ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta elektrotechnická

Katedra telekomunikační techniky

Inteligentní řízení veřejného osvětlení v koncepci IoT

Květen 2017 Autor: Bc. Josef Krpálek

Vedoucí práce: Ing. Bc. Lukáš Vojtěch, Ph.D.

Čestné prohlášení

Prohlašuji, že jsem zadanou diplomovou práci zpracoval sám s přispěním vedoucího práce a konzultanta a používal jsem pouze literaturu v práci uvedenou. Dále prohlašuji, že nemám námitek proti půjčování nebo zveřejňování mé diplomové práce nebo její části se souhlasem katedry.

Datum: 26. 5. 2017 v Praze

……..……
podpis autora práce

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Krpálek** Jméno: **Josef** Osobní číslo: **392943**

Fakulta/ústav: **Fakulta elektrotechnická**

Zadávající katedra/ústav: **Katedra telekomunikační techniky**

Studijní program: **Komunikace, multimédia a elektronika**

Studijní obor: **Sítě elektronických komunikací**

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Inteligentní řízení veřejného osvětlení v koncepci IoT

Název diplomové práce anglicky:

Intelligent management of public lighting in IoT concept

Pokyny pro vypracování:

Seznamte se současným stavem Low Power WAN technologií pro přenos zpráv v Internetu věcí. S využitím vybrané technologie realizujte inteligentní ovládací systém pro spínání a řízení veřejného osvětlení na základě meteorologických podmínek. Prozkoumejte možnosti umístění těchto periferií do dříku sloupu veřejného osvětlení či tělesa svítidla. Vytvořte DEMO vybraného řešení včetně dokumentace.

Seznam doporučené literatury:

[1] Dokumentace IQRF Alliance - dostupné na http://iqrfalliance.org/ [on-line]
[2] Dokumentace LoRa - dostupná na https://www.lora-alliance.org/ [on-line]
[3] Dokumentace Sigfox - dostupná na https://www.sigfox.com/ [on-line]
[4] Dokumentace IoT Overview Handbook - dostupná na http://www.postscapes.com/internet-of-things-handbook/ [on-line]

Jméno a pracoviště vedoucí(ho) diplomové práce:

Ing. Lukáš Vojtěch Ph.D., katedra telekomunikační techniky FEL

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: **13.10.2016** Termín odevzdání diplomové práce: **09.01.2017**

Platnost zadání diplomové práce: **30.09.2017**

Podpis vedoucí(ho) práce	Podpis vedoucí(ho) ústavu/katedry	Podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Diplomant bere na vědomí, že je povinen vypracovat diplomovou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v diplomové práci.

Datum převzetí zadání	Podpis studenta

Poděkování

V tomto prostoru bych rád poděkoval vedoucímu své Diplomové práce Ing. Bc. Lukáši Vojtěchovi, Ph.D. za pomoc, kterou mi poskytl při řešení práce a za čas, který mi při tom věnoval. Dále bych rád poděkoval svým rodičům nejenom za morální podporu, kterou jsem od nich dostal ale také za poskytnutí kontaktů na odborníky z oblasti.

Anotace

Tato diplomová práce se zabývá možností využití zařízení Internetu věcí jako ovládacího prvku pro systém veřejného osvětlení. Teoretická část práce je hlavně zaměřená na Low Power WAN technologie, které se vyznačují možností komunikace na velké vzdálenost při minimální vlastní spotřebě. V praktické části je popsán způsob realizace jednoduchého ovládání sítě veřejného osvětlení s možností regulování osvětlovacího tělesa pomocí hardwaru založeného na DALI protokolu. Pro tuto práci bylo také provedeno měření funkčnosti tohoto zapojení při umístění komunikačního modulu do dříku sloupu veřejného osvětlení. Poslední částí práce je finanční analýza tohoto řešení.

Klíčová slova: Internet věcí, IoT, IQRF, DALI, veřejné osvětlení, komunikace, síť

Summary

This thesis deals with possibility of using Internet of Things device to control public lightning. Theoretical part is mainly focused on Low Power WAN technologies. Most significant features of these thechnologies are long range comunication and low energy consumption. In practical part is described realization of simple controling device for street lightning with possibility of regulating iluminatning body with hardware based on DALI protocol. For this thesis was done measurement of comuniaction functionality when comunication module was placed inside of public lightning pillar. Last part of this thesis consist of financial analysis of this solution.

Key words: Internet of Things, IoT, IQRF, DALI, Public street lightning, Communication, Network

Obsah

1. Úvod

V poslední době nastal velký pokrok v rozvoji technologií Internetu věcí. S tímto rozvojem přichází na trh velké množství nových výrobků a služeb. Jednou z oblastí, na kterou tyto poznatky lze aplikovat je systém veřejného osvětlení. Principy funkčnosti veřejného osvětlení se v poslední době měnily pouze pozvolna. Nyní ale společně s poklesem cen LED osvětlovacích těles pro veřejné osvětlení přichází celá řada společností se svými inovacemi. Do budoucna se tedy budeme setkávat s celou řadou nových nebo modernizovaných systému veřejného osvětlení, které budou využívat možnosti bezdrátové komunikace se vzdáleným řídícím centrem. Většina těchto sloupů veřejného osvětlení bude v sobě také obsahovat další elektroniku, která může zajišťovat další rozmanité služby pro občany.

Tato diplomová práce se tedy zabývá možností využití specializovaného hardwaru pro úpravu stávajících sloupů veřejného osvětlení, tak aby byly schopny komunikovat jak s řídícím centrem, tak mezi sebou. Pro tento účel je využito komunikačních modulů IQRF a řídících systémů DALI protokolu. S využitím toho hardwaru je vytvořena ukázková aplikace, která po přijetí zprávy přes komunikační modul bude ovládat DALI světelný předřadník. Práce také obsahuje popis několika možných situací, kdy lze existující osvětlovací systém upravit podle konceptů Internetu věcí. Na těchto příkladech je ukázáno nejen co je zapotřebí pro tuto úpravu, ale také jsou v nich popsány další možné služby, které by se dali implementovat do těchto systémů. Tyto ukázky se týkají nejen veřejného osvětlení ale také možnosti využít této úpravy v komerční sféře. Diplomová práce se také zabývá problémy, které by mohly při využití veřejného osvětlení v úpravě pro internet věcí nastat.

2. Internet věcí

Internet věcí (Internet of Things, zkráceně IoT) je nový trend v oblasti kontroly a komunikace předmětů běžného využití mezi sebou nebo s člověkem, a to zejména prostřednictvím technologií bezdrátového přenosu dat a internetu [1]. Implementací IoT existuje široké spektrum od klasické žárovky, která bude měnit svoji svítivost v závislosti na intenzitě okolního osvětlení, až po domácí spotřebiče (např. automatickou pračku, posílající informace o stavu pracího cyklu do aplikace uložené v mobilním telefonu).

Komunikace v IoT probíhá zpravidla na úrovni machine-to-machine nebo s člověkem. Tato komunikace většinou probíhá bezdrátově. Pro komunikaci se využívá vícero technologií, díky kterým může zařízení poskytnout služeb IoT. V praxi jsou vedle mnoha dalších nejčastěji využívány technologie RFID, Bluetooth (low energy varianta), Zigbee a low power WAN. Výběr komunikačních technologií se řídí podle způsobu využití, ekonomické stránky, prostředí, v kterém bude technologie využívána, a jiných preferencí.

Existují dva základní způsoby, jakým jsou realizována zařízení využívající Internetu věcí. Prvním případem jsou stávající zařízení, která původně nebyla zamýšlena pro Internet věcí. V tomto případě musí proběhnout modifikace, která spočívá v připojení nových periferií nebo hardwaru, který bude zajišťovat přenos informací a vykonávání požadovaných úkonů. Druhou možností, se kterou se budeme v budoucnu stále více setkávat, jsou zařízení již z výroby uzpůsobená pro využívání technologií IoT. Tyto přístroje budou obsahovat vlastní komunikační a řídící jednotku. Řídící jednotka se bude starat o ovládání periferií, mezi které například mohou patřit senzory, aktuátory, výkonné prvky apod.

Každé zařízení využívající služeb internetu musí mít svou unikátní adresu. Z tohoto důvodu se využívá protokolu IPv6. Nástup tohoto protokolu je jedním z důvodu pro opětovný nárůst popularity IoT. Velikost adresního prostoru IPv6 je 128 b adresa, což odpovídá $2^{128} \approx 3x10^{38}$ adres, kde protokol IPv4 má pouze 4 miliardy ($4x10^{10}$) adres, které v současné době jsou téměř vyčerpány. Díky velikosti adresního prostoru protokolu IPv6 nebudou problémy se současnými odhady, které uvádějí, že v roce 2020 bude připojeno k Internetu věcí přes 20 miliard zařízení (zatímco v roce 2016 je připojeno kolem 6 miliard zařízení) [2].

V současné době existuje mnoho uskupení, které se věnují problematice standardizace v IoT. Mezi společnosti, které se sdružují do skupin usilujících o standardizaci prostředí Internetu věcí, patří jak malé firmy zabývající se technologiemi z tohoto prostředí, tak nadnárodní technologičtí giganti (např.: Samsung, Microsoft, Cisco, apod.) pro které tato oblast znamená možnost dalšího rozvoje. Někteří z těchto gigantů jsou součástí většího počtu těchto uskupení. Největším důsledkem tohoto rozprostření prostředků je že, stále neexistují žádné jednotné standarty ať už pro oblast komunikace, bezpečnosti nebo Internetu věcí jako celku. Většina existujíc uskupení se

zatím zabývá svými standarty (společnosti se snaží získat pro sebe část trhu, dokud ještě není plně rozvinutý), a tím vzniká silné konkurenční prostředí. Až budoucnost zodpoví, jestli finální standarty vzejdou od vítěze závodu inovací nebo jestli vznikne nezávislé těleso, které bude mít dostatečnou podporu od velkých hráčů na trhu, aby prosadilo své standarty.

Zatím je ale nejvyšší stupeň standardizace a kompatibility k nalezení u produktů pro inteligentní domácnost. Existují centrální prvky (hub), které jsou schopny komunikovat nejen se zařízeními od stejného výrobce (jednu z největších nabídek zařízení pro inteligentní domácnosti nabízí Samsung) ale také se zařízeními od vybraných partnerů. Ve většině případů se jedná o zařízení od stejných výrobců, mezi které například patří Google a Amazon, kde tito giganti spolupracují i s menšími výrobci centrálních prvků. V současné době mezi nejlepší centrální prvky patří Samsung SmartThings a Wink Hub [3].

2.1 Stručná historie Internetu věcí

Prvním zařízením, které komunikovalo s okolím prostřednictvím internetu, byl nápojový automat na colu, nacházející se na půdě Carneie Mellon Univerzity v Pittsburghu [4]. Již v roce 1982 toto zařízení bylo schopno oznamovat stav svých zásob, přes počítačovou síť. Až v roce 1991 byly principy Internetu věcí oprášeny, v souvislosti s publikovaným vědeckým článkem, který se zabýval budoucností počítačových sítí v 21. století. V letech 1993-1996 řada nadnárodních společností uvedla své koncepty inteligentních sítí jako např.: at Work od Microsoftu nebo Nest od Novellu. Samotný termín Internet of Things byl ale představen až v roce 1999 ve zprávě o technologii RFID. Od tohoto roku také nabývá koncept Internetu věcí na aktuálnosti. V následnicích letech jsou články na toto téma uvedeny v publikacích pro širokou veřejnost jako např.: The Guardian nebo Boston Globe. V roce 2005 uveřejnilo ITU první report na téma IoT. Poté v roce 2008 proběhla první Evropská konference na téma Internetu věcí a jeho perspektivním využití v praktických aplikacích. Od této doby opět nabývá celý koncept na popularitě. Posledním velkým milníkem pro internet věcí bylo uvedení protokolu IPv6 do reálného provozu. Od této doby také nastává dynamický rozvoj technologií Internetu věcí, které bude mít do budoucna široké uplatnění nejen pro širokou veřejnost ale i pro průmysl.

2.2 Low-power WAN technologie

IQRF, SigFox a LoRa patří mezi tvz.: Low-power WAN (LPWAN) technologie, které se používají pro realizaci zařízení Internetu věcí. Pro tento druh technologií je charakteristická malá spotřeba elektrické energie (jednotlivé technologie se značně liší,

proto bude u každé spotřeba zmíněna samostatně). IQRF, SigFox a LoRa patří mezi tvz.: Low-power WAN (LPWAN) technologie, které se používají pro realizaci zařízení Internetu věcí. Pro tento druh technologií je charakteristická malá spotřeba elektrické energie (jednotlivé technologie se značně liší, proto bude u každé spotřeba zmíněna samostatně). Většina implementací těchto technologií využívá jako zdroj energie baterii, z tohoto důvodu je nutné se snažit docílit co nejnižší spotřeby elektrické energie. Jedním ze způsobů, jak tohoto docílit je přes implementaci režimu standby (režim spánku). Tento režim lze použít díky tomu, že není nezbytně nutné, aby koncová zařízení mezi sebou neustále komunikovala nebo byla jinak aktivní. Dalším způsobem, jak lze snížit spotřebu elektrické energie je omezit datové toky mezi zařízeními. Většina technologií (nejen LPWAN) pro Internet věcí je tedy koncipována pro práci s malými přenosovými rychlostmi dat, které jsou v řádu jednotek až desítek kb/s.

Všechny LPWAN technologie pracují v ISM pásmu, což jsou frekvenční pásma pro volné využití v průmyslové, vědecké a lékařské, oblasti ale i pro osobní využití. Frekvence pásem schválených v České republice se pohybují v rozmezí 433-434 MHz a 863-870 MHz (ve světě se ještě využívá pásmo 902-928 MHz). Z hlediska využití ISM pásma existují omezení, která jsou specifikována v dokumentu Všeobecného oprávnění č. VO-R/10/05.2014-3 [5]. Hlavní podmínkou je omezení maximálního efektivního vyzařovaného výkonu na 10 mW pro pásmo 433-434 MHz a 25 mW pro 863-870 MHz.

2.3 IQRF

IQRF je první z low-power WAN technologií, které budou představeny. Tato technologie je vyvíjena českou společností Microrisc, sídlící v Jičíně [6] (založenou v roce 2004). Jedná se o kompletní řešení pro Internet věcí zahrnující jak hardware a software tak i protokoly pro přenos zpráv a podpůrné služby.

IQRF pracuje s přenosovou rychlostí 20kb/s. Energetická náročnost při přijímání dat závisí na zvoleném modu:

- 12,3 mA ve standrartním módu (STD mode)
- 233 μA v low-power módu (LP mode)
- 15 μA v extra low-power módu (XLP mode)

V režimu odesílání dat se spotřeba pohybuje v rozmezí 8-19 mA a v režimu spánku nepřesahuje spotřeba hranici 1 μA. Maximální vysílaný výkon modulů je závislý na typu modulu a vysílací frekvenci, maximální výkon je 12,5 mW ve frekvenčním pásmu 863-870 MHz a v pásmu 433-434 MHz není překročena úroveň 10 mW (ani v jednom případě nejsou překročeny hranice určené všeobecným oprávněním č. VO-R/10/05.2014-3). Hodnota vysílaného výkonu je softwarově nastavitelná v násobcích základní úrovně.

Technologie IQRF je založena na principu komunikačních modulů s proprietárním operačním systémem, který v současné době je ve verzi 3.08D. Tyto moduly se programují v programovacím jazyce C a s využitím definovaných příkazů v GUI. Dosah jednoho komunikačního modulu je v řádu stovek metrů v otevřeném prostoru a desítek metrů v zástavbě. Většího dosahu můžeme dosáhnout dvěma způsoby. Prvním je připojení antény k modulu. Výrobce dodává velké množství antén, které se liší typem, frekvencí, pro kterou jsou určeny, rozměry, způsobem připojení a cenou [7]. Druhý způsob je založen na použité topologii sítě, kdy se nezvyšuje dosah jednotlivých modulů, ale zvyšuje se efektivní plocha sítě. V takovémto případě může mezi dvěma koncovými zařízeními být až několik kilometrů. IQRF podporuje dvě základní topologie – peer-to-peer (p2p) a MESH, pro jejíž implementaci existuje proprietární protokol IQMESH. Defaultně jsou moduly v peer-to-peer módu, kdy síť neobsahuje žádný koordinační prvek a vysílané packety jsou přijímány všemi ostatními moduly. V tomto nastavení může síť obsahovat neomezené množství zařízení, a vše je řízeno aplikačním programem uživatele. Na rozdíl od topologie p2p v MESH topologii je použit koordinátor. Tímto jsme ale omezeni počtem zařízení v síti, kde maximum je 240 zařízení (až 239 zařízení a koordinátor). Mezi zařízení, které můžeme nalézt v síti, patří komunikační moduly, dedikované routery nebo specifická koncová zařízení. Komunikační modul v sítí může plnit funkci koncového bodu nebo routeru. Pokud by byl počet zařízení v síti nedostačující, můžeme využít možnost tzv. škálování sítě. V tomto případě nastavíme cílové moduly jako koordinátory pro sub-sítě. Sub-síť může také maximálně obsahovat 239 zařízení. Doporučuje se však vytvářet méně komplikované sítě z důvodu jejich jednoduší správy a pro ušetření systémových prostředků. Pod textem je vidět struktura IQRF packetu pro topologii p2p. Ze struktury je především vidět maximální velikost přenesených dat a zaměření se na přenos packetu bez chyb (dílčí CRC a celkové CRC).

