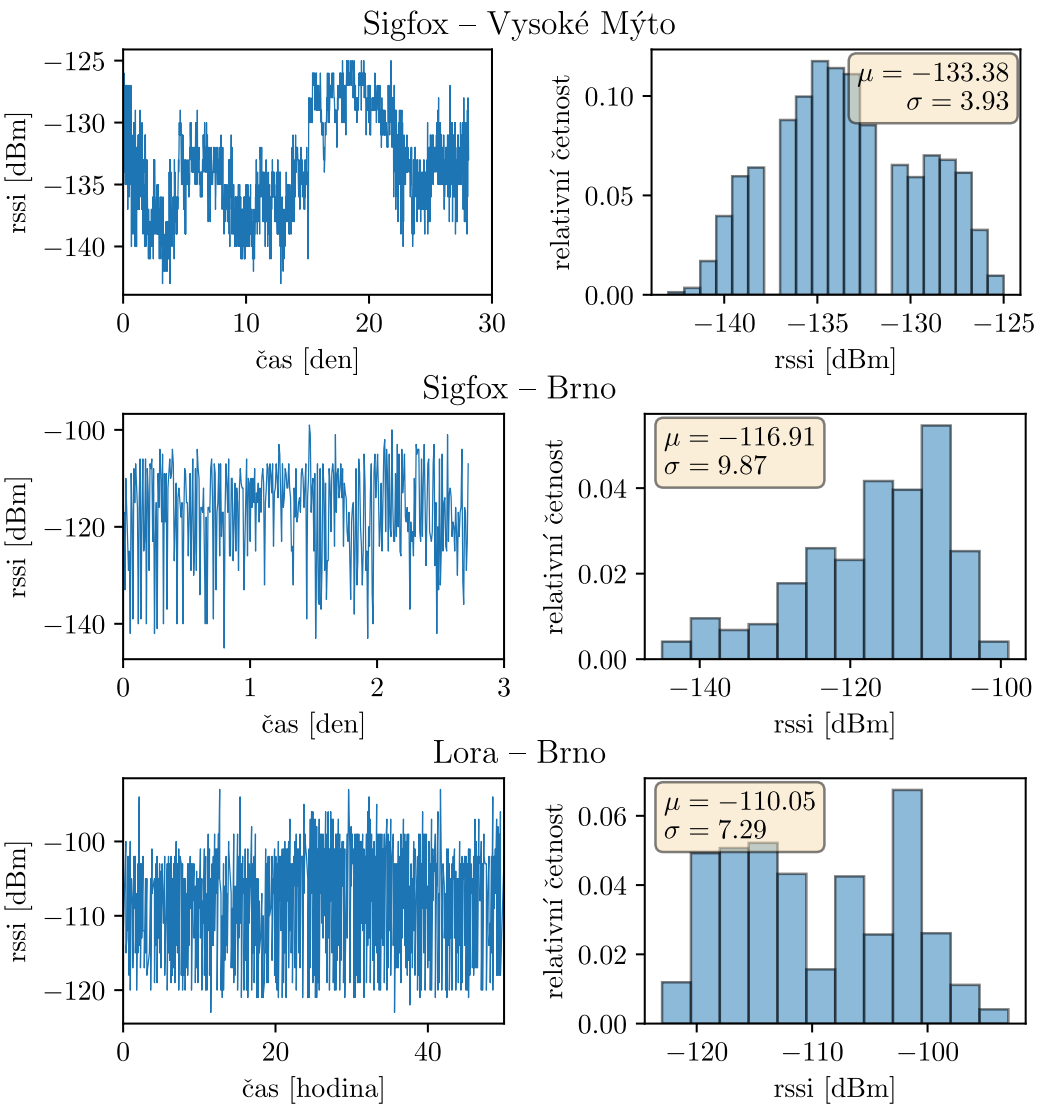


Obrázek 4.1: Pokrytí zájmových oblastí města Brna a Vysokého Mýta vysílači sítě LoRaWAN.

Testování probíhalo na dvou místech České republiky, a to v Brně a ve Vysokém Mýtě. V Brně bylo v dosahu pět vysílačů sítě LoRaWAN, jak je vidět na obrázku 4.1 vlevo, a ve Vysokém Mýtě byl dostupný signál ze dvou vysílačů, viz obrázek 4.1 vpravo. Počet základních stanic sítě Sigfox ve Vysokém Mýtě byl 5 a v Brně 10. Počty stanic sítě Sigfox byly odhadnuty na základě zaznamenaných unikátních identifikátorů. Služba Sigfox neposkytuje na svých stránkách bližší informace o základních stanicích a jejich poloze.

Ve Vysokém Mýtě probíhalo testování v údolí Bláhovského potoka na třech místech: venku, v horním patře a v suterénu zděné budovy. Venku byla síla signálu sítě Sigfox nejlepší a pohybovala se v průměru kolem $-124\,\mathrm{dBm}$. Síla signálu LoRaWAN byla $-118\,\mathrm{dBm}$, ale při aktivaci přes OTAA docházelo často k neuskutečnění aktivace.

Dlouhodobé měření síly signálu sítě Sigfox probíhalo v horním patře budovy. Nepřetržitá délka měření trvala 28 dní. Na obrázku 4.2 nahoře je vidět graf, jak síla signálu kolísá v průběhu měření a histogram naměřených hodnot s průměrnou hodnotou $\mu = -133{,}38\,\mathrm{dBm}$ a směrodatnou odchylkou $\sigma = 3{,}93\,\mathrm{dBm}$. Počet stanic, které přijaly stejnou zprávu, byl

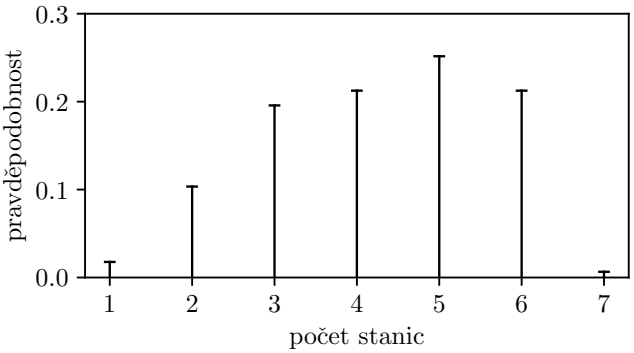


Obrázek 4.2: Naměřená síla signálu v síti Sigfox ve Vysokém Mýtě (nahoře), v Brně (uprostřed), v síti CRA v Brně (dole): levý sloupec ukazuje sílu signálu v čase a pravý sloupec histogram síly signálu za měřené období.

v průměru 2, přičemž maximální počet základních stanic v dosahu je 5. Průměrná ztrátovost paketů byla menší než 1% ze všech odeslaných zpráv.

Testování v suterénu probíhalo krátce a průměrná síla signálu v síti Sigfox byla −141 dBm. Zprávy přijímala pouze jedna základní stanice a ztrátovost zpráv se pohybovala kolem 40 %.