PAH			NTWINFO		DATA		CRC
PIN	DLEN	CRCH	NTW INFO	CRCN	DATA	CRCD	CRCS

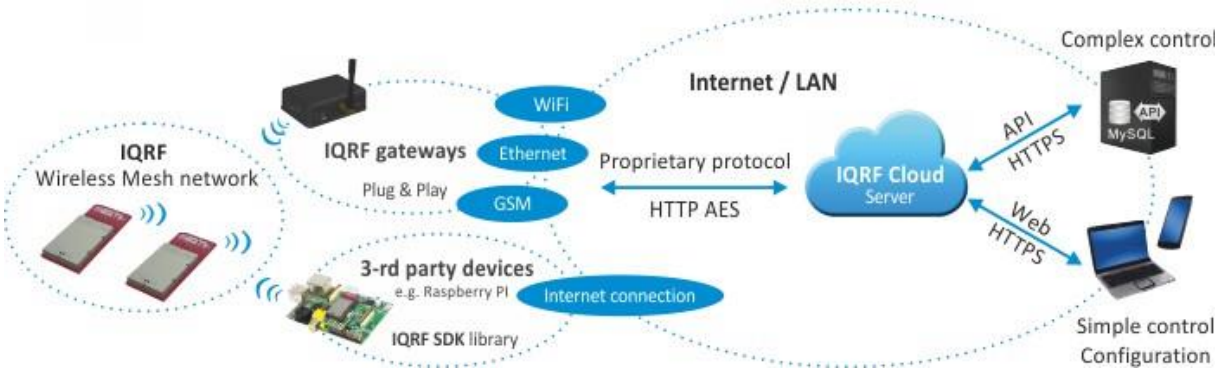
PIN	packet info
DLEN	data lenght
CRCH	header checksum
NTW INFO	networking info
CRCN	NTW INFO checksum
DATA	max 255B of users data (v IQRF OS 2.0 omezeno na 64B)
CRCD	data checksum
CRCS	Security checksum

Jak již bylo uvedeno moduly IQRF se programují s využitím programovacího jazyka C a s využitím definovaných příkazů v GUI, ve vývojovém prostředí IQRF IDE (Integrated Development Enviroment). IQRF IDE slouží nejen k programování modulů,

ale využívá se také jako testovací a servisní nástroj pro správu sítí IQMESH. Připojení modulů k počítači probíhá pomocí hardwarového programátoru (pokud je IQRF IDE spuštěné a připojíme programátor s vloženým komunikačním modulem k počítači, proběhne jeho automatická inicializace v IQRF IDE), který je součástí vývojářského kitu. Mezi podporovaná zařízení programu IQRF IDE ještě patří brány pro přístup do internetu (Gateway), které mají port rozhraní USB.

V otázce zabezpečení komunikace se využívá principů vrstveného šifrování dat. V procesu párování zařízení se vyžívá 128 b Bonding (párovacího) klíče, který je šifrován 128 b AES šifrou. Společně s kontrolou konzistence packetu se tímto dá zabránit útokům, které využívají slabin při inicializaci sítě. Samotná komunikace v síti je poté zabezpečena za použití 192 b síťového hesla, ze kterého se vytvoří Network (síťový) klíč (klíče jsou dynamicky měněny), který poté opět šifrován využitím 128 b AES algoritmu. Mezi další bezpečnostní opatření při přenosu patří kontrola celistvosti a pravosti packetů. Pracuje se také s kontrolou uživatelů, kdy uživatel má svůj autorizační 128 Users klíč, který je opět šifrován s využitím 128 b AES algoritmu. Do budoucna se plánuje s bezpečnostními updaty systému, v závislosti na nových trendech v bezpečnosti IoT síti. Z důvodu využívání algoritmu AES ve 128 b podobě, se také sleduje úroveň zabezpečení, která je tímto algoritmem poskytována. Pokud by byl tento algoritmus kompromitován, existují plány pro přechod na robustnější standardy [8].

Jednou z dalších výhod IQRF je možnost propojit uživatelskou síť s cloudovým řešením poskytovaným společností Microrisc. Díky této možnosti jsou data z uživatelské sítě přístupná kdekoliv ze světa pouze s malým úsilím vynaloženým na zprovoznění tohoto řešení. IQRF cloud se se stará o hlavně o sběr dat ze sítě, ale je z něj také možné posílat příkazy k řízení koncových zařízení. Jediným potřebným hardwarem pro realizaci tohoto řešení je brána pro přístup do internetu (Gateway). Další nezbytností je existující účet na stránkách cloudu [9]. Existuje zde také možnost, aby jeden účet spravoval vícero bran, ale také aby jedna brána byla přístupná z více účtů. Pro IQRF existuje množství bran, nejběžnějšími jsou takové, které mají realizovaný přistup do internetu pomocí technologií jako je Ethernet, Wi-fi nebo GSM. Méně časté jsou brány, které se připojí do USB rozhraní, které pro přístup do internetu využívají zařízení, ke kterému jsou připojeny. Instalace brány probíhá principem plug-and-play, kdy se celé nastavení brány provede přes IQRF IDE.



Obr. 1 IQRF cloud, převzato z [10]

Komunikace mezi serverem a bránou probíhá v režimu client/server. Tato komunikace je zabezpečená za využití protokolů šifrovaných algoritmem AES 128, a samotný přístup do cloudu je zabezpečený využitím protokolu https. Z cloudu si poté může uživatel číst datové logy, které obsahují časové údaje (timestamp) o době vzniku jednotlivých záznamů. K datům je možné přistoupit pomocí webového prostředí, které je vytvořeno přes JavaScrip nebo PHP. Existuje také možnost data zanášet do databázových systémů. Na všechny tyto situace je cloudová aplikace přizpůsobena. Samotné hostování služeb může být realizováno na IQRF cloudu, o kterém se zmiňuje předchozí text, nebo je zde možnost pro uživatele shromažďovat data na vlastní servery. Pro tento způsob realizace služeb, je nutné mít zakoupenou licenci, kde balíček služeb obsahuje nejen instalační soubory, ale také zdrojové kódy, díky kterým je možné udělat další úpravy systému.

Cloud pracuje se stejnými datovými strukturami, které se používají v lokálních IQRF sítích, což znamená, že v obou směrech komunikace probíhá se zprávami s maximální délkou užitečných dat 64 B. IQRF brána je pak schopna poslat do cloudu až 500 záznamů z jednotlivých koncových zařízení naráz. Doba mezi každým odesláním nashromážděných dat z brány na cloud je uživatelsky definovatelná. Zprávy se před odesláním drží ve vnitřním bufferu, a pokud by buffer přetekl, mažou se záznamy od nejstaršího. Poté v cloudu je možné držet maximálně 1000 přijatých záznamů, které se také po překročení limitu mažou od nejstarších. Protože cloud je schopen nashromáždit pouze vcelku omezené množství přijatých zpráv, existuje možnost tyto zprávy ukládat na externí uložiště. Maximální kapacita logu s odeslanými příkazy zpátky do sítě je 500 000. Tyto limity ale platí pouze pro IQRF cloud. V případě, kdy je aplikace zřízena na serverech uživatele, s využitím licence, je maximální počet záznamů limitován pouze velikostí úložného prostoru, vyhrazeného na logy.

2.4 LoRa

LoRa je druhou z představených LPWAN technologií. Na rozdíl od předchozí LPWAN technologie, je technologie LoRa otevřeným standardem, který je vyvíjen neziskovou organizací LoRa Alliance. Členové organizace sdílí své informace a společně vyvíjejí hardware a software, který poté je použitelný pro jejich vlastní implementace. Hardwarem se v tomto případě míní čipy pro přenosové moduly.

Protože existuje celá řada implementací technologie LoRa do hardwaru, je spotřeba modulů různá. Pro názornost je uveden příklad modulu od společnosti Four Faith s označením F8L10D-N LoRa Module [11]. Z datasheetu tohoto výrobku lze vyčíst spotřebu v různých módech:

- Přijímání <22 mA
- Vysílání 127-129 mA
- Režim spánku s nastaveným buzením <3 μA

- Režim spánku <2 μA

Jedním z dalších rozdílů oproti technologii IQRF je přenosová rychlost. LoRa využívá změn rychlostí přenosu, pro docílení optimalizace spotřeby a zlepšení škálovatelnosti sítě. Rychlost přenosu se pohybuje v rozmezí 0,3-22 kb/s. V Evropě ještě může LoRa využívat rychlosti 100 kb/s při GFSK (Gaussian frequency-shift keying) modulaci. Rychlosti přenosu se také liší podle implementace. Výše uvedený modul využívá 6 možných rychlostí 0,3; 1,2; 2,4; 4,8; 9,6; a 19,2 kb/s. Z tohoto důvodu se využívá algoritmu ADR (Adaptive datarate algorytm), který dynamicky mění rychlost přenosu, tak aby vysílané packety byly předány beze ztráty informace. Většina modulů je schopna vysílat s vyšším výkonem, než jsou stanoveny hranice pro vysílání podle všeobecného oprávnění č. VO-R/10/05.2014-3. Z tohoto důvodu je zapotřebí softwarově omezit maximální vyzářený výkon.

LoRa využívá vlastní modulace pro přenos dat. LoRa modulace podporuje široké množství topologií, kde doporučenou je hvězda. Centrálním síťovým prvkem v síti LoRa s topologií hvězdy je gateway, která je připojena do internetu přes většinu klasických technologií jako je ethernet, GSM apod. Moduly od některých výrobců jsou vytvářeny pro primární použití v topologii MESH, kde můžeme dosáhnout větších vzdáleností (podobnými způsoby jako u IQRF), nevýhodou je vyšší spotřeba, z důvodu vyšší režie sítě. Gateway pro technologii Lora jsou více kanálové (kanály mají většinou šířku 125 nebo 250 kHz) a podporují příjem zpráv od více modulů naráz. Moduly v topologii hvězda jsou napojeny na gateway přímo bez mezičlenů. Vzdálenosti, na které můžeme moduly připojit, jsou závislé na způsobu implementace a prostředí. V zástavbě je dosah modulů v řádu stovek metrů až jednotek kilometrů a jednotek kilometrů (v extrémních případech až do 20 kilometrů) ve volném prostoru. Maximální počet modulů, které mohou být připojeny k jedné gateway závisí na počtu packetů, které jednotlivé moduly odešlou v průběhu jedné hodiny. Gateway má omezené množství packetů, které je schopná zpracovat za jednu hodinu (limitace přenosové modulace). V praxi může Gateweay zpracovat na osmi kanálech okolo 1,5 milionů packetů za den. Z této hodnoty lze stanovit, že k jednomu zařízení může být připojeno až 62,5 tisíc modulů, pokud by každý modul odeslal 1 zprávu za hodinu [12]. Jeden packet může přenášet maximálně 256 b dat.

LoRa čipy a moduly se programují různými způsoby v závislosti na výrobci. Někteří výrobci preferují proprietární způsoby programovaní s vlastními programovacími prostředími. Jednou z dalších možností, která je v praxi využívána je programování přes jiné platformy jako je například Arduino nebo Raspberry pi.

Technologie LoRa specifikuje 3 varianty koncových bodů, které se převážně liší ve způsobu komunikace s gateway:

- Bidirectional end device – po vyslání zprávy následují 2 krátké sloty pro příjem zpráv. End device vysílá, pouze když potřebuje. Energeticky nejúspornější režim.

- Bidirectional end device with sheluded recieve slots – Oproti předchozí variantě otevírá vysílací kanál pro příjem v předem stanovené časy. Potřebná synchronizace s gateway.
- Bidirectional end device with max recieve slots – Kanál pro příjem zpráv je otevřen pouze v okamžiku vysílání.

Zabezpečení v sítích LoRa probíhá nadvakrát, nejprve při inicializaci zařízení v síti a poté v průběhu komunikace. Zabezpečení je řešeno s pomocí unikátních klíčů a encrypce. Koncový bod si při inicializaci požádá o spárování za použití zprávy obsahující 128 b AppKey (aplikační klíč). V dalších zprávách poté zahrnuje další unikátní identifikátory AppEUI a DevEUI společně s 2 B náhodně generovanou hodnotou DevNonce. Za pomocí těchto hodnot serverová strana komunikace provede autentifikaci koncového bodu. Při komunikaci se poté využívá šifrovacího algoritmu 128 b AES v Counter módu. Zprávy poté vyžívají dvou různých klíčů (klíč je vybrán v závislosti na hodnotě bitu FPort) – NwkSkey a AppSKey. Využívá se ještě dalších identifikátorů, jako jsou countery pro algoritmus AES (FCntUp a FCntDown), které jsou spravovány na obou stranách komunikace (countery by se neměly nikdy opakovat).

2.5 SigFox

Technologie SigFox je vyvíjena Francouzskou společností stejného jména od roku 2009. Společnost Sigfox se zaměřuje jak na vývoj hardwaru, tak softwaru, kde pro obchodní partnery je otevřena část trhu s koncovými zařízeními. Infrastruktura pro sítě této technologie se značně liší od konkurence (IQRF, LoRa…). Kompletní infrastruktura sítě SigFox je vlastněna Sigfoxem, kde jednotlivé koncové body se do ní pouze připojí. Společnost Sigfox se v tomto ohledu chce stát „celosvětovým operátorem“ pro sítě Internetu věcí.

Stejně jako u technologie LoRa, spotřeba energie bude opět demonstrována na příkladu koncového bodu. V tomto případe na zařízení Atmel ATA8520D [13]:

- 10,4 mA při přijmu
- 32,7 mA při vysílání
- 50 µA v idle režimu
- 5 nA pokud je zařízení vypnuto

Přechod mezi vypnutím a idle režimem je v průměru 10ms. Přenosové rychlosti u koncových modulů SigFox jsou 100 b/s při modlaci DBPSK (Differential binary phase-shift keying) nebo až 600 b/s s využitím modulací GFSK. Maximální vysílací výkon modulů se pohybuje okolo 25 mW ve frekvenčním pásmu 863-870 MHz, což stejná hodnota jako povolené maximum v České republice. Na rozdíl od technologií IQRF a LoRa, SigFox nevyužívá frekvenčního pásma 433-434 MHz.

Jak již bylo zmíněno, infrastruktura sítí využívající technologie SigFox, je vlastněna stejnojmennou společností. Díky této filozofii, je pro připojení zařízení do sítě zapotřebí pouze být v oblasti, která je sítí pokryta [14] a vlastnit komunikační modul SigFox. Topologie použitá v síti je peer-to-peer, kdy výrobcem udávané vzdálenosti na, které zařízení mohou komunikovat, jsou 3-10 km v zástavbě a 30-50 km ve volném prostoru. Koncové zařízení mohou, poslal až 140 zpráv/den (zpráva každých 11 minut) a s maximální velikostí dat ve zprávě 12 B. Celá síť se svým principem více podobá mobilním sítím než konkurenčním řešením sítí LPWAN technologií.

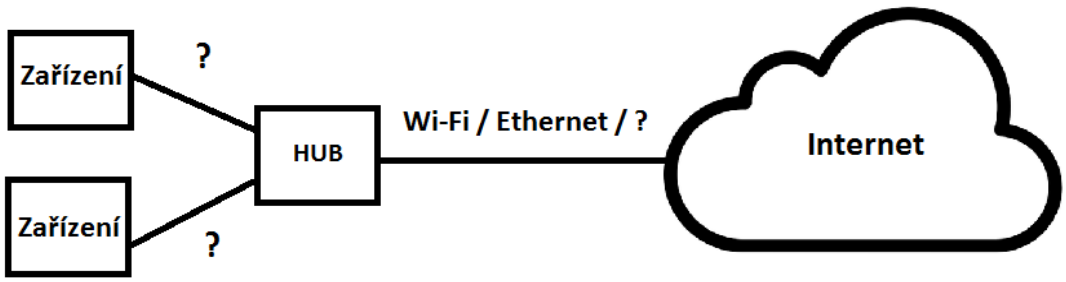
Stejně jako u technologie LoRa, způsob programování komunikačních modulů pro koncová zařízení se liší podle výrobce. V kontrastu k tomu infrastruktura je plně v péči společnosti Sigfox a není dostupná zvenčí.

Způsob zabezpečení sítě technologie SigFox se odvíjí ze způsobu realizace sítě. Hlavním bodem je způsob zabezpečení dat. Formát přenášených je zcela závislý na požadavcích zákazníka, z tohoto důvodu neexistuje jednotný způsob čtení dat v síti. Uživatel si také může použít jakékoliv další způsoby zabezpečení, které je schopen realizovat ve svém datovém prostoru zprávy (12 B). Samotná infrastruktura využívá další bezpečnostní mechanizmy jako je ochrana proti replay útokům, message scrambling a sequencing. Další výhodou technologie SigFox je způsob chodu koncových zařízení, většinu času tyto zařízení nevysílají a jsou v režimu spánku, takže je obtížné na ně útočit.