Síla signálu sítě Sigfox v Brně je lepší díky kvalitnějšímu pokrytí oblasti vysílači. Na obrázku 4.2 uprostřed je vidět kolísání signálu v průběhu měření, které trvalo 65 hodin, a histogram naměřených hodnot síly signálu (průměrná hodnota $\mu = -116{,}91\,\text{dBm}$ a směrodatná odchylka $\sigma = 9{,}87\,\text{dBm}$). Průměrný počet stanic, které zachytily stejnou zprávu, byl 6 z celkových 10 základních stanic.

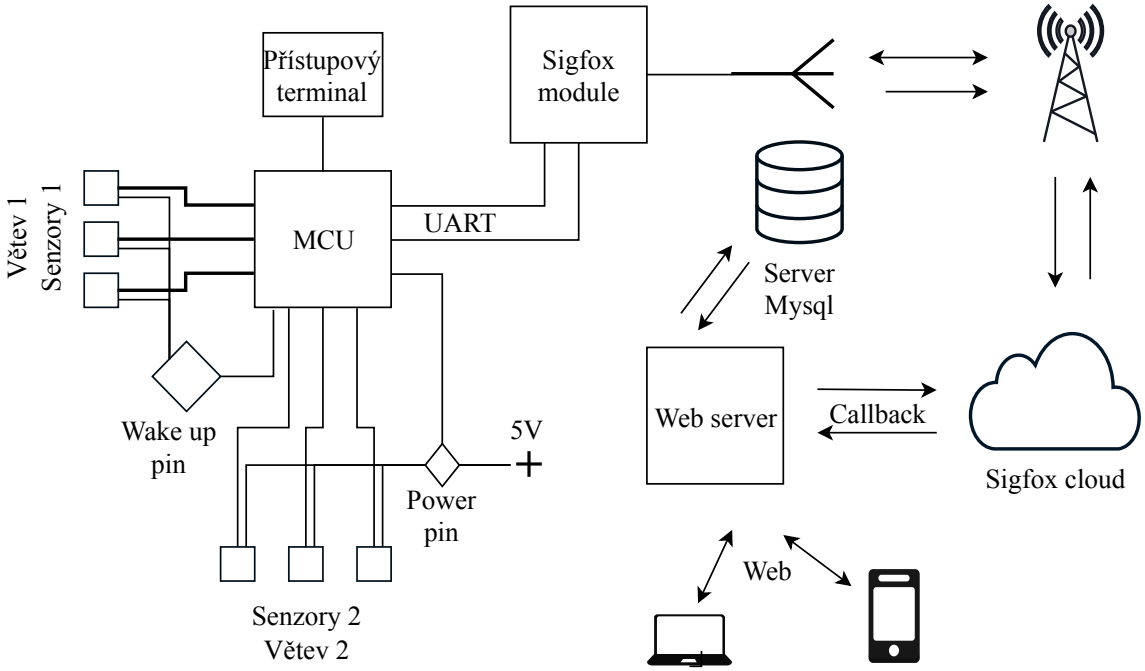


Obrázek 4.3: Pravděpodobnostní funkce počtu stanic sítě LoRaWAN, které přijaly stejnou zprávu.

Doba měření v síti LoRaWAN byla 51 hodin a kvalita naměřeného signálu všech stanic, které přijaly všechny zprávy, byla v průměru $\mu = -110\,\text{dBm}$, viz obr. 4.2 dole. Na obrázku A.9 je barevně odlišena kvalita signálu jednotlivých stanic. Při výběru nejlepší síly signálu z každé zprávy se průměr pohybuje okolo −104 dBm. Na obrázku 4.3 je pravděpodobnostní funkce počtu stanic, které přijaly stejnou zprávu. Za celou dobu testování se neztratila ani jedna zpráva. Z grafu vyplývá, že 25,1 % zpráv bylo zachyceno právě 5 stanicemi, 98,2 % zpráv zachytilo více než 1 stanice a 87,9 % zpráv zachytilo více než 2 stanice.

4.3 Architektura systému

Na obrázku 4.4 je schéma navrženého zabezpečovacího systému. Systém obsahuje dvě větve senzorů. První větev senzorů funguje po většinu času, je připojena na wake-up pin a funguje jako jakýsi budič mikrokontroleru. Tato větev je osazena senzory pohybu. Druhá větev obsahuje zařízení náročná na spotřebu energie a je ovládána jedním pinem. Aktivace této větve nastane až v případě události na první větvi. Mezi senzory umístěné na této větvi je alarm na zahnání útočníka, případně sem lze umístit kameru pro zaznamenání útočníka nebo spínač pro aktivaci osvětlení atd. Vestavěný systém pro vývojovou desku Arduino je napsaný pomocí frameworku Wiring. Tento systém se stará o komunikaci s modulem Sigfox, který slouží pro odesílání a příjem zpráv. Dále deleguje jednotlivá přerušení a cyklicky se probouzí pro odesílání ověřovacích zpráv a podle přijatých zpráv konfiguruje vlastnosti systému.



Obrázek 4.4: Blokové schéma zabezpečovacího systému.

V případě potřeby by mohl být systém rozšířen o třetí větev, která by mohla být osazena dalšími senzory, jako například teplotní a vlhkostní čidla, detektor hladiny vody a plynů, hlásiče požáru, detektor vlhkosti půdy atd. Naměřené hodnoty by se posílaly v rámci tzv. keep alive zpráv.

Systém se aktivuje a deaktivuje pomocí přístupového terminálu. Ten může mít více podob: tlačítko, numerická klávesnice pro zadání pinu, čtečka nebo zařízení s bezdrátová technologie.

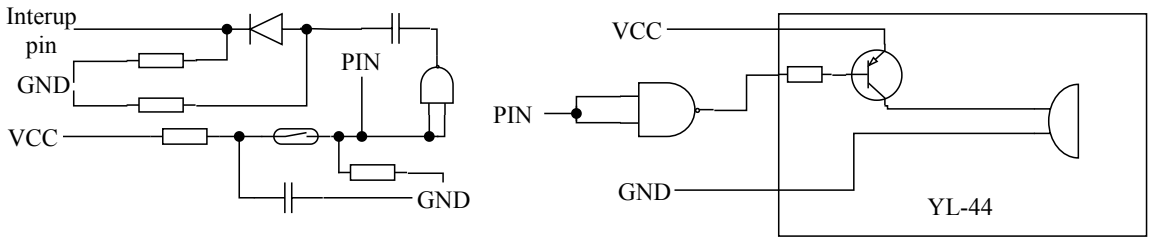
Přes komunikační modul jde signál přes anténu do nejbližších základních stanic. Zde se ke zprávě přidají parametry přenosu zprávy a odesílají se pomocí internetu do Sigfox cloud. Sigfox cloud zprávu zpracuje a pomocí nastavených callbacků zprávu přepošle na koncový server.

Na straně serveru běží PHP aplikace zajišťující příjem a zpracování příchozích zpráv. Data jsou ukládána do perzistentní paměti relační databáze MySQL pomocí PHP rozhraní PDO (PHP Data Objects). Webová aplikace zprostředkovává rozhraní mezi systémem a uživatelem. Přenos informací probíhá pomocí HTTPS a zobrazení pomocí webového prohlížeče.

4.4 Zapojení komponent

Jazýčkový odpor je zapojený na jeden pin s přerušením a na jeden pin bez přerušení. Jak je vidět na obrázku 4.5 vlevo, jedna strana jazýčkového kontaktu je zapojena přes 1 kΩ odpor, který brání probití daného pinu při sepnutí. Dále je tu připojen jeden kondenzátor, který zajistí stabilní logickou hodnotu. Druhá část jazýčkového kontaktu je připojena na kondenzátor o velikosti 1 nF, který slouží jako detekce nástupní hrany. Z pinu s přerušením je odváděna hromadící se energie přes odpor 10 kΩ.

Bzučák je aktivní v logické 0. Při použití funkce tone ve frameworku Wiring je bzučák aktivní v logické 1. Tudíž je dobré bzučák připojit přes nějaký invertor. Zde je vytvořen



Obrázek 4.5: Zapojení jazýčkového kontaktu (vlevo) a bzučáku (vpravo)

hradlem NAND, kde je výstupní pin připojen na vstupní piny hradla a výstupní pin z hradla je připojen na vstupní pin bzučáku.

Komunikační modul je připojen pomocí sériového rozhraní UART a jednoho probouzejícího pinu. Toto rozhraní má přesně definovaný formát komunikace a začíná znaky „AT“. Pro odeslání zprávy je nutné poslat řetězec ve tvaru AT$SF=[zpráva]. Pro obousměrnou komunikaci je třeba přidat na konec zprávy hodnotu 1. Pro uspání komunikačního modulu je potřeba poslat řetězec ve tvaru AP$P=2. Modul také umožňuje čtení různých dat[4] ze svých senzorů nebo z paměti modulu.

4.5 Návrh databáze

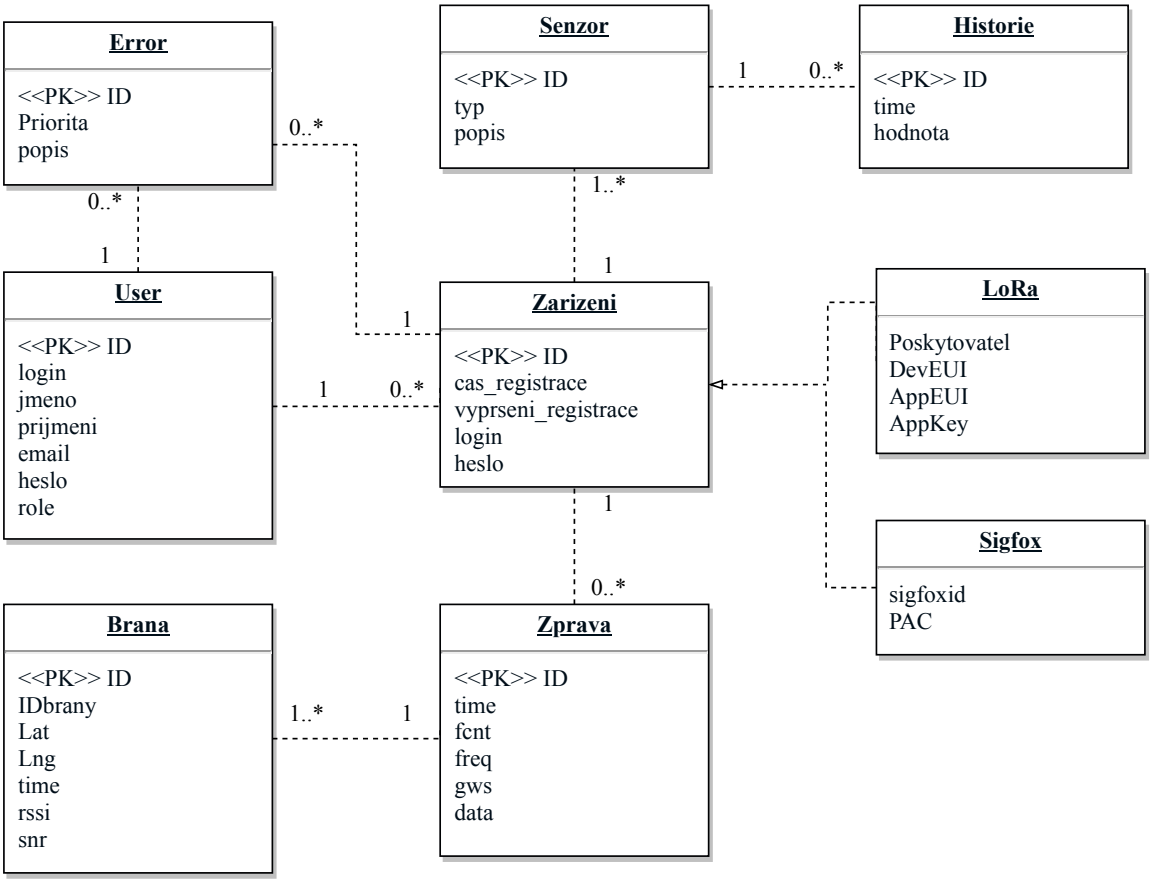
Hlavní částí backendu je relační databáze MySQL pro perzistentní ukládání dat. Jak je vidět na ER diagramu na obrázku 4.6, databáze obsahuje 9 tabulek:

- User – slouží pro ukládaní informací o uživatelích: přihlašovací údaje a role v systému.
- Zařízení – do této tabulky se ukládají informace o zařízení a přihlašovací údaje do jednotlivých rozhraní.
- LoRa – obsahuje jednotlivé parametry pro autentizaci zařízení v síti a poskytovatele dané služby.
- Sigfox – slouží pro ukládání identifikátorů do sítě Sigfox.
- Zpráva – obsahuje data přijaté zprávy a čas přijetí.
- Brána – slouží pro podrobné ukládání informací z každé brány, která přijala danou zprávu.
- Senzor – obsahuje informace o jednotlivých senzorech připojených k zařízení.
- Historie – do této tabulky se ukládají jednotlivé změny hodnot senzorů.
- Error – je logovací tabulka chyb přijatých od operátora.

Každý uživatel má možnost připojení jednoho a více zařízení. Ta pomocí specializace nastaví podle konkrétního operátora a specifickými identifikačními hodnotami.

Jednotlivé příchozí zprávy se ukládají do tabulky Zpráva. Pro zaznamenání chybových stavů je tu tabulka Error. Uchovává se v ní typ chyby, popis chyby a priorita.

[4] https://www.iottoall.com/docs/produkty/0/6/lpwan_sigfox_node_datasheet_v1.pdf



Obrázek 4.6: ER diagram databáze.