3 Bezpečnost v prostředí Internetu věcí

S masovým rozšířením Internetu věcí nastává otázka ohledně bezpečnosti v této oblasti. Jak již bylo zmíněno v kapitole 2 jedním z největších problému v této oblasti je, že nejsou stanoveny standardy pro Internet věcí a tato skutečnost platí i u problematiky bezpečnosti. Aplikace Internetu věcí zahrnují jak využití v průmyslové sféře, veřejné infrastruktuře tak pro osobní použití. V každé z těchto oblastí by mělo být hlavní prioritou zamezení neoprávněného přístupu a manipulace se zařízeními v síti. Zneužití jednotlivých zařízení může vést k finančním ztrátám, ale je zde také možnost, že cíleně pozměněný chod přístrojů může mít fatální následky na zdraví uživatele. Bezpečnost Internetu věcí by měla splňovat kritéria kybernetické bezpečnosti.

V různých oblastech využití zařízení Internetu věcí jsou potřebné různé stupně zabezpečení dat, proti jejich odposlouchávání a manipulaci s nimi. V oblasti osobního využití zařízení Internetu věcí se z větší části jedná o „chytrou“ domácnost, kde jednotlivé domácí spotřebiče jsou připojeny k internetu a komunikují s uživatelem přes aplikaci ve smartphonu nebo přes centrální prvek pro inteligentní domácnost. Samostatná zařízení využívají pro přístup k internetu nejčastěji technologie wi-fi. U systémů s centrálním prvkem existují různá řešení komunikace zařízení-hub a hub-internet, kde tyto řešení se budou lišit podle výrobce spotřebiče. Propojení zařízení-hub je téměř vždy bezdrátové a většinou bude využívat některou z rozšířených technologií pro bezdrátový přenos na krátké nebo střední vzdálenosti jako např.: wi-fi, zigbee, bluetooth apod. Možností pro připojení hubu k internetu je méně, dva hlavní způsoby jsou přes wi-fi nebo ethernetem k routeru domácí sítě. Centrální prvek v domácích sítích je jedním (měl by být) z důležitých prvků zabezpečení zařízení IoT. Toto zařízení v sobě může implementovat další bezpečnostní mechanizmy, které chybí nebo by bylo nákladné implementovat do samostatných koncových zařízení, jako je například šifrování dat, firewall apod. Další výhodou těchto řešení je možnost využití jiných technologií pro přenos dat, jak již bylo zmíněno výše. Sítě wi-fi jsou na trhu delší dobu a existuje tedy větší množství materiálů popisující slabé stánky této technologie.



Obr. 2 Vizualizace přístupu zařízení do internetu v síti s centrálním prvkem

Mezi nejpravděpodobnější důvody útoků na chytré domácnosti budou pokusy o získání informací o stavu a zvycích jejich členů. Takto získané informace mohou být

zneužity za pomocí social engineeringu. Manipulace se zařízeními v tomto prostředí mohou zahrnovat cílené ovlivňování funkce domácích spotřebičů (od změny teploty ovlivněním termostatu až závažnější útoky vedené na chytré bezpečnostní zařízení). Dohromady tyto útoky mohou například vést k páchání Tresné činnosti (nejčastěji loupeže).

U využití principů a technologií Internetu věcí v infrastruktuře měst, se většinou operuje na větších vzdálenostech a jedná se o mnohem rozmanitější skupinu aplikací než se kterými se můžeme setkat v domácnostech. Každá síť v této kategorii má na starosti jiné zařízení, z tohoto důvodu se u každé bude lišit cíl útoků. U některých aplikací není důležité, jestli bude útočník schopen číst přenášená data, pokud by ovšem nebyl schopen použít přečtené zprávy pro vytvoření falešných. Příkladem takovéto sítě může být síť pro ovládání veřejného osvětlení (téma této práce). Útočník sice může číst přenášená data od jednotlivých pouličních osvětlení, ale většinu těchto informaci je schopen získat i jiným způsobem. Jediná citlivá data, která jsou ve většině případů přenášena ve zprávě takovéto aplikace, jsou informace o interním označení lamp (jednotlivé řešení tohoto problému se mohou lišit a mohou obsahovat další klíčové informace o infrastruktuře systému). Na druhou stranu v této aplikaci, stejně jako u všech ostatních, je nezbytně nutné, aby útočník nebyl schopen se dostat k ovládání napadaného zařízení. Dalším hypotetickým příkladem podobné infrastrukturní aplikace mohou být boxy pro vyzvednutí balíčků nacházející se na veřejných místech. Pro takovouto aplikaci je důležité, aby útočník ani nebyl schopen zjistit stav jednotlivých boxů.

V průmyslové sféře je situace ochrany dat a správné funkčnosti sítě nekompromisní. Jakékoliv zásahy do systému mohou znamenat finanční ztráty v závislosti na velikosti postihnutého pracoviště. Útoky, které v této oblasti budou nejčastější a nejdestruktivnější (pokud budou úspěšné), jsou odposlouchávání / odcizení dat (průmyslová špionáž) a sabotáže zařízení a infrastruktury IoT s cílem omezit nebo zastavit výrobu. Z výše uvedených skutečností by měli informační technologie splňovat nejpřísnější kritéria kybernetické bezpečnosti jak v oblasti hardwaru, softwaru a komunikačních prostředků, tak i v oblasti lidských zdrojů. Otázkou ovšem zůstává, jakým způsobem budou technologie IoT expandovat do této sféry. Většina možných míst, kde by bylo možné využít aplikací zařízení Internetu věcí, je již realizována jiným způsobem, který má dobře vyřešenou otázku bezpečnosti.

3.1 Současný stav zabezpečení

Internet věcí je v době vzniku toho dokumentu stále ještě v začátcích svého rozšíření pro využití širokou občanskou veřejností. Z tohoto důvodu se zde setkáváme s bezpečnostními nedostatky a trhlinami, které se již v prostředí kybernetické bezpečnosti vyskytli v minulosti. Některé z těchto nedostatků jsou závažné z důvodu naprostého ignorování některých zásad, které v ostatních úsecích oboru považovány za naprostý

základ. Další text je proto zaměřen na rozbor současného stavu bezpečnosti v IoT. Tímto tématem se také zabývá velké množství analýz, které se problémem zabývají podrobněji např.: odborné materiály od BitDefenderu [15] a Veracode [16].

Většina bezpečnostních mezer, které je v současné době možné nalézt v prostředí IoT, se již v minulosti vyskytla v prostředí internetu. Z větší části se tak stalo v prostředí webu, kde internetové stránky můžeme brát jako paralelu k inteligentním zařízením. Web má delší historii a většina současných bezpečnostních problémů IoT již v jeho prostředí byla vyřešena. Některé z těchto řešení jsou do určité míry implementovatelné do prostředí Internetu věcí. Existují však zde limitující faktory, které se v největší míře vyskytují u malých zařízení, kde zatím není možné zajistit dostatečný výpočetní výkon pro potřebné operace, které budou zajišťovat ochranu.

V prostředí IoT musí být vše bez výjimky zabezpečeno proti cíleným útokům. Toto je jeden z hlavních důvodů, proč se v současné diskutuje na téma rozvoje v této oblasti. Nejprve je tedy zapotřebí specifikovat oblasti, na které bude zaměřena bezpečnost IoT. Přístup k zařízení, přenos dat a systém cloudových služeb jsou hlavní oblasti, které je nutné zabezpečit. V každé z těchto oblastí by se měli dodržovat alespoň minimální úrovně zabezpečení. Cloudové služby pro IoT jsou na rozdíl od zbylých dvou oblastí na dobré úrovni bezpečnosti. Jedná se totiž o dlouhodobě používaný koncept, kde není potřeba vysokého stupně úprav pro využití serverové struktury jakožto IoT cloudu.

V následujícím odstavci jsou popsány některé nedostatky, které byly objeveny u výrobků, které již byly uvedeny na trh. Tyto příklady vychází z výše zmíněných bezpečnostních analýz. Pravděpodobně nejzávažnějším nedostatkem se kterým se lze setkat je přenos zpráv ve formě volného textu. Tento problém se vyskytl jak u přenosu zpráv mezi zařízením a přístupovým bodem (do internetu) tak i v samotné komunikaci v internetu. Útočník, který je schopen tyto zprávy odchytit se dozví všechny informace o zařízení bez dalšího vloženého úsilí. Použitím šifrovacích algoritmů se dá zabránit těmto situacím. Tyto algoritmy ale musí být dostatečně robustní a musí být správně implementovány. Na trhu byl objeven produkt, který komunikoval s klientskou aplikaci zprávami ve volném textu a pouze daty zašifrovanými 128 bitovým AES algoritmem. Přestože heslo bylo šifrované, bylo lehce prolomitelné, protože klíč šifry byl sestaven s využitím MAC adresy zařízení a jeho identifikačním číslem, kde tyto údaje byly poslány před heslem ve volném textu. V této chvíli má potenciální útočník vše potřebné pro prolomení šifry a získání hesla. S tímto je spojená další slabina, která se může vyskytnou u takovýchto zařízení, a to je neschopnost bránit se podstrčení falešných zpráv pro manipulaci s nimi. Tento problém se dá odstranit vynucením autentifikace a autorizace zpráv mezi koncovými body. Mezi další slabiny současných zařízení například patří nedostatečné zabezpečení (někdy nepřítomnost zabezpečení) komunikace při inicializaci spojení po spuštění nebo restartu systému, slabá ochrana testovacích a debugovacích procesů běžících na pozadí (kterými mohou prosakovat data ze systému), atd.

Jedním z největších bezpečnostních rizik v oblasti kybernetické bezpečnosti je ale stále lidský faktor. Ne všechna zařízení vynucují pevná hesla (alespoň 7 znaků, použití

malých a velkých písmen, využití číslic atd.). Slabá hesla jsou náchylná k brute force útokům a pokud útočník pronikne do systému, je většina implementovaných bezpečnostních mechanizmů irelevantní. Další oblastí, kterou někteří uživatelé ignorují, je zabezpečení přístupu k wi-fi, přes kterou jsou zařízení připojena do internetu. Velké množství wi-fi síti stále ještě používá bezpečnostní šifrovací algoritmus WEP, který je snadno prolomitelný v řádu jednotek až desítek minut (v závislosti na množství dat přenášených na síti). Novější zařízení naštěstí zcela upouští od zahrnutí WEP algoritmu a většinou defaultně operují s modernějším WPA2-PSK, který je mnohem náročnější na prolomení. Dalším z častých opomenutí při zabezpečení domácích sítí je ponechání defaultních přihlašovacích údajů k zařízením. Existuje ještě řada dalších doporučení, čemu se vyvarovat při realizaci domácí sítě se zařízeními IoT např.: vypnutí vzdáleného přístupu k zařízením, použití kabelových spojů místo bezdrátových (v místech kde je to možné). Neméně důležité je provést průzkum trhu a seznámení se s nejnovějšími trendy v oblasti bezpečnosti IoT.

3.2 Přehled nejčastějších útoků v IoT

Stejně jako u ostatních částí otázky bezpečnosti Internetu věcí, jsou i způsoby útoky prováděné na zařízení IoT podobné již známým způsobům z prostředí počítačových sítí. Tato podkapitola proto bude zaměřena na seznámení s nejčastějšími z možných útoků.

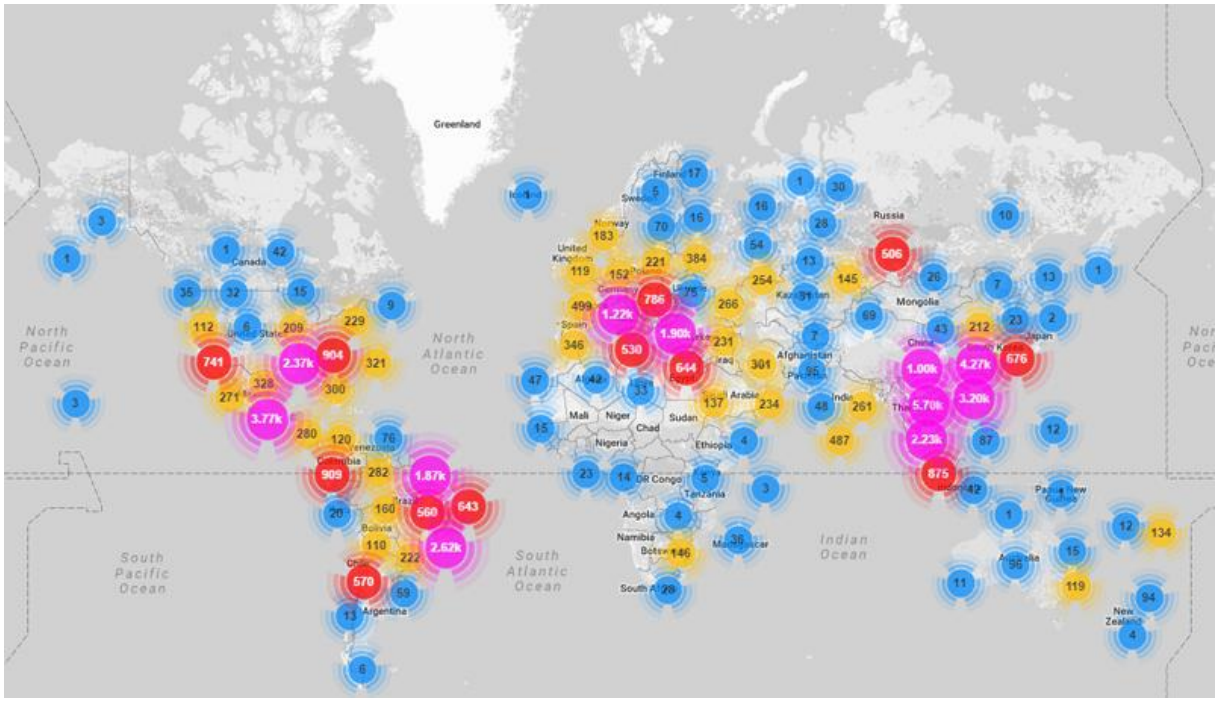
Man-in-the-middle attack – V tomto druhu útoku, narušitel odposlouchává a manipuluje s komunikací mezi dvěma zařízeními. Principem je přesvědčit obě strany spojení, že stále komunikují napřímo mezi sebou. Pro tento účel musí být útočník schopen vytvářet falešné zprávy, se kterými je schopen překonat bezpečnostní mechanizmy spojení. Nejčastěji je možné tento útok provést v sítích s nedostatečnou (popřípadě chybějící) autentifikací spojení. Dostatečně robustní autentifikace na zabezpečeném kanále je také nejúčinnější ochranou před tímto druhem útoku.

Replay attack – Tento útok se provádí úmyslným zpožděním nebo opakováním reálných zpráva od jednoho zařízení s cílem zmatení druhého. Tímto způsobem si může útočník vynutit nesprávnou nebo duplicitní sekvenci odpovědí od zařízení, ze které je schopen získat informace nutné pro přístup k tomuto zařízení. Ochrannou proti tomuto útoku zahrnutí dalších kontrolních informací, které jsou platné pouze pro jedno použití. Jiným možným způsobem ochrany je zavedení synchronizace mezi zařízeními.

Denial of service (DoS) – Principem tohoto útoku je vyřazení zařízení z provozu jeho přetížením pomocí velkého množství zpráv (většinou se jedná o zprávy s prázdnými požadavky na cíl útoku). Nezbytnou znalostí pro provedení tohoto útoku je znalost IP adresy cíle. Bezpečnostní opatření před tímto druhem útoku se většinou implementují na síťové prvky před potencionální cíl útoku. Jelikož pro úspěšné provedení tohoto útoku je potřebné velké množství zařízení, které mají za úkol posílat požadavky na cíl útoku, tak

se v prostředí IoT setkáváme s jiným úskalím. IoT zařízení se díky svému vysokému počtu a nízkému stupni zabezpečení staly častým cílem jiných druhů útoky (nejčastěji malware) se záměrem jejich infikovaní, aby byly následně využity jako zdroj síťového provozu pro útoky DoS.

Malware – Termín malware je zkratkou pro malicious software, tedy pro software určený k narušení chodu infikovaného zařízení (mezi nejčastější cíle patří počítače, mobilní telefon a v současné době IoT zařízení). Jak bylo zmíněno, existuje velké množství zařízení IoT s nedostatečným zabezpečením. Nejčastěji se jedná o zneužití rozšířenosti slabých hesel, jak se tomu stalo v případě malwaru Mirai [17]. Ten obsahoval seznam nejčastějších hesel a způsobem brute force byl schopen proniknout a infikovat zařízení pro jejich využití při DoS útocích. Jedním ze největších problémů malware útoku jako je Mirai, je skutečnost, že škodlivý software může zůstat aktivní v zařízeních po dlouhou dobu bez povšimnutí. Na Obr. 3 je zobrazena mapa rozšíření zařízení infikovaných malwarem Mirai.



Obr. 3 Rozšíření malwaru Mirai, převzato z [17]

Útoky na lokální sítě – Pokud se povede útočníkovy nabourat do lokální sítě (nejčastěji získáním hesla od špatně zabezpečené wi-fi) obsahující inteligentní zařízení, tak může ve velké části případů převzít plnou kontrolu nad těmito zařízeními. Tohoto je možné dosáhnout, protože jedním z rozšířených nedostatků je přenos zpráv v místní síti ve volném textu. U zařízení, která ještě komunikují s cloudovou službou musí útočník ještě provést Man-in-the-Middle útok, pro získání kontroly nad tímto zařízením.