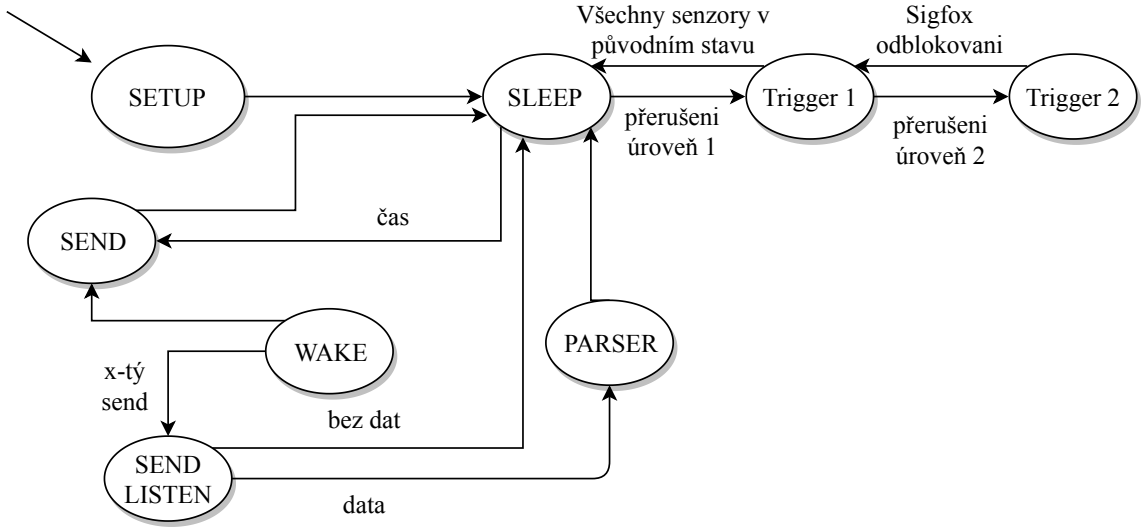
4.6 Návrh GUI

Navrhované grafické webové rozhraní je pro uživatele a administrátora oddělené a je zpřístupněné po přihlášení. Hlavním prvkem rozhraní je menu umístěné v horní části, umožnující orientaci na webové stránce. Implementována je pouze základní funkčnost uživatelského rozhraní potřebná pro fungování zabezpečovacího systému.

Na úvodní stránce administrátorského rozhraní je tabulka s výpisem chyb, viz obrázek A.3. Z úvodní stránky se může uživatel dostat pomocí menu na další stránky, zobrazit si jednotlivé sítě a historii příchozích zpráv s jejich parametry v tabulce (obrázek A.4). U jednotlivých zpráv lze zobrazit mapu se základními stanicemi, které tuto zprávu přijali, a tabulku s podrobnými informacemi o zprávě z každé stanice. Administrátorské prostředí umožňuje správu uživatelů.

Po přihlášeni do uživatelského rozhraní vidí uživatel aktuální seznam senzorů a jejich stav, který je graficky odlišený. Pro přidání nového senzoru do tabulky je zobrazen formulář, který po vyplnění hodnot přidá senzor do tabulky. Po kliknutí na název senzoru se uživateli zobrazí jeho historie s časem a jeho hodnotou, nastavení jednotlivých parametrů přenosu zpráv nebo zařízení. Je také umožněn přistup k historii příchozích zpráv a nastavení akcí pro chybové stavy. V záložce nastavení si uživatel nastaví, jak často chce posílat zprávy, zda je zařízení aktivní.

4.7 Konečný automat



Obrázek 4.7: Konečný automat pro vestavěný systém

Po startu se zařízení dostane do stavu SETUP a nastavuje jednotlivé piny, kontroluje funkčnost jednotlivých senzorů a odesílacího modulu. Pokud vše proběhne v pořádku, přesune se do stavu SLEEP, kdy nejdříve uspí vysílací modul a následně samo sebe. Z tohoto stavu se v pravidelných intervalech budí do stavu WAKE k odeslání „keep alive“ zprávy. Pomocí jednoho z pinů zapne vysílací modul a pokud je nastavený na odeslání nějaké hodnoty senzoru, tak přečte daná data. Pokud pouze odesílá zprávu, přejde do stavu SEND, vytvoří a odešle zprávu. Počká dokud nepřijde z vysílacího modulu potvrzovací odpověď, že zpráva byla odeslaná, a přejde do stavu SLEEP. Při obousměrné komunikaci přejde do stavu SEND/LISTEN, vytvoří zprávu a odešle ji do modulu. Pokud nepřijde odpověď, přechází do stavu SLEEP. Přijde-li odpověď, přechází do stavu PARSER, ve kterém dekóduje příchozí zprávu, upraví parametry aplikace a přejde do stavu SLEEP.

Pokud přijde přerušení z prvního pinu, přejde do stavu TRIGGER1 a zapne druhý okruh senzorů. Pokud je nastaveno odeslání zprávy, odešle zprávu o probuzení. Zapíše, který z připojených pinů vyvolal probuzení, a poté se zařízení znovu uspí. Pokud přijde přerušení z prvního okruhu a je to znovu nástupní hrana, poznamená si pin a zase se uspí. Jsou-li všechny piny v logické 0, tak se vypne druhý okruh senzorů a znovu se uspí.

Přerušení z druhé řady senzorů znamená hlavní nebezpečí. V takovém případě se může zapnout další okruh, který bude sloužit jako poplašný systém. V takovém případě se zařízení neuspává. Čeká, dokud mu nepřijde informace z vysílacího modulu, zda to byl oprávněný nebo neoprávněny přístup, a podle toho se buď uspí nebo zkontroluje situaci ve střeženému objektu.

Z každého stavu se může dostat do stavu FAIL. Při problému s komunikačním modulem může zapnout informační led diodu a nadále pokračuje v kontrolování jednotlivých senzorů. V případě problémů v první řadě senzorů, které neovlivňují funkci ostatních senzorů na dané větvi, zařízení informuje pomocí komunikačního modulu o problému. Pokud chyba ovlivňuje všechna čidla na prvním okruhu, vypne se přerušení na první okruh a zapne se druhý okruh. V případě problému druhého okruhu, zařízení cyklí a pouze posílá „keep alive“ zprávy.

4.8 Implementace

Webové rozhraní má několik podčástí. Ve složce `module` jsou zdrojové kódy pro příjem zpráv od jednotlivých služeb. Hlavní soubor je `databaze.php`, který slouží pro připojení do MySQL databáze s rozhraním PDO. Ve zprávě od CRA přijdou všechny příchozí stanice a ukládaní do databáze probíhá tak, že nejdříve se uloží samotná zpráva a se získaným id zprávy se ukládají jednotlivé základní stanice. Zprávy od služby Sigfox chodí tak, jak přijdou do Sigfox cloudu a je potřeba je rozlišovat pomocí logické hodnoty DUPLICATE. První zpráva se uloží do tabulek zpráv a základních stanic. Ostatní se ukládají už jenom do tabulek základních stanic. Soubory s předponou `s_` obsahují rozhraní k zasílání zpráv zpět k zařízení.

Administrátorské rozhraní je ve složce `admin`. Jsou zde implementované funkce pro výpis jednotlivých zpráv z databáze. Délka výpisu je limitovaná klauzulí na 20 položek na stránku a zprávy jsou seřazené sestupně od poslední zprávy po první. Prohlížení dalších stránek zpráv je pomocí metody POST. Každá zpráva má identifikátor, který identifikuje jednotlivé základní stanice, které ji přijali. Základní stanice se zobrazí na stránce `gate.php`, které je metodou GET předán daný identifikátor zprávy (obrázek A.5. Na zobrazené stránce je mapa s body označujícími jednotlivé základní stanice. Tato interaktivní mapa je vytvořená pomocí služby API HERE maps[5], která umožňuje přidávat body podle přiřazených souřadnic (Lat, Lng) na mapový podklad. Nejdříve je nutné vytvořit si API klíč na stránkách HERE maps. Poté se JavaScript funkcí addMarkersToMap jednotlivé body vytvoří a následně se zobrazí na mapovém podkladu.

Pro uspání vestavěného systému byla použita knihovna LowPower.h. Ta umožňuje uspat zařízení pomocí funkce powerDown, které je předána předdefinovaná doba spánku. Tato knihovna umožňuje snížení spotřeby zařízení například vypnutím analogově-digitálního převodníku. Umožňuje probouzení zařízení pomocí přerušení na jednom ze dvou pinů.

Přerušení je umožněno u Arduino Nano pouze na dvou pinech. Nastavení přerušení je udělané funkcí attachInterrupt, které se předá číslo pinu, ukazatel na funkci a událost, při které se má vyvolat přerušení. Stav byl nastaven na přerušení při vzestupné hraně (FALLING), jelikož jazýčkový kontakt je při rozepnutí v logické 1 a při sepnutí klesá do logické 0.

Pro čtení dat z teplotního senzoru DS18B20 jsou použity knihovny DallasTemperature.h[6], která obsahuje nástroje pro dekódovaní dat ze senzorů, a OneWire.h[7], která slouží pro komunikaci se senzory.

Pro sériovou komunikaci mezi zařízením a komunikačním modulem je použita knihovna SoftwareSerial.h. Pomocí funkce Serial() je inicializováno rozhraní nad danými piny. Přenosová rychlost komunikace je nastavena funkcí begin().

4.9 Rozšiřitelnost systému

Nedílnou součástí je i rozšiřitelnost systému. Systém byl navržen tak, aby umožňoval jednoduché rozšíření poskytovatelů služeb IoT pomocí specializace tabulky zařízení. Pro přidání nového poskytovatele stačí vytvořit novou tabulkou generalizace a dva zdrojové kódy do složky `modules`. Jeden z nich bude přijímat příchozí zprávy, dekódovat je a následně ukládat do databáze. Druhý bude fungovat jako rozhraní pro posílání zpráv zpět k zařízení.

[5] https://developer.here.com/products/maps
[6] https://www.arduinolibraries.info/libraries/dallas-temperature
[7] https://www.arduinolibraries.info/libraries/one-wire

Díky tomu, že je kód napsaný v knihovně Wiring, je možné ho přeložit i pro ostatní typy vývojových desek Arduino a desky podporující programování na platformě Arduino IDE. Možnost rozšíření připojených senzorů je řešeno vytvořením polí pro jednotlivé senzory, které umožňují všechny piny obsluhovat.

Kapitola 5

Závěr

Předložená práce se zabývá návrhem zabezpečovacího systému komunikujícího s využitím technologií používaných v rámci sítě pro internet věcí. Konkrétně byly zvoleny sítě Sigfox a LoRaWAN, se kterými bylo nutné se seznámit v rámci návrhu systému. Parametry těchto technologií byly popsány v kapitole 2 (Internet věcí).

V kapitole 3 (Hardware) byl popsán hardware potřebný pro sestavení základního testovacího obvodu navrhovaného zabezpečovacího systému, jsou to senzory pro detekci pohybu, akustický bzučák a anténa pro komunikaci se sítí Sigfox. Jako možná srdce systému byly zvoleny dvě vývojové desky Arduino a Lopy (Pycom). Seznámení se sítí LoRaWAN bylo možné díky desce Lopy, která umožňuje komunikovat jak s touto sítí tak i se sítí Sigfox.

Kapitola 4 (Zabezpečovací modul) se zabývá vlastním návrhem zabezpečovacího systému, popisem a implementace jeho jednotlivých částí. Nejprve byly otestovány jednotlivé technologie a služby sloužící pro komunikaci se sítěmi Sigfox a LoRaWAN. Samotný prototyp zabezpečovacího systém byl postaven na vývojové desce Arduino Nano a komunikačním modulu, který zprostředkovává komunikaci se sítí Sigfox. Byl vytvořen firmware obsluhující jednotlivé senzory a zabezpečující komunikaci s komunikačním modulem. Jednotlivé části softwaru byly navrženy tak, aby byla co největší rozšiřitelnost systému.

Možnosti dalšího rozšiřování navrženého zabezpečovacího systému

- připojení a implementace záznamu obrazu pomocí kamery;
- přidání klávesnice pro aktivaci a deaktivaci systému pomocí pinu;
- přidání třetí větve senzorů – teplotní a vlhkostní čidla, apod.;
- rozvoj uživatelského rozhraní, implementace administrátorského rozhraní;
- připojení baterie a optimalizace s ohledem na spotřebu energie.

Literatura

[1] admin: LoRaWANSpecification. [Online; navštíveno 19.04.2019].
URL http://www.techplayon.com/lora-long-range-network-architecture-protocol-architecture-and-frame-formats/

[2] Alliance, L.: LoRaWAN Specification. [Online; navštíveno 28.04.2019].
URL https://lora-alliance.org/sites/default/files/2018-05/lorawan1_0_2-20161012_1398_1.pdf

[3] Mekki, K.; Bajic, E.; Chaxel, F.; aj.: A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express*, ročník 5, č. 1, 2019: s. 1 – 7, ISSN 2405-9595, doi:https://doi.org/10.1016/j.icte.2017.12.005.
URL http://www.sciencedirect.com/science/article/pii/S2405959517302953

[4] Michalec, L.: PIR detektor: skvělý sluha, ale zlý pán. [Online; navštíveno 13.04.2019].
URL
https://vyvoj.hw.cz/automatizace/pir-cidlo-skvely-sluha-ale-zly-pan.html

[5] Paul: Sigfox downlink in details. [Online; navštíveno 17.04.2019].
URL https:
//www.disk91.com/2017/technology/sigfox/sigfox-downlink-in-details/

[6] REYCOM: INTERNET VĚCÍ - BEZDRÁTOVĚ A S VELKÝM DOSAHEM. [Online; navštíveno 17.04.2019].
URL http://www.raycom.cz/data/article/filemanager/LoRa.pdf

[7] REYCOM: INTERNET VĚCÍ - BEZDRÁTOVĚ A S VELKÝM DOSAHEM. [Online; navštíveno 16.04.2019].
URL https://www.loraserver.io/loraserver/features/device-classes/

[8] rydepier: Active Buzzer Alarm Type YL-44. [Online; navštíveno 10.04.2019].
URL https://rydepier.wordpress.com/2015/05/24/active-buzzer-alarm/

[9] Sigfox: Coverage. [Online; navštíveno 15.04.2019].
URL https://www.sigfox.com/en/coverage

[10] Sigfox: SDR Dongle. [Online; navštíveno 15.04.2019].
URL https://support.sigfox.com/products

[11] Sigfox: Sigfox opens its network with a brand-new Micro Base Station. [Online; navštíveno 16.04.2019].
URL https://www.sigfox.com/en/news/sigfox-opens-its-network-brand-new-micro-base-station

[12] Sigfox: Sigfox service maps. [Online; navštíveno po přihlašení 14.04.2019].
URL https://backend.sigfox.com/welcome/coverage