Útoky na Cloud – Někteří výrobci IoT poskytují cloudová řešení pro své výrobky (existují i případy kdy je připojení do cloudu vynucené). Cloud je většinou dobře zabezpečen před útoky na svou strukturu, ať už funguje na hardwaru třetích stran nebo

u výrobce technologie. V kontrastu k této skutečnosti, většina služeb není dobře chráněná před neoprávněným vniknutím. Opět se zde setkáváme s problematikou nevynucování silných hesel v kombinaci s nedostatečnou ochranou před opakovanými neúspěšnými pokusy o přihlášení [18]. Některé ze současných cloudových služeb také mají nedostatečně vyřešené algoritmy pro obnovu zapomenutých hesel, kdy při procesu systém poskytuje citlivé informace o majiteli účtu, nebo dokonce nevyžaduje autorizaci pro dokončení změny hesla.

Direct Access – Téměř všechna zařízení (nejen síťová) jsou mnohem náchylnější k neoprávněným zásahům, pokud má útočník fyzický přístup k nim. V takovémto případě si útočník může vytvořit zadní vrátka pro přístup systému nebo pozměnit chod zařízení bez větších problémů. Zkušení útočníci mohou s takovýmto přístupen být i schopni číst obsah vnitřní paměti zařízení nebo jeho firmware. Největším problémem pro tento druh útoku je získání fyzického přístupu k zařízení na potřebnou dobu pro provedení modifikace zařízení nebo jeho chodu. Z tohoto důvodu útočníci jsou většinou z okruhu přátel majitele zařízení, v tomto případě se většinou jedná pouze o neškodné upravení chodu zařízení za účelem žertu. Jedním z alternativních způsobů, jak získat zařízení se kterým bylo manipulováno je při koupi z druhé ruky. V tomto případě mohou být potencionální následky mnohem závažnější. Z tohoto důvodu by se měl každý vyvarovat možnosti koupě zabezpečovacích zařízení, jako jsou bezpečnostní kamery a zámky z druhé ruky. Ke stejným následkům může dojít i v situaci pokud se útočníkům podaří infiltrovat výrobce zařízení. Poté za pomoci falešných softwarových updatů jsou útočníci schopni provést stejné zásahy do zařízení, jako kdyby měli k nim přímí přístup, ale v mnohem větším měřítku. Pokud se na takovéto zásahy přijde včas, je možné vše vrátit do původního stavu bez větších škod, bohužel ne vždy je možné reagovat včas a na některé z těchto útoků se nemusí přijít dlouhou dobu.

4 Veřejné osvětlení

Velkou částí této diplomové práce je také práce s veřejným osvětlením. V pozdějších částech textu se bude využívat názvosloví z této oblasti, proto je nutné popsat základní části veřejného osvětlení. Na Obr. 4 a je vidět popis moderního sloupu veřejného osvětlení.

Obr. 4 Popis sloupu veřejného osvětlení, převzato z [19]

Takovéto sloupy se vyrábí hlavně z válcovaných ocelových trubek následně upravených pozinkováním (využívají se také jiné možnosti úpravy povrchu např.: nátěr barvou), ale je také možné se setkat se sloupy z litiny a podobných materiálů. Výška sloupů se může pohybovat od 3 m a může přesáhnout až 12 m.

Starší sloupy veřejného osvětlení byly ještě běžně osazeny paticí. Osazování sloupů paticemi je v současné době spíše výjimečné. Při tomto řešení se elektrická výzbroj pro sloup umisťovala do patice místo dovnitř dříku stožáru. Patice se vyráběly z betonu, plastů nebo litiny (historické/okrasné).

Osvětlovací tělesa (Svítidla podle Obr. 4) používaná v současné době se dělí převážně do dvou kategorií, a to výbojky a LED světla. Výbojky se využívají hlavně plněné sodíkovými nebo metalhalogenidovými plynovými směsmi. V minulosti se ve velké míře používalo rtuťových výbojek, které ale způsobují vysoké světelné znečištění. LED světla se začala využívat teprve nedávno poté, co bylo možné dosáhnout podobných hodnot světelného toku jako u výbojek. Podle různých laboratorních testů, budou LED svítidla schopná dosáhnout vyšších hodnot světelného toku než výbojky. Nejvyšší nevýhodou LED světel je stále ještě jejich vysoká cena.

Elektrická výzbroj sloupů veřejného osvětlení je umístěna v dříku stožáru za dvířky. Elektrická výzbroj je souhrnný termín pro nezbytné zařízení, které zajišťují provoz sloupu. Jedná se hlavně o svorky umožňující propojit silové obvody v trase stožárů, dále napojení a pojistky pro svítidlo ve stožáru.

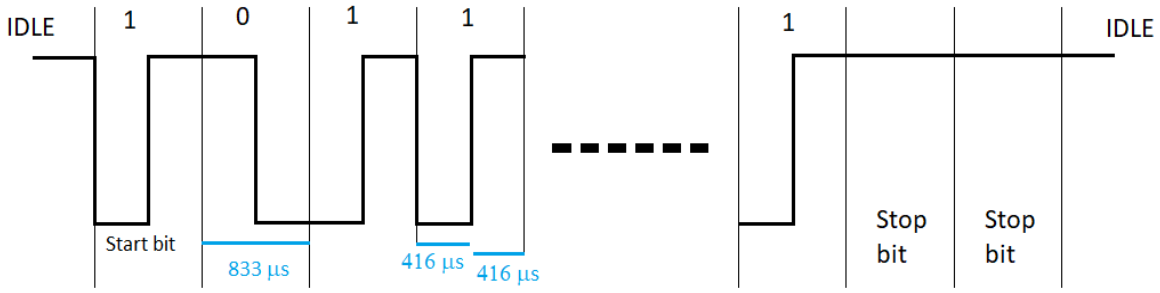
4.1 Protokol DALI

DALI (Digital Addressable Lightning Interface) je komunikační protokol pro systémy ovládání osvětlovacích soustav. Protokol DALI je definován normou IEC 62386 [20]. Jedná se o nástupce analogového systému 1 – 10 V. Systémy DALI se používají hlavně pro ovládání osvětlení v kancelářských budovách, ale je možné je využít i v lampách veřejného osvětlení. Světelné zdroje jsou ovládány pomocí předřadníků, kterými je možné regulovat úroveň osvětlení, dobu náběhu mezi jednotlivými úrovněmi osvětlení, světelné scény ale lze také kontrolovat stav osvětlovacího tělesa apod. Komunikace mezi předřadníkem a centrálním řídícím prvkem probíhá po páru vodičů (DALI sběrnice). Tato sběrnice je koncipována tak, že nezáleží na tom, jakým způsobem jsou vodiče zapojeny. Řídícím prvkem je většinou počítač (server), který je připojen ke sběrnici. DALI sběrnici je k počítači možné připojit přes redukci na jiné rozhraní, a to nejčastěji na Ethernet nebo sériovou linku RS232.

DALI protokol umožnuje využívat:

- Až 64 jednotlivých osvětlovacích těles
- Až 16 skupin osvětlovacích těles
- Až 16 různých nastavení osvětlení

Signál přenášený mezi jednotlivými zařízeními využívá principů Manchesterského kódu, kdy náběžná hrana je považována za logickou „1“ a sestupná hrana za logickou „0“. Vyšší úroveň napětí je v rozmezí +9,5 – +22,5 V a nižší úroveň se pohybuje mezi -6,5 V - +6,5 V. Protokol DALI pracuje s rychlostí 1200 b/s, z čehož plyne, že délka celého pulzu 833 μs +/- 10 %.



Obr. 5 Ukázka signálu DALI protokolu

DALI protokol využívá několika druhů zpráv, mezi které patří:

- master -> slave

začátek rámce	adresa	data	konec rámce
1 b	8 b	8 b	2 b

- master <-> master

začátek rámce	adresa	data	konec rámce
1 b	8 b	16 b	2 b

- slave -> master (odpověď na zprávu master -> slave)

začátek rámce	data	konec rámce
1 b	8 b	2 b

Struktura adresové části rámce je poté YAAA AAAS:

- Y: typ adresy (0 – krátká adresa / 1 – skupinová adresa)
- A: adresové bity, až 64 jednotlivých adres
- S: určení druhu zprávy (0 – data obsahuji úroveň osvětlení / 1 – data obsahují příkaz)

Struktura datové části rámce master -> slave, jak již bylo zmíněno, je řízena bitem S z adresové části. Pokud je bit S v 0, poté se v datové části nastaví úroveň osvětlení v 253 krocích (pokud je hodnota 00hex poté se světlo zhasne, při FFhex se zpráva ignoruje). V případě, že je bit S v 1, poté se v datové části zprávy nachází příkaz pro ovládání předřadníku. Tabulka jednotlivých příkazů je k dohledání v normě IEC 62386 [20].

4.2 Současný stav inteligentního veřejného osvětlení

S rozvojem technologií Internetu věcí a poklesem cen LED osvětlovacích těles, nastává v poslední době rozvoj inteligentních sloupů veřejného osvětlení. Velké množství společností se snaží přijít na trh s co nejzajímavějším a nejúspornějším řešením pro inteligentní veřejné osvětlení. Nejedná se pouze o regulaci úrovně osvětlení na vnějších klimatických podmínkách, ale také o možnost nabídnout širokou škálu nových služeb.

Jak již bylo řečeno nejčastěji řešeným problémem v této oblasti, je možnost regulace osvětlení. Tohoto se většinou dosáhne nastavením světelného profilu v řídící jednotce (může se jednat o systém DALI nebo o jiný specializovaný hardware). Velkou výhodou je, že je možné zasáhnout do pracovního režimu osvětlení na dálku z řídícího centra, tak jak to je koncipováno v systému od společností Philips a Vodafone [21]. S tímto je provázaná možnost plné kontroly a monitoringu systému veřejného osvětlení. V takovémto případě jednotlivé lampy hlásí svůj stav a poruchy, které na nich mohou nastat. Na rozdíl od těchto řešení, která jsou spíše koncipována pro majitele veřejného, jsou ostatní chytrá řešení cílena na občany a většinou se jedná o služby sloupu veřejného osvětlení. Mezi tyto projekty patří chytré lampy Pražské Energetiky, které se nacházejí v Pražských částech Holešovice a Vršovice. Tyto sloupy veřejného osvětlení mají zabudovány senzory měření hluku, teploty, tlaku, vlhkosti vzduchu a stavu ovzduší. Dále je lze využít pro připojení na internet nebo pro dobíjení elektroniky včetně možnosti nabití elektromobilu [22]. Jiným směrem se vydali v Německém Wipperfürthu, kde mají v historickém centru města lampy s vybavené barevnými LED moduly pro speciální světelné scenérie. Tyto lampy také disponují Bluetooth rozhraním, které spolupracuje s mobilní aplikací WippApp, přes kterou se dají získat turistické a historické informace o okolí lampy veřejného osvětlení, se kterou aplikace komunikuje [23]. V budoucnu se budeme setkávat s velkým množstvím dalších různorodých aplikací s tím, jak se budou ve městech obměňovat a modernizovat systémy veřejného osvětlení.

Většina inteligentních stožárů veřejného osvětlení, jak již bylo řečeno, komunikuje s řídícím centrem. Tato komunikace může probíhat několika způsoby. Druh komunikace většinou závisí na rozsahu služeb inteligentní lampy (velikosti datového provozu). Jedním z faktorů pro výběr technologie je volba topologie zapojení, kdy každá lampa může mít svůj vlastní komunikační modul, který komunikuje s dispečinkem. Jiné řešení spočívá v použití centrálního prvku, který na základě dílčích komunikací s jednotlivými moduly umístěných ve stožárech veřejného osvětlení komunikuje s dispečinkem. Mezi komunikační technologie, se kterými dále můžeme setkat patři LPWAN technologie, M2M SIM karty [21] apod. Přestože se většinou využívá bezdrátových technologií je také možné se setkat připojením inteligentních lamp do již fungující infrastruktury rozvodů internetu. Popřípadě je také možné se setkat s osamocenými systémy, které nekomunikují s okolním světem, ale poskytují jiné služby, díky kterým se dají nazvat inteligentními.

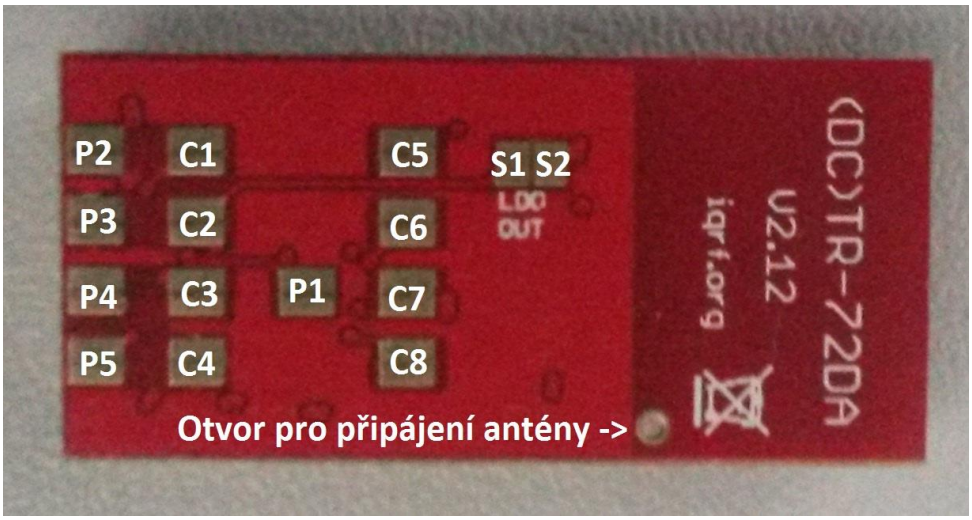
5 Představení IQRF hardwaru a principů práce s ním

Praktickou ukázkou využití zařízení Internetu věcí bude realizace demo aplikace ovládání veřejného osvětlení. Nejprve je ale nutné si představit hardware technologie IQRF a jak se s ním pracuje. Pro realizaci dema bude použit vývojářský kit IQRF DS-START-04.

5.1 Obsah vývojářského kitu DS-START-04

Development kit pro IQRF obsahuje následující komponenty, které jsou zobrazeny na Obr. 6 - Obr. 8:

- 3x IQRF komunikační modul TR-72DA, Obr. 6 [24]
- 1x Programátor CK-USB-04A, Obr. 7
- 2x Univerzální přenosový koncový modul DK-EVAL-04A, Obr. 8
- 1x USB to Micro USB kabel
- 1x USB flash disk se softwarem, dokumentací a příklady pro IQRF moduly

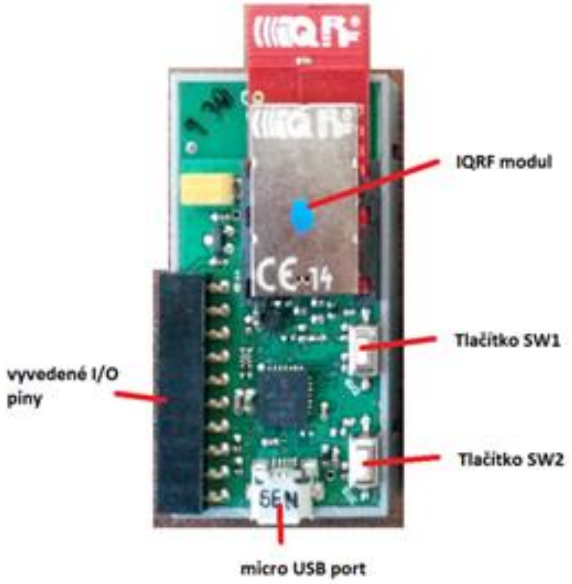


Obr. 6 Zadní strana komunikačního modulu TR72-DA

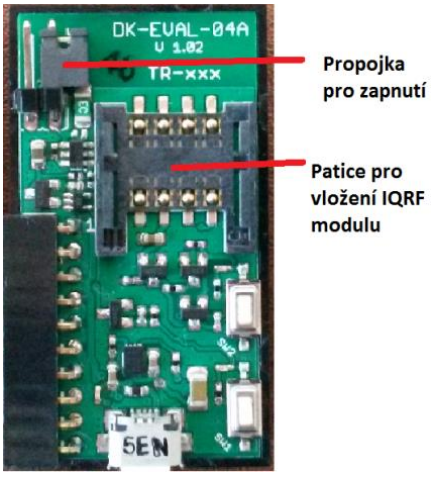
Popis jednotlivých vývodů z komunikačního moduluTR-72DA:

- C1 – obecný I/O, vstup analogového komparátoru
- C2 – obecný I/O, napěťový výstup Vout = +3 V LDO
- C3 – Vin vstup pro napájení

- C4 – Zem
- C5-C8 – obecný I/O
- P1-P5 – pouze pro účely výrobce
- S1-S2 – propojení umožní používat C2 jako napěťový LDO výstup



Obr. 7 IQRF programátor CK-USB-04A s vloženým komunikačním modulem



Obr. 8 Popis rozdílných součástí DK-EVAK-04A (oproti CK-USB-04A) bez komunikačního modulu

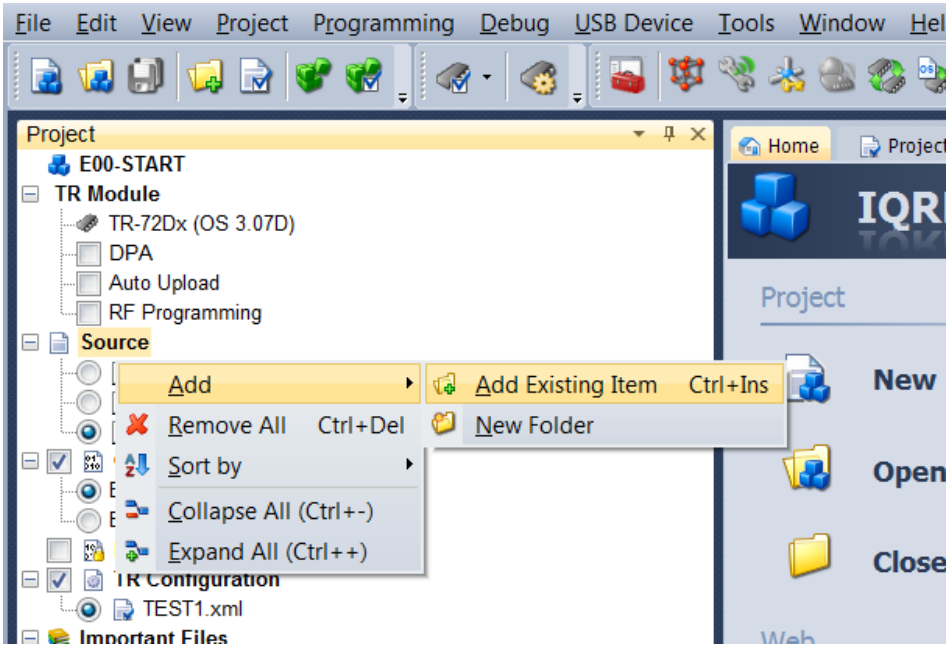
5.2 Příprava vývojářského prostředí

Pro naprogramování jednotlivých komunikačních modulů bude použit program IQRF IDE, který je v současné době ve verzi 4.36 (v době vzniku této práce). Instalační souboru a dokumentace pro tento program se nalézá na flash disku, který je součástí vývojářského kitu. Na disku se nalézá soubor iqrf_ide_432_setup, který se nachází v adresáři …/IQRF_OS307_7xD/ IQRF_IDE. Alternativně je možné stáhnout instalační soubor z webu výrobce [25]. Po spuštění souboru započne instalace, ve které se budeme řídit instrukcemi na obrazovce. Při instalaci je potřebné také zvolit výchozí adresář pro projekty. Po úspěšném ukončení instalace, je možné spustit vývojové prostředí, kde bude nabídnuta možnost upgradovat program na nejnovější verzi (na disku se nachází instalátor pro verzi 4.32).