[13] Sigfox: The full specification. [Online; navštíveno 13.04.2019].
URL https://build.sigfox.com/sigfox-device-radio-specifications#the-full-specification

[14] SimpleCell: Ceník telekomunikačních služeb. [Online; navštíveno 20.04.2019].
URL https://simplecell.eu/wp-content/uploads/2017/02/CEN%c3%8dK_TELEKOMUNIKA%c4%8cN%c3%8dCH_SLU%c5%bdEB_v4.0.docx.pdf

[15] SimpleCell: Co napsala média o umístění Sigfox traumabodů v Brdech . [Online; navštíveno 20.04.2019].
URL https://simplecell.eu/co-napsala-media-o-umisteni-sigfox-traumabodu-v-brdech/

[16] SimpleCell: Faq. [Online; navštíveno 15.04.2019].
URL https://simplecell.eu/faq/

[17] SimpleCell: Sigfox. [Online; navštíveno 10.04.2019].
URL https://simplecell.eu/technologie-sigfox/

[18] Thomas Telkamp, L. S.: Ground breaking world record! LoRaWAN packet received at 702 km (436 miles) distance. [Online; navštíveno 15.04.2019].
URL https://www.loraserver.io/loraserver/features/device-classes/

[19] VENTURES, N.: LoRaWAN - OTA or ABP? [Online; navštíveno 10.04.2019].
URL https://www.newieventures.com.au/blogtext/2018/2/26/lorawan-otaa-or-abp

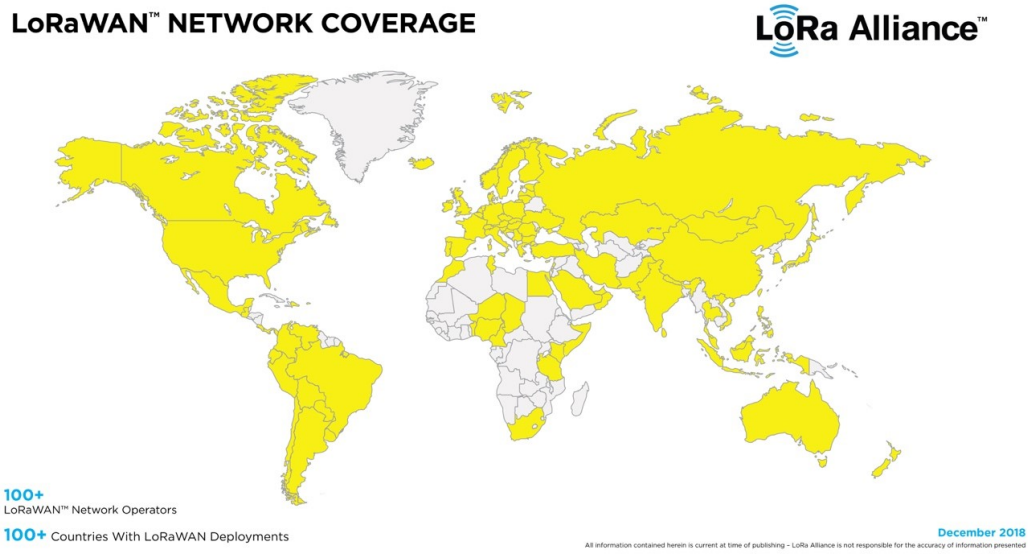
[20] Wikipedia: Jazýčkový kontakt. [Online; navštíveno 15.04.2019].
URL https://cs.wikipedia.org/wiki/Jaz%C3%BD%C4%8Dkov%C3%BD_kontakt

[21] ČTÚ: Všeobecné oprávnění. [Online; navštíveno 18.04.2019].
URL https://www.ctu.cz/sites/default/files/obsah/ctu/vseobecne-opravneni-c.vo-r/10/12.2017-10/obrazky/vo-r10-122017-10.pdf

Příloha A

Obrazové přílohy

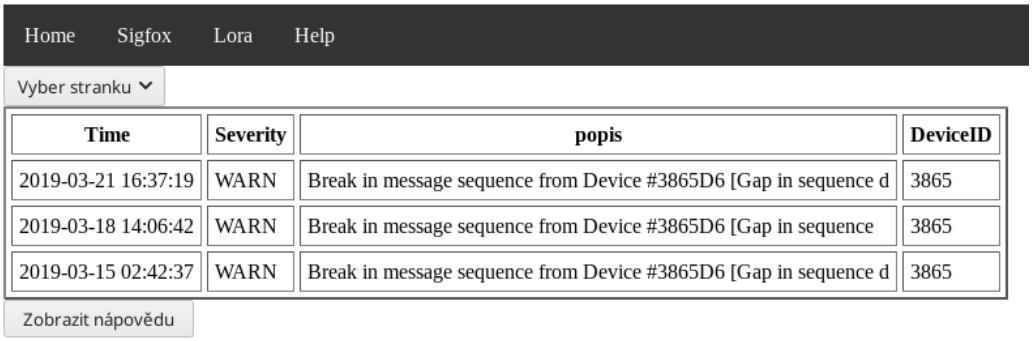
A.1 Mapy pokrytí



Obrázek A.1: Mapa zemí zapojených do LoRa alliance.

Obrázek A.2: Světové pokrytí komunitní sítí The Thing Networks.

A.2 Webové rozhraní služeb



Obrázek A.3: Výpis chybových hlášeních na hlavní stránce.

Home Sigfox Lora Help

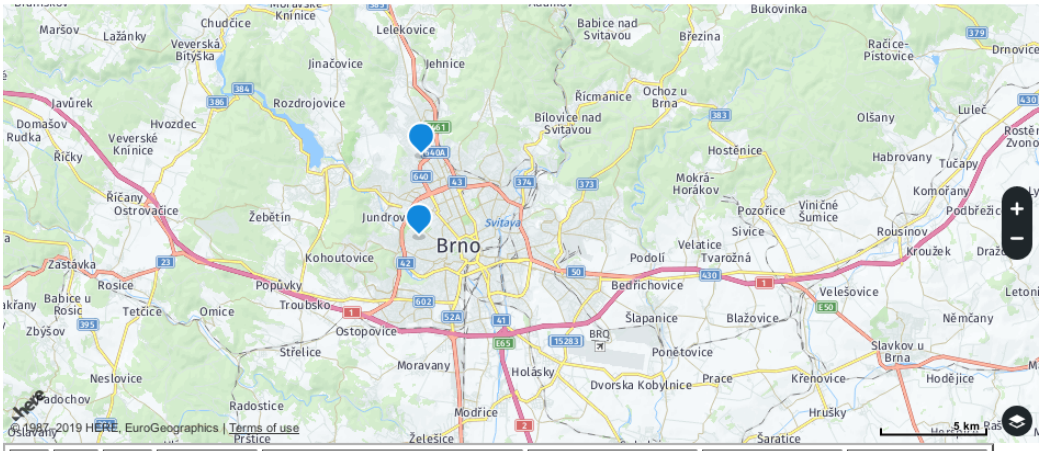
Vyber stranku

ID	cmd	seqno	EUI	time	fcnt	port	freq	toa	dr	ack	gws	bat	data
337	gw	91038757	70B3D5499D3E047C	2019-05-12 20:01:57	0	2	868500000	46	SF7 BW125 4/5	0	2	255	0100
336	gw	91037740	70B3D5499D3E047C	2019-05-12 19:57:18	0	2	867900000	46	SF7 BW125 4/5	0	6	255	0100
335	gw	90134547	70B3D5499D3E047C	2019-05-09 12:21:32	0	2	867500000	46	SF7 BW125 4/5	0	4	255	0100
334	gw	90133180	70B3D5499D3E047C	2019-05-09 12:14:21	0	2	867700000	46	SF7 BW125 4/5	0	4	255	0100
333	gw	90121565	70B3D5499D3E047C	2019-05-09 11:15:15	0	2	867700000	46	SF7 BW125 4/5	0	3	255	0100
332	gw	90021316	70B3D5499D3E047C	2019-05-09 02:24:48	0	2	868100000	46	SF7 BW125 4/5	0	1	255	0100
331	gw	90020211	70B3D5499D3E047C	2019-05-09 02:18:29	1	2	867900000	51	SF7 BW125 4/5	1	5	255	0200
330	gw	90018386	70B3D5499D3E047C	2019-05-09 02:08:28	0	2	867700000	46	SF7 BW125 4/5	0	5	255	0100
329	gw	90017204	70B3D5499D3E047C	2019-05-09 02:02:08	0	2	867500000	51	SF7 BW125 4/5	0	1	255	010203
328	gw	90010302	70B3D5499D3E047C	2019-05-09 01:24:11	0	2	867500000	46	SF7 BW125 4/5	0	2	255	0100
327	gw	90004963	70B3D5499D3E047C	2019-05-09 00:55:41	234	2	867500000	46	SF7 BW125 4/5	0	3	255	eb00
326	gw	90003177	70B3D5499D3E047C	2019-05-09 00:45:38	233	2	867500000	46	SF7 BW125 4/5	0	4	255	ea00

Obrázek A.4: Výpis jednotlivých zpráv.

Home Sigfox Lora Help

Základni stanice, které přijaly zprávu a jejich vlastnosti.

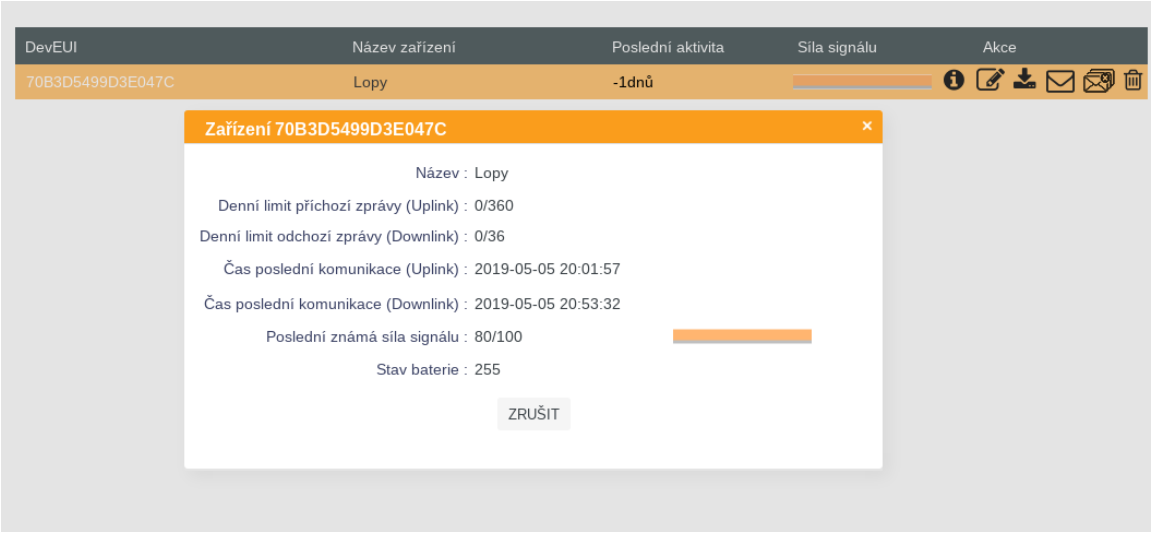


ID	rssi	snr	tss	time	gweui	lat	lon
337	-102	5.80	2147483647	2019-05-12T18:01:57.315492157Z	024B08FFFF0500A9	49.198810100000	16.579589600000
337	-117	-1.00	2147483647	2019-05-12T18:01:57.336184Z	B827EBFFFF42036B	49.232253064162	16.580902329879

rssi	úroveň signálu [dBm] přijatého na GW dle GWEUI
snr	úroveň odstupu signálu o šumu [dB] přijatého na GW dle GWEUI
ts	lokalizovaný čas příchodu uplink zprávy na centrální LNS
time	UTC čas příchodu uplink zprávy na GW
gweui	identifikátor LoRaWAN GW, formát 16 HEX znaků
lat	zeměpisná šířka GW dle GWEUI
lon	zeměpisná délka GW dle GWEUI

Obrázek A.5: Výpis stanic, které přijaly zprávu.

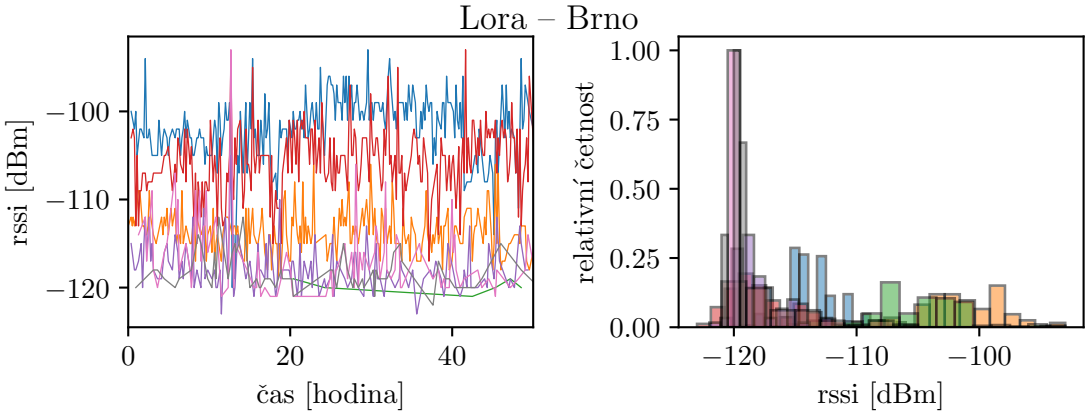
Obrázek A.6: Tabulka přidání nového zařízení do databáze CRA.



Obrázek A.7: Zobrazení podrobností o zařízení v síti CRA.