Ještě předtím, než je možné začít programovat, musí se založit projekt a zkontrolovat některé nastavení a funkce. Nový projekt je možné založit po rozkliknutí lišty *Project* a zvolení možnosti *New Project* (klávesová zkratka Shift+Ctrl+N). V tomto budě je nutné zadat jméno projektu a vybrat výchozí adresář. Nyní by se mělo otevřít okno Project, ve kterém je možné spravovat zdrojové kódy, a jejich zkompilované verze (soubory s příponou .hex). V tomto okně musíme zkontrolovat, jestli je vybrána správná verze přenosových modulu, které budeme používat a také operační systém modulů. Do nastavení se dostaneme přes lištu *Project* a položku *Properities -> TR Module,* kde vybereme hodnoty Select TR Module: TR-72Dx a Select OS: OS 3.07D. Pokud se hodnoty lišili, tak by mohla nastat chyba při kompilaci jednotlivých zdrojových kódů (toto nastavení je použito v této práci, z důvodu využití knihoven pro verzi operačního systému OS 3.07D).

Zdrojové kódy pro jednotlivé přenosové moduly se musí založit mimo prostředí IQRF IDE (k projektu je možné připojit pouze již existující soubory). V pracovním adresáři proto vytvoříme nový soubor textového editoru (například notepad++) a uložíme ho s příponou .c (v notepad++ můžeme postupovat způsobem: uložit jako - Uložit jako typ: C source file(*.c)). Všechny úpravy zdrojového kódu budou posléze probíhat za použití externího textového editoru. Poté co jsou soubory založeny, je potřeba je připojit k projektu. Tohoto se docílí tak, že v okně Project se klikne pravým tlačítkem myši na položku source a zvolí se možnost Add -> Add Existing Item (Obr. 9). V tuto chvíli se otevře nové okno s průzkumníkem, ve kterém se postupně vyberou oba soubory se zdrojovými kódy.

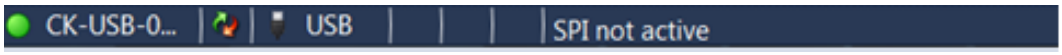
Před přesunem k samotnému programování je potřebné vysvětlit některé často opakující se úkony – kontrola stavu připojení zařízení k počítači, kompilace zdrojových kódů a jejich nahrání do komunikačního modulu.



Obr. 9 Připojení zdrojového kódu k projektu

- Připojení programátoru k počítači: Do počítače se bude připojovat pouze programátor CK-USB-04A (šedý kit), pomocí rozhraní USB. Kontrola stavu připojení se poté zobrazí v dolní části obrazovky, kde obě možnosti (nepřipojeno/připojeno) jsou vidět na Obr. 10, respektive na Obr. 11.

Obr. 10 Stav připojení programátoru k *PC – nepřipojeno*



Obr. 11 Stav připojení programátoru k *PC – připojeno*

- Kompilace zdrojového kódu: Kompilaci se provede vybráním požadovaného zdrojového kódu (okno Project -> source) a stiskem klávesy F10. Kompilací vznikne soubor s příponou .hex, který se opět zobrazí v okně Project.
- Nahrání kódu do komunikačního modulu: Do komunikačních modulů se nahrávají soubory .hex vzniklé kompilací. Vybráním požadovaného .hex souboru (okno Project -> Output Hex) a stiskem klávesy F5 (před nahráním se musíme ujistit, že máme zaškrtnuté políčko Output Hex, jinak vyskočí chybová hláška).
- Každý zdrojový kód musí obsahovat také cestu k adresářům, ve kterých se nachází knihovny, které bude program využívat. Knihovna, která bude využívána, se jmenuje template-basic.h. Na flash disku, který je součástí vývojářského kitu, je cesta k této knihovně: .../Development/include/IQRF_OS. Je však výhodné si knihovnu uložit do pracovního adresáře a poté použít příslušnou cestu. Bez

zahrnutí této knihovny by jednotlivé programy nešli zkompilovat. Celý příkaz na zahrnutí knihovny poté má následující tvar *#include "../../../Development/include/IQRF_OS/template-basic.h"*

- Pozn.: V následujícím textu zabývajícím se programováním modulů je několikrát odkázáno na IQRF OS refenence guide (IQRF OS v3.08D Ref. guide for TR-7xD [26]). V tomto dokumentu je popsána funkcionalita a syntaxe jednotlivých příkazů, které jsou specifické pro IQRF moduly (IQRF moduly se programují za pomocí rozšířené verze jazyka C).

5.3 Ukázky principů programování IQRF modulů

V této kapitole budou popsány jednoduché aplikace využití IQRF. Na těchto ukázkách budou vysvětleny jednotlivé principy funkcionality IQRF hardwaru, které poté budou použiti při řešení samotné praktické části práce.

Načtení dat do bufferů:

Pro práci s daty v programovém prostudí IQRF IDE je nejjednodušší využít již existujíc bufferů. Přestože každý buffer má svůj vlastní specifický účel, lze jej využít i jako datové struktury, které mají vlastní příkazovou sadu pro práci s nimi. Buffery se dají naplnit daty dvěma způsoby. Prvním způsobem je nahrání dat do paměti EEPROM. Použitý příkaz pro nahrání dat do paměti je #pragma cdata[__EEAPPINFO] = "0123" (tento příkaz je mimo hlavní metodu), kde jsou mezi uvozovkami příslušná data. Takto uložená data se načtou do bufferuINFO za použití příkazu getInfo(). Data lze přesouvat do jiných bufferů nebo pamětí příkazem Copy, kde plná syntaxe obsahuje počáteční lokaci dat a cílovou např.: copyBufferRF2COM(); (viz. Reference guide). Druhým způsobem, kterým je možno manipulovat s daty je napřímo je uložit do požadovaného bufferu. Pro načtení dat tímto způsobem se bude na buffer pohlížet jako na pole, kdy každý bit, který chceme načíst, uložíme zvlášť příkazem bufferINFO[0] = '0'; kde číslo v [] určuje pořadí jednotlivého bytu v bufferu.

Nastavení hodnoty výstupního pinu:

Pro ovládání jednotlivých pinů je nejprve nutné je inicializovat. Inicializace se v kódu nachází ještě před hlavní metodou programu. V hlavní metodě programu je nutné nastavit prvotní hodnotu pinu. Stejným příkazem se také mění výstupní hodnota pinu. Inicializace a nastavení hodnot pinu je zobrazeno v Ukázce 1:

Ukázka 1:

```
#define RE2_TRIS        TRISC.2     //
#define RE2_IO          LATC.2      // Inicializace pinu C2

Void APPLICATION()
{
RE2_IO = 0;                         // Nastavení výstupu na nulovou hodnotu
RE2_TRIS = 0;
…

If (x==1)
RE2_IO = 1;                         // Nastavení výstupu na +3V
}
```

Bezdrátový příjem dat:

Další často využívanou částí programu je přijímání zpráv od jednotlivých modulů v síti. V tomto případě je celkový kód jednoduchý a obsahuje pouze detekci přijatých dat a poté jejich uložení a výpis, jak je vidět na Ukázce 2.

Ukázka 2:

```
if (RFRXpacket())               // Kontrola přijetí zprávy
{
        pulseLEDR();            //  LED indication
        copyBufferRF2COM();     //  Uložení příchozích dat
        startSPI(DLEN);         // Odeslání dat přes SPI
}
```

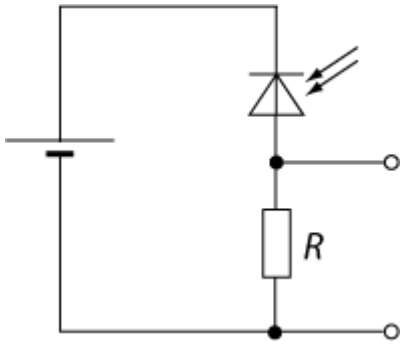
Nastavení IQMESH protokolu:

Každý koncový bod musí obsahovat nastavení síťového protokolu IQMESH. Bez tohoto nastavení by modul zůstal v nastavení pro peer-to-peer přenos. Tohoto se docílí použitím metod pro nastavení koordinátoru, zapnutí směrování, nastavení filtrování sítě atd. Nejprve je nutné do programu zahrnout hlavičky metod a poté je znovu zavolat v programu. Celý proces je k vidění v Refenence guide.

5.4 Realizace ovládání osvětlovacího tělesa soumrakovým senzorem

Další ukázkou, kterou lze za pomocí IQRF modulů realizovat je ovládání rozsvícení lampy veřejného osvětlení za pomocí jednoduchého soumrakového senzoru.

Realizace senzoru je provedena s využitím fotodiody a odporu v zapojení diody jako spotřebiče.



Obr. 12 Zapojení fotodiody

V tomto zapojení se na odporu vytvoří úbytek napětí, v závislosti na osvětlení E_V. Součástky zvolené pro toto zapojení jsou: fotodioda Vishay BPW34 (datashet [27]) a rezistor R = 15 kΩ. Hodnota rezistoru byla učena ze závislosti Závěrného světelného proudu I_{RA} na Osvětlení E_V, kde tato závislost je k nalezení v datasheetu fotodiody. Z IQRF modulu potřebujeme využít vývody pro komparátor C1, zdroj napětí C2 a zem C4. Pro aktivaci pinu C2 jakožto zdroje napětí je potřebné zkratovat dohromady oba piny S1.

Pin C1 je vstup pro analogový komparátor, který bude ovládat tuto aplikaci. Jakožto základ pro programovou část komparátoru se využije jednoho z ukázkových zdrojových kódů pro IQRF. Jedná o soubor z adresáře s pokročilými ukázkami programování IQRF modulů. Tyto ukázky se nachází na flash disku, který je součástí development kitu, v adresáři ...Examples/IQRF_OS/Advanced_examples. Jedná se o ukázku využívající funkci komparátoru. Z tohoto zdrojového kódu se převezme nejen kompletní metoda pro komparátor, ale také způsob, jakým se vyvolá přerušení způsobené změnou stavu komparátoru. Toto přerušení poté zavolá uživatelskou funkci, ve které se poté vykoná požadovaný efekt – rozsvícení / zhasnutí osvětlovacího tělesa. Tato funkce je k vidění v ukázce 3. Posledním zásahem do kódu poté bude nastavení hodnoty pro komparátor. Příkaz k tomuto účelu určený je uvnitř funkce void initComparator(void) a jeho syntaxe je DACCON1 = 16;. Hodnoty pro komparátor se nastavují krocích od 0 (0 V) do 31 (2,9 V).

Ukázka 3:

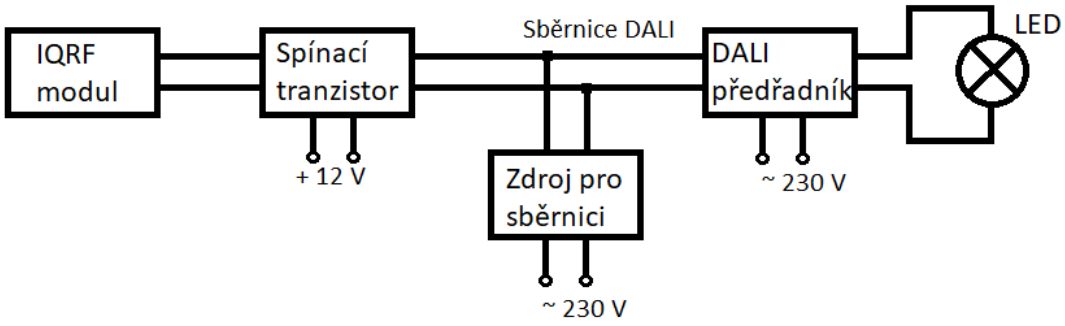
```
if (C2IF)                       // Kontrola přerušení
{
        C2IF = 0;               // Vyčištění příznaku přerušení
        if (C2OUT)              // Kontrola výsledku komparace
        {
                RE5_IO = 1;     // Rozsvícení
        }
        else
        {
                RE5_IO = 0;     // Zhasnutí
        }
}
```

V případě aplikace, kdy fotodioda bude ovládat rozsvícení sloupu veřejného osvětlení je potřeba fotodiodu umístit do takové polohy, aby nebyla ovlivněna světlem z osvětlovacího tělesa sloupu veřejného osvětlení. Z tohoto důvodu je nejvýhodnějším řešením fotodiody vyvést na vrchol osvětlovacího tělesa. Při takovémto umístění také minimalizují problémy s možným zastíněním fotodiody.

Kontrola rozsvícení v závislosti na úrovni vnějšího osvětlení se dá realizovat i jinými způsoby. Prvním z nich je vzít několik IQRF modulů a dedikovat je pro monitoring úrovně okolního osvětlení. Kde každý modul by měl na starosti část sítě. Tímto způsobem se dá vyhnout problémům se světelným rušením (ať už zastíněním nebo rušením od jiných světelných zdrojů). Další výhodou je snížení zátěže baterie a tím prodloužení doby její životnosti. Na druhou stranu se zesložití topologie sítě a je potřebné implementovat robustnější algoritmy na identifikaci zpráv. Druhým způsobem je centrální ovládání celé sítě, kde je možné použít stejných principů jako v předchozím případě anebo využít již existujících řešení senzorů pro IQRF [28]. Na trhu, již také existují podobná řešení, která ale ve většině případu fungují pouze s možností nastavení úrovně osvětlení nebo času kdy se bude svítit. Tato řešení zatím fungují pouze lokálně bez jakékoliv komunikace s možným centrálním prvkem.

6 Realizace DEMO aplikace

Hlavní praktickou ukázkou využití IQRF modulů pro ovládání veřejného osvětlení bude jejich využití, jako ovládacího prvku v obvodu s DALI předřadníkem. Moduly v tomto zapojení budou mít na starosti nejen komunikaci s okolním světem (ostatní moduly, koncentrátor, server), ale také budou, zajišťovat generování zpráv pro DALI předřadník. Tento předřadník poté bude zajišťovat ovládání stavu světelného zdroje. Výhodou takovéhoto zapojení je možnost kompletní regulace světelného zdroje, nastavení různých světelných profilů, možnost ovládání jednotlivých lamp veřejného osvětlení nebo jejich skupin. Na Obr. 13 je vidět blokové schéma pro toto zapojení.