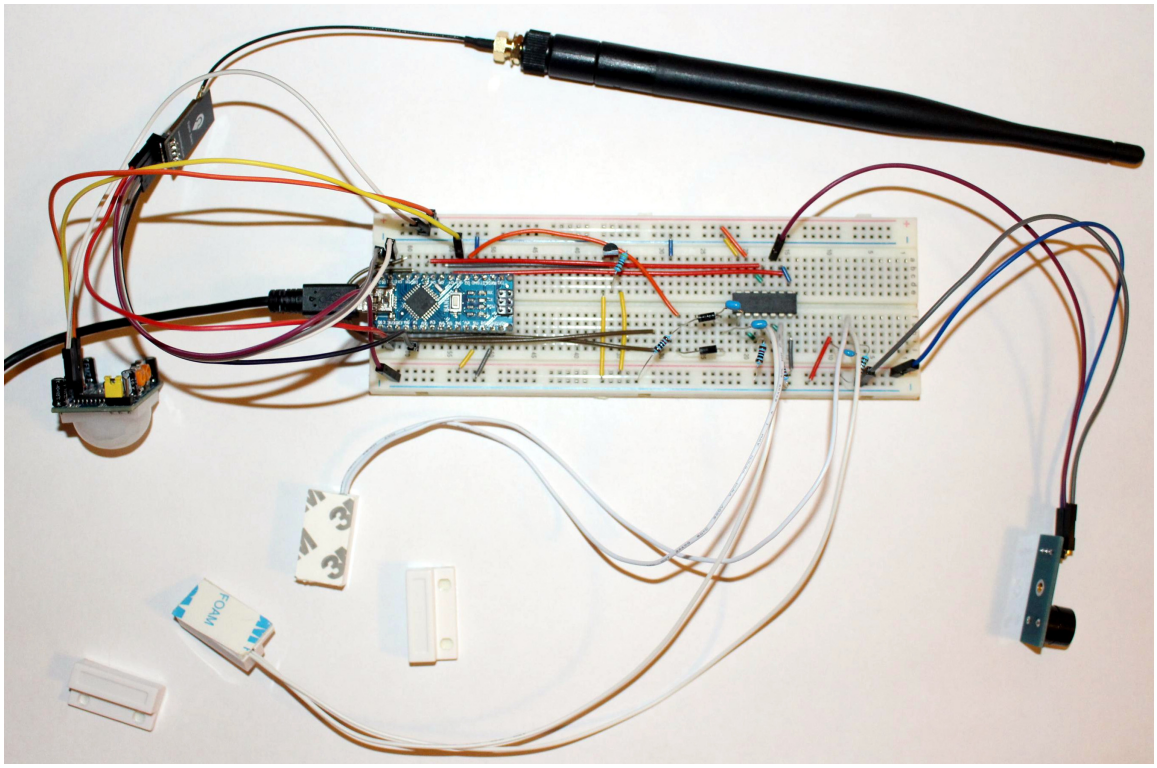
Obrázek A.8: Sigfox výpis callbacků.

A.3 Měření signálu



Obrázek A.9: Pokrytí signálem sítě LoRaWAN (CRA) s rozlišením jednotlivých stanic.

A.4 Prototyp testovacího bezpečnostního systému

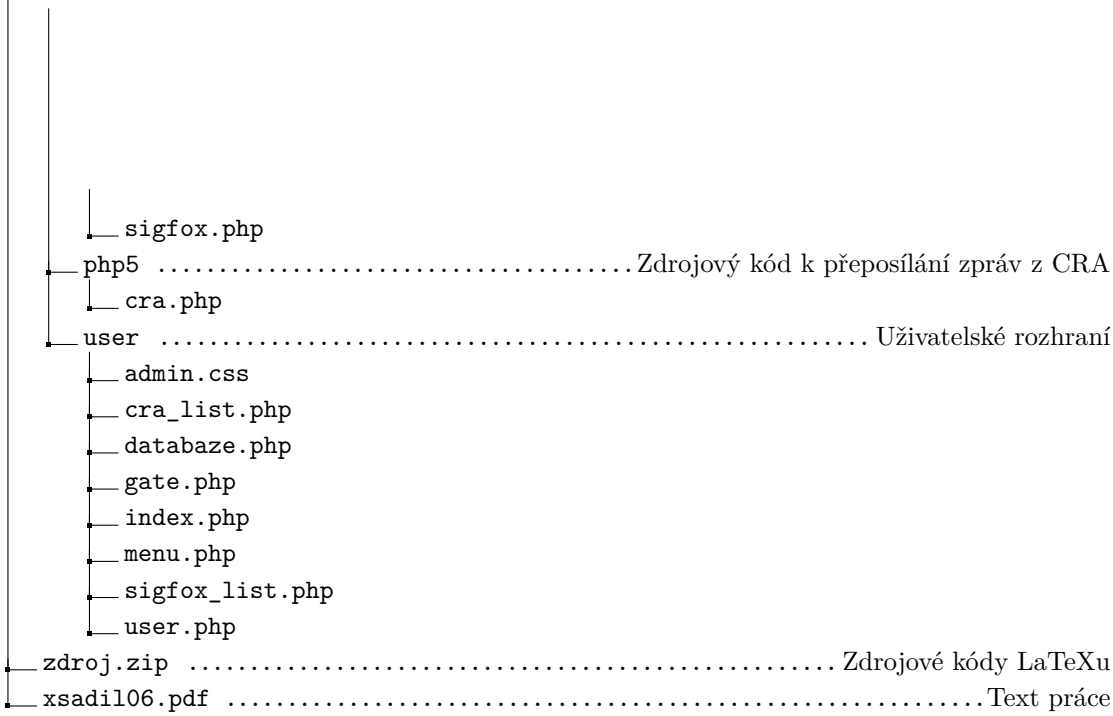


Obrázek A.10: Prototyp navrženého zabezpečovacího systému.

Příloha B

Obsah přiloženého CD

```
.
├── arduino ..... Zabezpečovací modul
│   └── main.ino
├── grafy ..... Zdrojové kódy ke grafům
│   └── pokryti
│       ├── Lora.csv
│       ├── TESTTEMP.csv
│       ├── TESTTEMP2.csv
│       ├── lora_pokryti.pdf
│       ├── lora_pokryti.svg
│       ├── lora_pokryti_stanice.pdf
│       ├── lora_pokryti_stanice.svg
│       ├── notebook.tex
│       ├── pocet_stanic.pdf
│       ├── pocet_stanic.svg
│       ├── pokryti.html
│       ├── pokryti.ipynb
│       ├── pokryti.pdf
│       ├── pokryti_sigfox_lora.pdf
│       ├── sigfox_pokryti_VM.pdf
│       ├── sigfox_pokryti_VM.svg
│       ├── sigfox_pokryti_brno.pdf
│       └── sigfox_pokryti_brno.svg
├── pycom ..... Zdrojové kódy k testování sítí
│   ├── lorawan.py
│   └── sigfox.py
└── web
    ├── databaze ..... Kód pro vytvoření databáze
    │   └── databaze.mysql
    └── modul ..... Zdrojové kódy ke zpracovaní zpráv od poskytovatelů
        ├── cra.php
        ├── databaze.php
        ├── main.php
        ├── s_cra.php
        └── s_sigfox.php
```


sigfox.php
php5 ..... Zdrojový kód k přeposílání zpráv z CRA
cra.php
user ..... Uživatelské rozhraní
admin.css
cra_list.php
databaze.php
gate.php
index.php
menu.php
sigfox_list.php
user.php
zdroj.zip ..... Zdrojové kódy LaTeXu
xsadil06.pdf ..... Text práce