Obr. 13 Blokové schéma zapojení DEMO aplikace

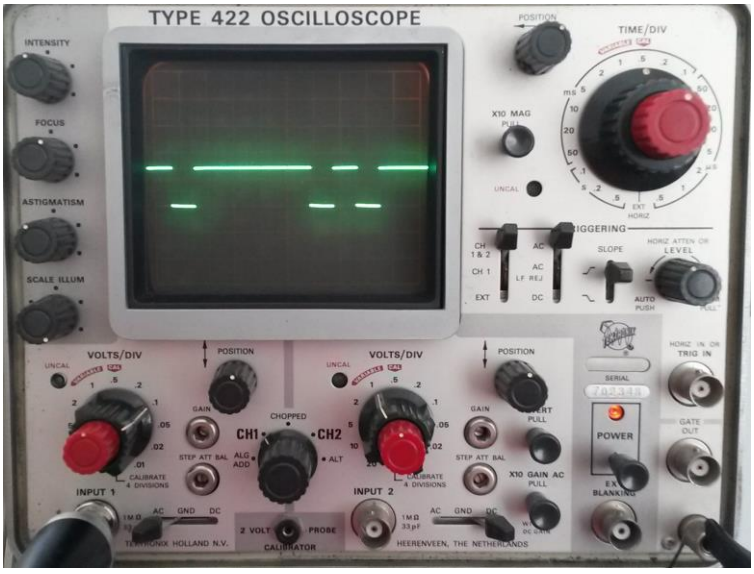
Jak již bylo naznačeno IQRF modul má na starosti 2 úkoly. Prvním je komunikace s ostatními moduly v síti a komunikace s koncentrátorem (serverem). Druhým úkolem je generování signálů pro DALI předřadník. V tomto případě se bude jednat pouze o překlad přijatých dat (data jsou, již ve tvaru DALI příkazu) a jejich následné odeslání po sběrnici. Jelikož IQRF moduly mají maximální výstupní napětí +3 V, je nutné toto napětí převést na vyšší napěťovou hladinu, protože protokol DALI, pracuje se signály, které mají vyšší hodnotu v rozmezí +9,5 - +22,5 V (nízká hodnota je v rozmezí -6,5 - +6,5 V viz kapitola 4.1). Tohoto docílíme připojením IQRF modulu před tranzistor zapojený ve spínacím režimu. Výstup tranzistoru je poté připojen na sběrnici DALI vedoucí k DALI předřadníku. Ke sběrnici je ještě připojen zdroj pro sběrnici, který napájí předřadník. K předřadníku je poté připojeno LED světlo, které se má ovládat.

6.1 Programování IQRF modulu

Program, který bude nahraný v IQRF modulu má na starosti komunikaci a generování signálu pro DALI předřadník. Komunikace v tomto případě bude řešená

stejným způsobem jako u ukázek z kapitoly 5.3 pro příjem zpráv a připojení do sítě IQMESH.

Pro generování signálu pro předřadník DALI, je potřebné napsat zcela nový kód. Prvním krokem pro přípravu tohoto programu je výběr výstupů z IQRF modulu, které budou použity pro připojení sběrnice. V tomto případě se použije pin C2 (obecný I/O) a pin C4 (zem). Pin C2 je nutné inicializovat ještě před začátkem hlavní metody, a uvnitř metody je nutné ho nastavit na hodnotu 0. Signál, který poté budeme vysílat přes pin C2 má tvar Manchesterského kódu, kde log „1“ je reprezentována vzestupnou hranou, log „0“ sestupnou (viz kap. 4.1) a délka jednoho pulzu je 833 μs (polovina pulzu se kterou se bude pracovat je poté 416 μs). Tyto parametry signálu je tedy potřebné simulovat programově. Pro zjednodušení kódu se použije kódování, kde nově log „0“ bude reprezentována dvěma bit 01 a log „1“ bude 10. Takovýto způsob kódování je zvolen také z důvodu využití invertujícího měniče napětí. Takto zakódované jednotlivé bity poté budou generovány změnou stavu pinu C2. Důležitým prvkem zde je časování, aby bylo dosaženo potřebných hodnot délky pulzu. Jedním z problémů operačního systému, který IQRF moduly používají, je že nejnižší jednotka čekání je, kterou lze funkcí vyvolat 1ms (příkaz waitMS(1);). Z tohoto důvodu je nutné využít možnosti generování zpoždění pomocí vnitřních hodin PIC (Peripheral Interface Controller), který je na součástí IQRF modulu. IQRF moduly TR-72D obsahují PIC PIC16LF1938. Nastavení časování proběhlo pomocí příkladů práce s časovači, které jsou dostupné pro PIC obvod PIC16F877 [29], který je ze stejné rodiny jako PIC16LF1938. V materiálu [29] je zobrazen ukázkový kód pro časování s příklady výpočtů potřebných parametrů. Nejdůležitějším z těchto parametrů je počet cyklů, kolikrát proběhne základní hodnota zpoždění. Podle uvedených materiálů proběhl pouze předběžný výpočet této hodnoty, přesná hodnota byla nalezena, po změření průběhu na osciloskopu Tektronix TYPE 422. Na Obr. 14 je vidět snímek z osciloskopu s jednoduchým testovacím průběhem s již správně nastavenými parametry (přes pin C2 se posílá ve smyčce 8b: 1111 1010).



Obr. 14 Zobrazení testovacího půběhu na osciloskopu

Data, která se takto budou překládat a posílat přes pin C2 na sběrnici jsou data, která modul přijme od ze serveru. Obsah zprávy se přesune z bufferRF do bufferCOM, se kterým se poté bude pracovat. Jednou z výhod DALI protokolu je způsob adresace, jelikož každý předřadník má svou vlastní adresu nebo je přiřazen do skupiny. Díky této vlastnosti DALI protokolu, nemusíme programově řešit, jestli je příkaz určen pro danou lampu nebo ne. V ukázce 4 je vidět část kódu pro nastavení časování.

Ukázka 4:

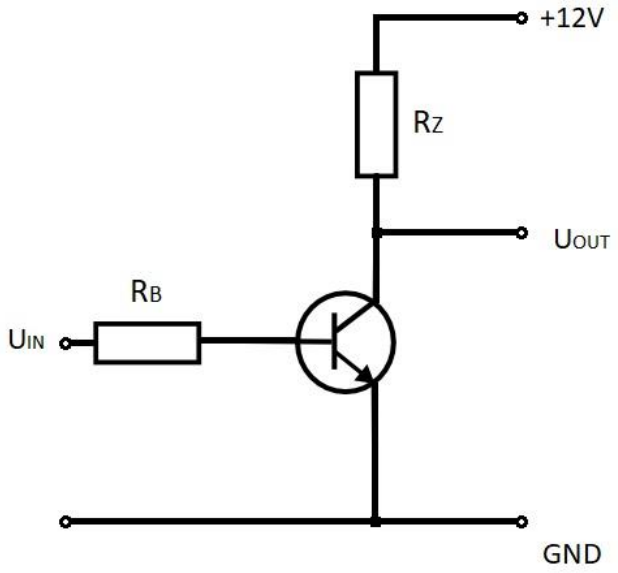
```
RE2_IO = 0;
RE2_TRIS = 0;                // inicializace pinu C2
int Count = 0;               // počet cyklů
int x = 0;;                  // pomocná proměnná
T2CON=0b00000100;            // inicializace T2CON (prescaler a postscaler)
TMR2=0;                      // hodnota start
PR2=0xF;                     // hodnota stop
.
.
.
while(!TMR2IF);                    // program zastaví zde dokud TMR2IF nebude 1
TMR2IF=0;                          // reset hodnoty TMR2IF
Count++;                           // inkrementace proměnné obsahující počet cyklů
if(Count==35)                      // 35 cyklů odpovídá potřebnému zpoždění
{
        Count=0;                   // reset proměnné Count
        if(bufferCOM[x]==0x30)     // posílaný bit je v 0 nebo 1
        {
                RE2_IO = 0;        // pin C2 v nízké úrovni
                x++;               // inkrementace proměnné s počtem bytů zprávy
                if(x==38)          // vysílaná zpráva obsahuje 38 b
                {
                        x=0;       // reset pomocné proměné
                        waitMS(5); // čekání 5 ms mezi 2 zprávami
                }
        }

        else

.
.
.
```

6.2 Změna napětí signálu

Jelikož IQRF moduly generují maximální napětí +3 V a zařízení podle DALI protokolu pracují se signály s vyšší úrovní +9,5 - +22,5 V, je proto potřebné signál převést na vyšší napěťovou hladinu. Pro tento účel je využito zapojení tranzistoru ve spínacím režimu. Jedná se o jednoduché zapojení využívající malého množství součástek (tranzistor a 2 odpory). Toto zapojení je vidět na Obr. 15. Pro účely této úlohy se tedy bude vstupní signál měnit na +12 V (U_N).



Obr. 15 Zapojení tranzistoru ve spínacím režimu

V tomto zapojení je tranzistor při nízké logické úrovni na vstupu rozpojen a na výstupu tedy bude +12 V. Poté co na vstup přivedeme vyšší logickou úroveň, tranzistor se sepne a výstup se spojí se zemí, z čehož plyne, že napětí na výstupu se bude blížit 0 V. V tomto zapojení se signál nejen převádí na vyšší úroveň, ale také invertuje (inverze signálu je řešena programově).

Pro toto zapojení potřebné využít spínacího tranzistoru. Pro testovací zapojení byl zvolen spínací NPN tranzistor BSY 34, který je podle datasheetu [30] schopen pracovat do frekvencí okolo 250 MHz. Proudový zesilovací činitel tranzistoru, který byl použit pro testování tohoto zapojení je β= 45 (β byla změřena přístrojem Digital Multimeter M890G). Pro výpočet odporů je nutné si stanovit proud na kolektoru I_C.

Výpočet odporu R_Z a R_B pro I_C = 200 mA a U_{SAT} = 0,2 V:

$$R_Z = \frac{U_N - U_{SAT}}{I_C} = \frac{12 - 0{,}2}{0{,}2} = 59\ \Omega$$

Pro výpočet odporu R_B je nutné znát proud I_B

$$I_B = \frac{I_C}{\beta} = \frac{0{,}2}{45} = 44\ mA$$

$$R_B = \frac{U_{IN}}{I_B} = \frac{3}{0{,}0045} = 681{,}2\ \Omega$$

Pokud by byl použit jiný spínací tranzistor, je nutné zjistit jeho parametr β (ať už z datasheetu nebo ho znovu změřit) a poté podle toho znovu přepočítat hodnoty odporů.

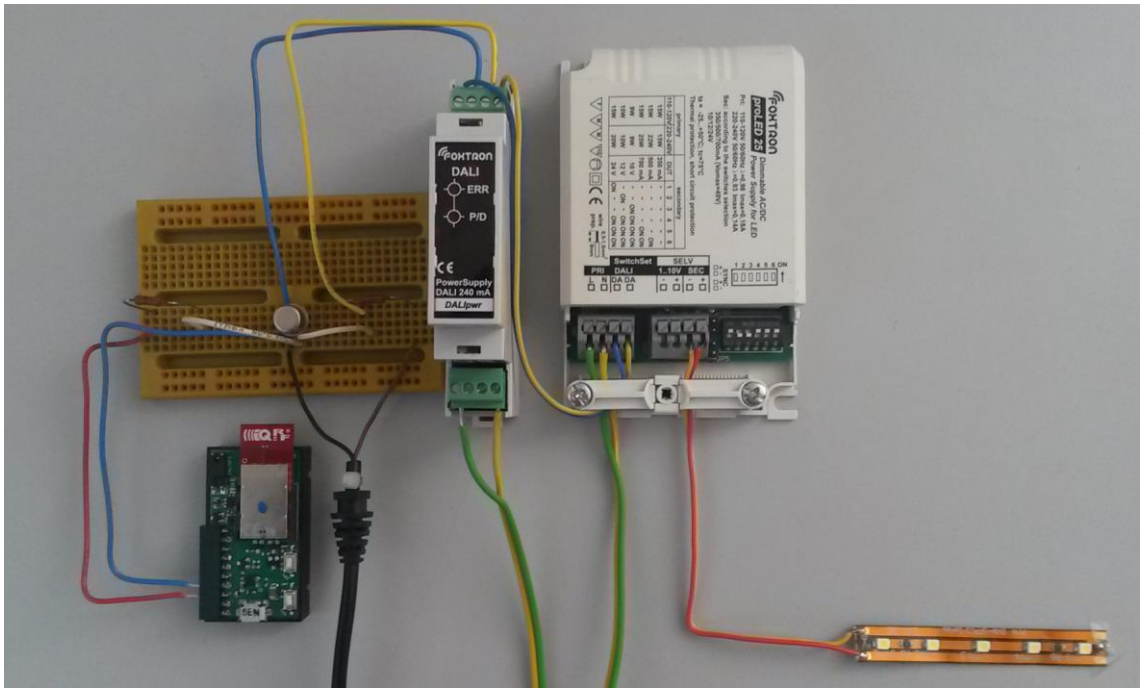
6.3 Připojení DALI hardwaru

Výstup tranzistoru (zapojeného ve spínacím režimu) je připojen na DALI sběrnici, ke které je na druhé straně připojen předřadník a paralelně napájecí zdroj pro sběrnici, jak je vidět na blokovém schématu zapojení (Obr. 13). Sběrnice je dvouvodičová a je navržená takovým způsobem, aby bylo jedno, jak jsou jednotlivé vodiče zapojeny (lze je prohodit). Předřadník se stará o ovládání světla v závislosti na jeho nastavení nebo na přijatých příkazech. Pro nastavení předřadníku je potřebné na sběrnici připojit další specializovaný hardware, který má redukci na některé z rozhraní, které jsou běžné pro počítače (Ethernet, RS232 apod.). Pokud je takto sběrnice připojena k počítači se specializovaným softwarem, poté je možné nastavit vlastnosti předřadníku. Hlavní věcí, kterou je nutno nastavit je adresa jednotlivých předřadníků, popřípadě skupinová adresa. Také je možné nastavit různé světelné scény (jeden předřadník může mít nastaveno až 16 různých scén). Další nastavení se mohou lišit podle výrobce hardwaru. Zdroj pro sběrnici DALI, je nezbytnou součástí zapojení a musí být navržen podle normy IEC 62386 [20]. Zdroj se stará o napájení předřadníků. Každý předřadník potřebuje být napájen maximálním napájecím proudem 2 mA. Maximálně na jedné sběrnici může být připojeno 64 předřadníků, kdy většina zdrojů je navržena na maximální odběr proudu mezi 200 až 250 mA. Ke sběrnici poté může být také připojen další DALI hardware, jako jsou např. světelná čidla nebo jiná ovládací zařízení. Počet dalších zařízení je omezen maximálním dodávaným proudem, kdy většina těchto zařízení odebírá maximálně 4 mA.

Pro tuto úlohu byl vybrán předřadník proLED25 od české společnosti Foxtron. Hlavním parametrem při jeho výběru byla skutečnost, že tento předřadník je určen pro LED světla. Většina DALI předřadníků je totiž určená pro zářivková světla do kancelářských budov. Napájecí zdroj byl poté také zapůjčen od společnosti Foxtron a jedná se o model DALIpwr. Pro nastavení předřadníku byl využit software DALIconfig, kdy předřadníku byla nastavena adresa. Na výstup předřadníku byl pro testovací účely připojen pásek s regulovanými LED. Informace o předřadníku proLED25, zdroji pro sběrnici DALIpwr a softwaru DALIconfig lze nalézt na stránkách společnosti Foxtron [31].

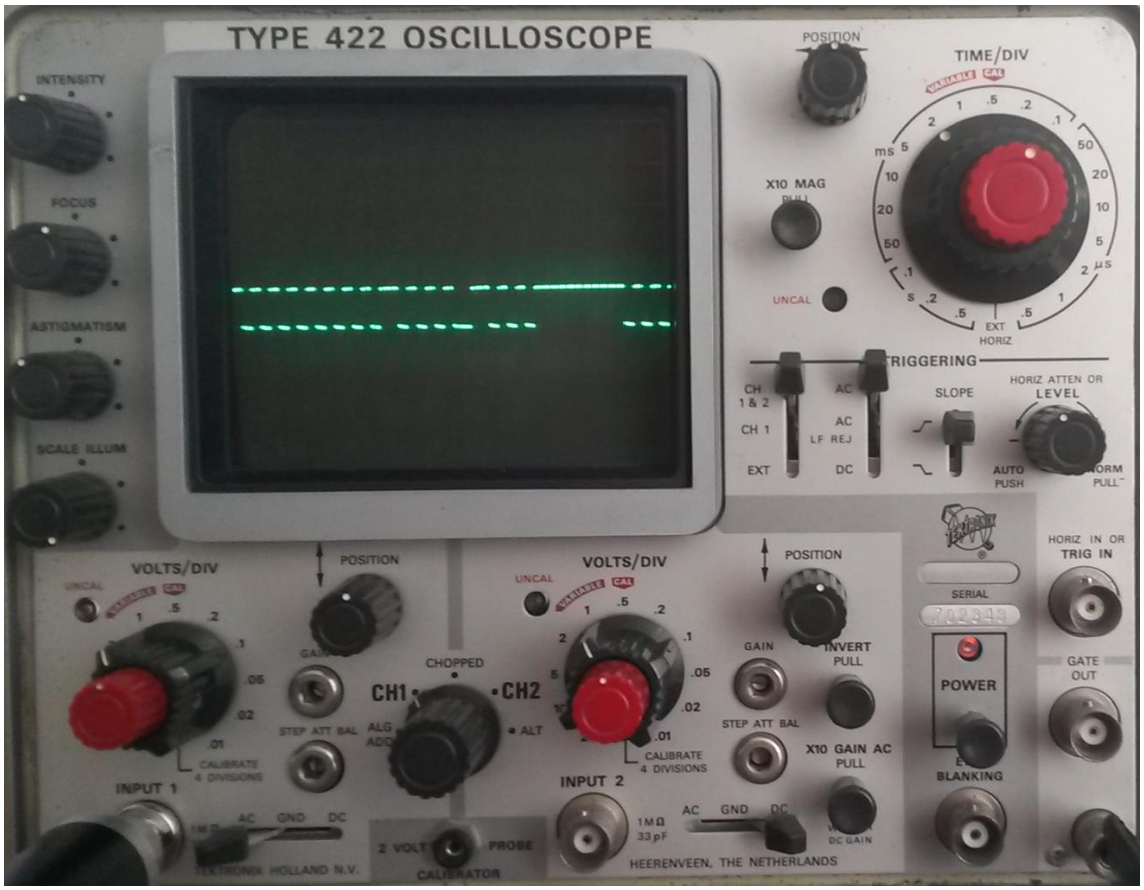
6.4 Testování vysílání dat

Na Obr. 16 je vidět reálné testovací zapojení. Pro testovací účely byl upraven kód z kapitoly 6.1, kdy vysílaný příkaz pro předřadník byl opakován v cyklu (mezi jednotlivými cykly bylo nastaveno zpoždění 1 ms). Vysílaný příkaz má za úkol snížit intenzitu rozsvícení světla o jeden stupeň a po dosažení nejnižší úrovně světlo zhasne. Tento příkaz byl vybrán z několika důvodů. Po připojení napájení do obvodu je prvotní stav LED rozsvíceno, snižováním intenzity v krocích (s využitím jednoduché programové smyčky) je tedy možné zhasnout. Druhým důvodem je zvýšení legitimity celého testování, bez použití zbytečně složitého testovacího kódu. Pokud by test probíhal pouze tak, že by se příkazem zhaslo, nebylo by prokazatelné, jestli zhasnutí proběhlo na základě příkazu nebo chyby (např.: předřadník by LED pásek zhasl po přijetí neplatného kódu jakožto bezpečnostní opatření).



Obr. 16 Testovací zapojení

Prvním testem byla ověřena správnost vysílaného kódu. Pro tento test byl výstup tranzistoru připojen na osciloskop. Na Obr. 17 je vidět koncová část zachyceného signálu. Z toho úseku lze hlavně určit konec zprávy. Stop bit pro DALI zprávu je 2 b ve vyšší napěťové úrovni, ve které poté zůstane signál 1 ms (nastavené zpoždění) až do začátku další zprávy.



Obr. 17 Zachycení zprávy DALI osciloskopem

Druhý test byl zaměřen na celkovou funkčnost zapojení. V tomto případě byl výsledek kontrolován vizuálně.

6.5 Modelové situace pro využití navrhnutého zapojení

Jak již bylo řečeno, toto zapojení je hlavně určeno pro systémy veřejného osvětlení, ale lze ho implementovat v jakékoli prostředí kde je výhodné využít bezdrátového přenosu mezi jednotlivými osvětlovacími tělesy. V následujících odstavcích tedy bude představeno několik řešení pro osvětlovací systémy, které lze upravit pro služby IoT za použití popsaných řešení z této kapitoly.

Sportovní areál:

První modelovou situací, kde lze využít řešení popsaného v této práci je areál sportoviště, který se skládá z několika vnitřních hal a venkovních kurtů. Tento příklad je použit, jelikož na něm lze ukázat rozmanitou škálu aplikací IoT.

Serverová aplikace pro tuto ukázku bude muset zajišťovat: komunikaci s jednotlivými koncovými body, komunikaci s mobilními aplikacemi, webové rozhraní areálu, přístup k jednotlivým databázím, komunikaci s bankovní aplikací atd. Databáze, které budou pro správný chod celého systému potřeba, jsou databáze uživatelů (osobní údaje, přihlašovací údaje, stav peněžních prostředků převedených do systému apod.), sportovišť a jednotlivých světelných scéna (příkazů pro ovládání DALI předřadníků).

V této ukázce budeme uvažovat různá zapojení pro vnitřní a pro vnější sportoviště. V případě vnitřních sportovišť budeme předpokládat, že každé bude mít svůj osvětlovací systém propojen DALI sběrnicí, ke které bude připojen jeden komunikační IQRF modul. U venkovních sportovišť je výhodnější, když každé osvětlovací těleso bude mít svůj vlastní IQRF modul. V obou případech je však nutné přiřadit každému předřadníku vlastní adresu a přidat ho do adresní skupiny podle určeného sportoviště.

Takto vybavený sportovní areál bude mít vlastní webové stránky a mobilní aplikaci pro smartphony, kde si registrovaní uživatelé budou moci předem rezervovat jednotlivá sportoviště. Areál sportoviště je také pokryt wi-fi signálem pro přístup na internet, aby bylo co nejjednodušší využít tuto mobilní aplikace pro ovládání systému osvětlení. U vstupu ke každému sportovišti poté bude umístěna RFID čtečka, kdy po přiložení klubové karty nebo čipu, se spustí rezervace a aktivují se světla na sportovišti. Druhou možností, jak aktivovat světla na sportovišti a začít rezervaci je po přihlášení se k uživatelskému účtu přes mobilní aplikaci nebo přes terminál s dotykovou obrazovkou, který se nachází v prostorách sportovního areálu (tento terminál může být v nejjednodušším případě realizován tablem se spuštěnou mobilní aplikací). Po vypršení rezervace se osvětlení sportoviště začne postupně utlumovat a zůstane dalších 10 minut (nebo do opětovné aktivace dalším uživatelem) na takové úrovni, aby bylo možné sportoviště bezpečně opustit, než se celkově vypne. Rezervaci bude možné ukončit předčasně všemi výše uvedenými způsoby.

Díky využití protokolu DALI je možné mít na předřadníku nastaveno až 16 různých světelných scén. Uživatel sportoviště si tedy bude moci vybrat z těchto typů osvětlení několika způsoby. Prvním možnost výběru bude již při rezervaci sportoviště. Druhý způsob možnosti změny druhu osvětlení je za pomoci mobilní aplikace nebo po přihlášení se k terminálu. Základní scenérie, kterou lze zvolit je rozsvícení všech světel na 80 – 90 % (podle parametrů sportoviště). Díky tomuto nastavení lze poté regulovat úroveň osvětlení nejen na nižší hodnoty ale také na vyšší, popřípadě je možné si vybrat některou z předpřipravených asymetrických světelných scenérií. V případě venkovních sportovišť je možné vybrat možnost regulace osvětlení v závislosti na venkovních podmínkách. Pro tento způsob regulace se využije principů popsaných v kapitole 5.4 (Realizace ovládání osvětlovacího tělesa soumrakovým senzorem). Každý IQRF modul

by k sobě měl připojen soumrakový senzor (nemusí se jednat o takový, jako byl popsán v kapitole 5.4). Modul by poté musel být naprogramován tak aby zkontrolovat příchozí zprávu a při vyhodnocení toho, že byl přepnut do režimu sledování venkovních podmínek by začal ovládat předřadník podle dat vyhodnocených vícestupňovým komparátorem (při použití jiného soumrakového senzoru by musel být kód upraven jinak). Tento mód by se poté ukončil nastavením na jinou scenérii. Serverová aplikace by před touto změnou musela ještě poslat specifický příkaz pro ukončení tohoto módu.

Cena pronájmu sportoviště bude hlavně závislá na druhu sportoviště a době pronájmu. Do ceny ale také může být částečně promítnut zvolený druh osvětlení, bude se však jednat pouze o malou část ceny pronájmu. Doba pronájmu sportoviště se bude počítat po minutách, aby bylo možné pronájem ukončit předčasně. Vyúčtování za využití sportoviště by probíhalo dvěma způsoby. Tyto způsoby jsou placení předem při rezervaci nebo periodické platby za využití sportoviště v uplynulém období. Uživatelé by měli, možnost si také přesunou peněžní prostředky na svůj účet v systému sportovního areálu, ze kterého mohli probíhat oba druhy plateb. V prvním případě placení je nutné počítat se dvěma specifiky. Jelikož se platí předem, je nutné při rezervaci vybrat osvětlovací scénu, a podle tohoto výběru pak nebude možné vybírat z celého spektra světelných scén, ale pouze těch, za které bylo zaplaceno nebo levnějších. Druhým specifikem tohoto způsobu placení je možnost ukončení pronájmu předem, kdy peníze za zbylé zaplacené minuty pronájmu se vrátí na účet uživatele pro použití při budoucích pronájmech sportovišť. Při periodickém placení se konečná cena odvíjí pouze od času využití jednotlivých sportovišť při vybraných osvětlovacích módech.

Venkovní prostory průmyslového areálu:

Druhou ukázkovou situací možnosti využití implementace IoT je způsob úpravy venkovních prostorů v průmyslovém areálu. Na rozdíl od předchozí ukázky zde budou tyto způsoby využití pouze naznačeny. V průmyslovém areálu je situace jednoduší než v předchozím případě, zde se jedná pouze o regulaci osvětlení v závislosti na denní době a stavu úrovně okolního osvětlení.

Pro tuto situaci budeme uvažovat, že každé světla uvnitř areálu má svůj vlastní komunikační modul a předřadník a je k nim ještě připojeno pohybové čidlo. V době, kdy se v areálu pracuje, se jedná opravdu pouze o regulaci stavu osvětlení tak aby v žádném případě nebyla ovlivněna možnost plného provozu v prostorech areálu. Po ukončení provozu v areálu se osvětlení přepne do dalšího režimu, kdy plnou kontrolu nad ním má ostraha areálu. Nyní se úroveň osvětlení v celém areálu sníží, popřípadě se nechají rozsvíceny pouze některé ze světel (nechají se rozsvíceny pouze některé skupiny světel podle jejich skupinových DALI adres). V tento okamžik se také moduly přepnou tak aby spolupracovaly s pohybovým čidlem. Kdy po zaznamenání pohybu se změní intenzita svícení tohoto (popřípadě se rozsvítí) světla na určitou dobu. Pokud by bylo zapotřebí rozsvítit některou část areálu v tuto dobu a ostraha se v tu dobu nenacházela na stanovišti u vjezdu do areálu, tak by se to dalo provést přes terminál umístěný v prostoru za

vjezdem. K tomuto terminálu by se připojilo zaměstnaneckou kartu s RFID čipem. Přes tento terminál by byl možný pouze přístup k základním funkcím jako je rozsvícení světel celém areálu nebo jeho jednotlivých částech v případě rozlehlejších areálů.

Veřejné osvětlení:

Poslední ukázkou možnosti implementace IoT do osvětlení je systém veřejného osvětlení. V tomto případě není nutné se zabývat velkým množstvím služeb, ale o to důležitější je bezchybná funkčnost těch, které jsou implementovány. U veřejného osvětlení se tedy setkáme s regulací osvětlení, komunikací s řídícím centrem, monitoringem stavu, v jakém se osvětlovací těleso nachází a také klimatické podmínky v okolí sloupu veřejného osvětlení.

Regulace úrovně osvětlení a komunikace s řídícím centrem je řešena už samotným použitím DALI předřadníku a komunikačního modulu IQRF. U funkce monitoringu stavu osvětlovacího tělesa je ale zapotřebí dalších úprav navrhnutého řešení. Jedná se nejenom o softwarové úpravy ale také o hardwarové. Většina zpráv pro DALI předřadník je pouze typu master -> slave, ale některé z těchto zpráv mohou vyvolat odpověď. Pro čtení této odpovědi by bylo nutné realizovat měnič napětí z úrovní používaných DALI protokolem zpátky na +3 V. O příjem těchto zpráv by se staral komparátor, který by po přijetí celé zprávy z DALI sběrnice ji přeposlal na server v řídícím centru. Jelikož DALI předřadník dokáže sledovat pouze stav světelného tělesa, které je k němu připojeno, je také nutné k IQRF modulu připojit další senzory které budou sledovat další veličiny nejenom uvnitř lampy ale také v jejím okolí.

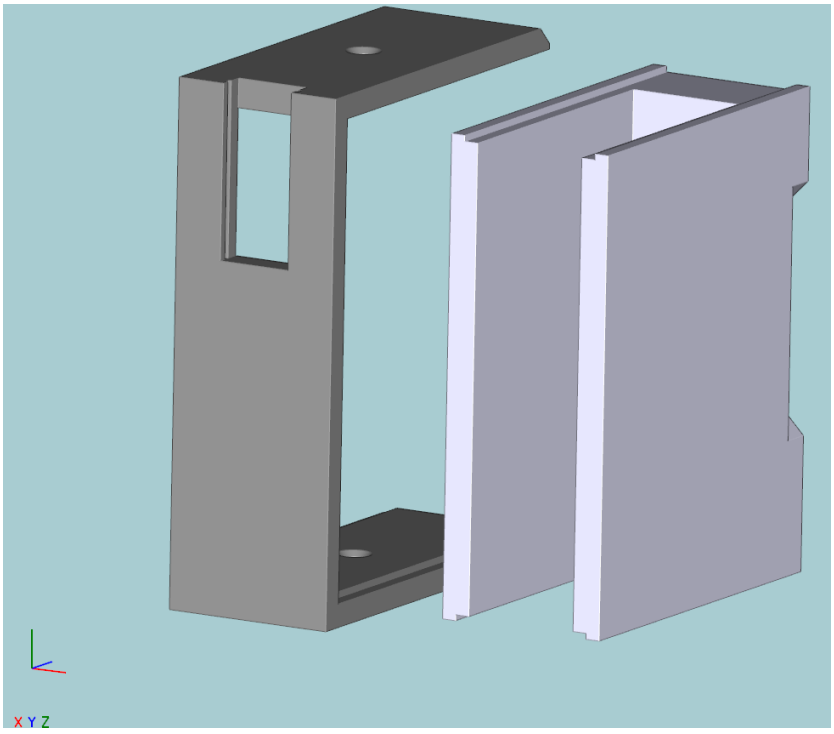
6.6 Návrh ochranného krytu

V poslední ukázce z předchozí podkapitoly se mluví o možnosti využití zapojení ve sloupech veřejného osvětlení. Jelikož se ale nemůžeme umístit komunikační modul do dříku sloupu veřejného osvětlení samostatně, je zapotřebí pro něj navrhnout kryt. Tento kryt musí být mýt dostatečné vnitřní rozměry, aby byl schopen pojmout komunikační modul, plošný spoj s měničem napětí a zdroj energie (baterii). Při návrhu krytu je také nutné dbát na vnější rozměry, aby se kryt vešel do dříku sloupu.

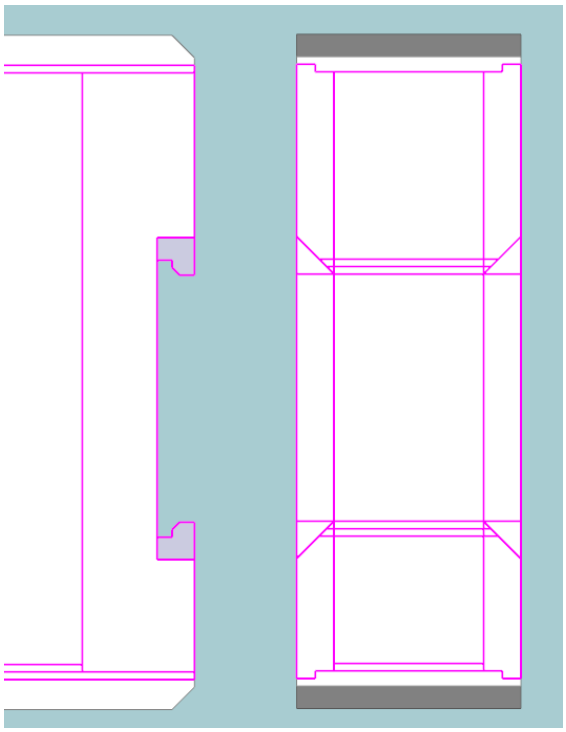
Pro návrh obalu byl použit software VariCAD (verze 2017 1.1), ve kterém je možné navrhnout 3D modely a posléze je uložit ve formátu .stl, který se používá při 3D tisku.

Maximální rozměry pro ochranný obal pro zařízení jsou 90x30x70 mm (V/Š/D). Tyto rozměry byly zvoleny s ohledem na vnitřní prostor sloupu veřejného osvětlení a na velikosti komunikační modulu a ostatního použitého hardwaru. Samotný kryt se skládá ze dvou částí, které se do sebe zasunou, kde finální podoba výrobku je vidět na Obr. 18.

Všechny stěny, kromě zadní strany druhé části krytu, jsou široké 5 mm. Díky tomu nám uvnitř zbývá 20 mm na šířku. Přední strana krytu (tmavě šedá), obsahuje slot pro zasazení komunikačního modulu, kde kontakty na druhé straně modulu jsou plně přístupné z vnitřní strany. Výřezy pro zasunutí modulu jsou široké 1 mm, tloušťka modulu je 0,5 mm, takže je zde stejně velká vůle. Vůle byla zvolena vyšší z důvodu tolerancí, se kterými je potřebné počítat při 3D tisku (poměr kvalita tisku / cena za kus). Přední část ještě obsahuje otvory pro přívod kabeláže (silnoproudé vodiče, přívody světelného senzoru). Posledním prvkem předního dílu je 2 mm vykrojení, které je zrcadleno na zadním, pro bezpečné zasunutí obou částí do sebe. U této části nebyla záměrně zvolena žádná vůle z důvodu zpevnění konstrukce při sestavení. Zadní díl (světle šedý), kromě ližin pro spojení obou částí, ještě obsahuje připojení na DIN lištu (DIN EN 50022), která má šířku 35 mm (tento druh lišty se používá v praxi pro uchycení elektrické výzbroje ve sloupech veřejného osvětlení). Uzpůsobení pro připojení na lištu je vidět na Obr. 19, kde je zobrazena část pohledu z boku a na zadní stranu, v obrázku jsou také zvýrazněny vnitřní hrany zadního dílu.



Obr. 18 Ochraný kryt



Obr. 19 Zadní strana ochranného krytu

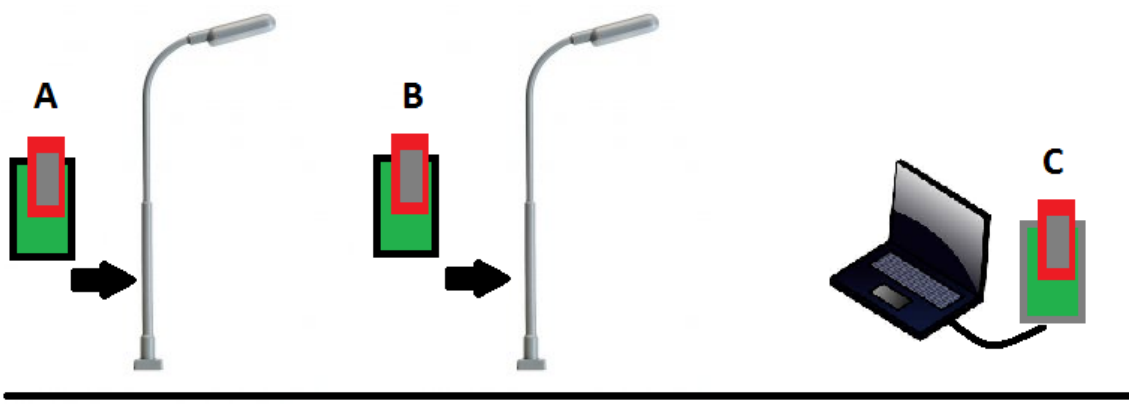
Z běžných materiálů používaných pro 3D tisk je nejvhodnější ABS (Acrylonitrile butadiene styrene), který se běžně používá pro ochranné obaly elektrických zařízení. Jedná se o plastový materiál vyráběný z ropy, který je oproti ostatním materiálům stálejší za vyšších teplot a začíná se deformovat až při teplotách kolem 100 °C (např.: materiál PLA se může začít deformovat již při teplotách překračujících 60 °C). Další výhodou tohoto materiálu je jeho cena v surovém stavu, na druhou stranu má nevýhodu složitějšího tisku, kdy je potřeba vyšších teplot při tisku a delší doby pro vychladnutí výrobku, což negativně ovlivňuje cenu výsledného výtisku.

Největší nevýhodou tohoto řešení je cena při výrobě malého množství kusů, v současné době totiž ještě 3D tisk není dostatečně levný. V takovýchto případech je lepší (levnější) využít již existujících obalů pro elektroniku.

7 Měření parametrů vysílače při umístění v dříku sloupu

Jedním z cílů této práce je také prozkoumat možnost uložení komunikačního modulu do dříku sloupu veřejného osvětlení. Většina řešení, které jsou v současné době na trhu, využívá umístění komunikačního modulu k osvětlovacímu tělesu. Toto zapojení má svoje výhody a nevýhody. Největší nevýhodou zde je umístění komunikačních modulů ve špatně dosažitelné oblasti (několik metrů nad zemí). Na druhou stranu zde nenastává problém s odstíněním signálu, protože komunikační moduly jsou umístěny v krytu světla, který tolik neutlumí signál. Z tohoto důvodu většinou komunikační moduly nemají problémy s dosahem a silou vysílaného signálu mezi jednotlivými stožáry. V případě umístění modulu do dříku je proto nutné počítat s rušením od elektrické výzbroje umístěné ve dříku, a také s odstíněním způsobeným stěnami dříku, které jsou většinou z hliníku, oceli nebo litiny.

Pro samotné měření byl využit vývojářský kit DS-START-04, kde do každého komunikačního modulu byl nahrán jednoduchý program, pro základní otestování komunikace dvou modulů umístěných v dříku sloupu. S pomocí Obr. 20, bude popsána funkce kódů nahraných do jednotlivých modulů, kde celé zdrojové kódy jsou k nalezení v příloze.



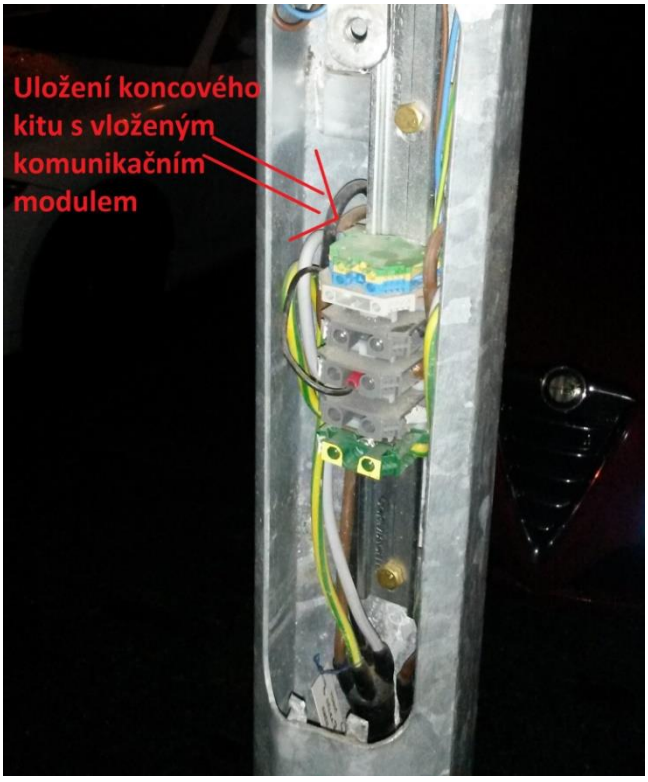
Obr. 20 Měřící pracoviště

Kód nahraný do modulu A (označení modulů podle Obr. 20) zajišťuje periodické vysílání zpráv z modulu, všem možným příjemcům, což teoreticky by mělo znamenat, že vysílaná zprávy bude přijata moduly B a C. Periodické zasílání je zajištěno nastavením čekání a while cyklu, který po skončení čekací periody odešle zprávu s identifikátorem modulu A. Modul B je nastaven na příjem zpráv, kdy po přijetí zprávy od modulu A, vyšle zprávu s vlastním identifikátorem. Modul C, který je připojen k počítači, má za úkol přijímat všechny IQRF zprávy na určeném kanálu a frekvenci (všechny moduly mají

nastaveny stejné parametry). Tyto zprávy se poté vypíšou v programovém prostředí IQRF IDE v Terminal logu. V síti není zapnuté žádné směrování, aby bylo zamezeno falešným výsledkům, kdy modul C by zachytil zprávu od modulu A, kterou by poté směroval na modul B, od kterého by poté přijal další zprávu. V takovémto případě by výsledky nebyly korektní, protože by bylo ověřeno pouze, že vysílaný signál je dostatečně silný, aby z vnitra dříku sloupu dosáhl k modulu C, který se nachází ve volném prostoru, ale nebylo by ověřeno, jestli možná přímá komunikace mezi moduly A a B, kde oba jsou odstíněny stěnami dříku sloupu. Další z výhod této konfigurace je možnost přesunou jeden z modulu A nebo B do jiného vzdálenějšího sloupu veřejného osvětlení, bez toho aby bylo řešeno, který modul se přenáší.

Podmínky 1. měření:

- Vysílací frekvence: 868 MHz
- TX Power: 7 (maximální vysílací výkon IQRF modulů odpovídající 11 dBm)
- Vzdálenost mezi sloupy: 20 m
- Materiál stěny dříku sloupu: Ocel 11353
- Tloušťka stěny dříku sloupu: 4 mm
- Kompletní elektrická výzbroj; umístěná ve dříku sloupu (Obr. 21)
- Venkovní teplota: okolo +5 ^{o}C
- Uložení komunikačního modulu dle Obr. 20.



Obr. 21 Dřík sloupu požitý v 1. měření

Podmínky 2. měření:

- Vysílací frekvence: 868 MHz
- TX Power: 7 (maximální vysílací výkon IQRF modulů odpovídající 11 dBm)
- Vzdálenost mezi sloupy: 25 m
- Materiál stěny patice sloupu: Beton
- Tloušťka stěny patice sloupu: 25 mm
- Kompletní elektrická výzbroj; umístěná v patici sloupu (Obr. 22)
- Venkovní teplota: okolo -5 °C

Obr. 22 Patice sloupu použitá ve 2. měření

7.1 Výsledek měření

Při prvním měření za popsaných podmínek bylo zjištěno, že se neoperuje s dostatečně silným vysílacím výkonem. Při uložení obou modulů do dříků sloupu neproběhla žádná komunikace mezi moduly A a B. Jediná komunikace, která v tomto rozložení proběhla, byla komunikace mezi moduly A a C na vzdálenost maximálně 5 m. Pro docílení zamýšlené komunikace, bylo potřebné vyjmout jeden z modulů ven ze

sloupu a přiblížit se na vzdálenost alespoň 5 m ke druhému sloupu, aby byly zachytávány zprávy od obou modulů (A, B). Přijímané zprávy, ať už pouze od modulu A nebo od modulů A a B, přicházely pravidelně v určených intervalech a bez chyb. Přestože se jedná o krátké a jednoduché zprávy, lze ze zatím zjištěných skutečností usoudit, že hlavní příčinou nefunkční komunikace mezi moduly A B, bylo utlumení signálu způsobené průchodem přes ocelové stěny sloupu.

Ve druhém měření, které proběhlo za drasticky jiných podmínek, byla pozorována správná funkčnost připraveného testovacího programu. Toto nastalo i přesto, že měření proběhlo na vetší vzdálenost a při větší tloušťce stěny sloupu (dříku / patice). Hlavním důvodem, proč vše fungovalo, je to, že pro konstrukci patice sloupu byl použit beton. Beton na rozdíl od ocele (kovu) neodstíní signál do takové míry, aby přenos nebyl možný na určenou vzdálenost. Při tomto měření byl také otestován přenos zpráv na vzdálenost 50 m (ob jeden sloup). V tomto případě komunikace stále probíhala, ale již se začaly ztrácet zprávy od modulu B. Na obrázcích 23 (měření na 25 m) a 24 (měření na 50 m) je vidět výpis z Terminal Logu programu IQRF IDE, kde je tato skutečnost zdokumentována (na Obr. 23 by po zprávě 172 a 173, která je od modulu A měla následovat zpráva od modulu B).

240	14:46:52.151	Rx	4	1000	31.30.30.30.
241	14:46:52.411	Rx	1	0	30.
242	14:46:54.911	Rx	4	1000	31.30.30.30.
243	14:46:55.171	Rx	1	0	30.
244	14:46:57.671	Rx	4	1000	31.30.30.30.
245	14:46:57.931	Rx	1	0	30.
246	14:47:00.441	Rx	4	1000	31.30.30.30.

Obr. 23 Výpis z IQRF IDE – měření na 25 m

170	14:44:31.283	Rx	4	1000	31.30.30.30.
171	14:44:31.543	Rx	1	0	30.
172	14:44:34.043	Rx	4	1000	31.30.30.30.
173	14:44:36.803	Rx	4	1000	31.30.30.30.
174	14:44:39.573	Rx	4	1000	31.30.30.30.
175	14:44:39.833	Rx	1	0	30.
176	14:44:42.333	Rx	4	1000	31.30.30.30.

Obr. 24 Výpis z IQRF IDE – měření na 50 m

Měření na 50 m proběhlo hlavně z důvodu využití protokolu IQMESH ve finální aplikaci. Protože při zapnutém směrování v síti je možné, aby síť stále fungoval i při výpadku

jednoho z modulů, a proto je nutné otestovat kvalitu přenosu i na vyšší vzdálenost (alespoň ob jeden sloup).

7.2 Důsledky výsledku měření

Jelikož Druhé měření provedeno na starších sloupech veřejného osvětlení ještě využívajícího konstrukce s betonovou paticí, které se v praxi téměř do nových projektů nenasazuje, je nutné spíše pracovat s výsledky prvního měření. Z výsledků prvního měření (a částečně i z druhého) se došlo k závěru, že nelze provést realizaci zapojení v původním navrhovaném stavu, a je zapotřebí upravit zapojení.

Existují dva hlavní způsoby na odstranění problému. Prvním je instalace přídavné antény. Pro IQRF existuje druhů několik antén od výrobce. Nejpravděpodobněji by bylo vhodné zvolit anténu v provedení AN-D01-U.FL, kde se jedná o PCB anténu s kabelem o délce 1 m. Tato anténa (AN-D01) se však dá pořídit samostatně, v tom případě by ale bylo nutné, řešit přizpůsobení přívodního kabelu k anténě. Alternativně, při použití jiné z cenově dostupných antén by mohl nastat problém s místem uvnitř sloupu. Další z nevýhod je nutnost přizpůsobení sloupu pro umístění antény. Pro omezení rušení by bylo vhodné anténu umístit do výšky kolem 2 - 3 m. V takovéto konfiguraci je také stále nutné počítat s možností dalšího stínění v případech, kdy do prostoru mezi lampy například zaparkuje osobní automobil. Toto řešení představuje nové problémy pro původní návrh, kdy hlavní výhodou zkoumaného konceptu byla jednoduchost instalace a manipulace se součástmi zapojení.

Druhou možností řešení problémy je využití již v praxi implementovaného konceptu umístění komunikačních modulů k osvětlovacímu tělesu. Velkou nevýhodou tohoto řešení je omezený přístup k zařízení. Výška stožárů veřejného osvětlení se pohybuje v rozmezí 4–6 m pro parkové osvětlení, 8–12 m pro uliční a kolem 14 metrů pro dálniční osvětlení. Z těchto hodnot je patrné, že pro přístup i k nejmenším sloupům veřejného osvětlení by bylo potřebné vyzdvihovací plošiny. Jakýkoliv zásah do takovéhoto zařízení vyžaduje vyšších nákladů, ať už se jedná o diagnostiku problému nebo jeho odstranění. Další z úskalí, se kterým je potřeba počítat je možnost rušení, které bude způsobené osvětlovacím tělesem, ať už se jedná o sodíkovou výbojku, LED světlo nebo jiné.

8 Finanční analýza řešení

Jedním z důležitých aspektů implementace popsaného řešení systému veřejného osvětlení je jeho finanční přínos. Na finanční přínos tohoto řešení je potřebné nahlížet z dlouhodobého hlediska. Z tohoto důvodu v této kapitole bude popsán zjednodušený finanční náhled na tuto problematiku.

Jelikož popsané řešení se dá implementovat jak do stávajících systémů veřejného osvětlení, tak do nových výstaveb, je potřebné se zaměřit v hlavní míře na cenu hardwaru, který je nutný pro úpravu. Pro každé zapojení je potřebný IQRF modul, DALI předřadník, zdroj pro DALI sběrnici, napájecí zdroj pro měnič napětí a další součástky jako například tranzistor a odpory, které jsou o několik řádů levnější než zbytek. V tabulce 1 je vidět rozpis cen jednotlivých vyjmenovaných součástí zapojení.

Tabulka 1:

součástka	model	cena / kus	reference	pozn.
		Kč/kus		
Komunikační modul	TR-72DA	323,00	[32]	
Předřadník	proLED25	1198,00	[31]	
Zdroj sběrnice	DALIpwr	2783,00	[31]	(a)
Zdroj pro měnič	DIN15W12	279,00	[33]	

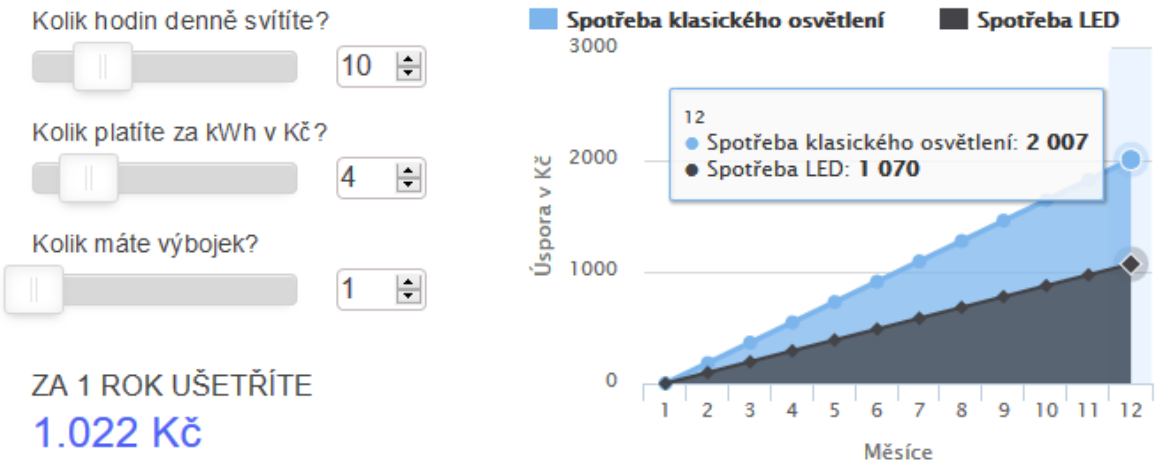
Pozn. (a): Většina zdrojů pro DALI sběrnice, které jsou na trhu k mání je koncipována pro napájení sběrnic, ke kterým bude připojeno větší množství předřadníků. Z tohoto důvodu jsou tyto zdroje relativně drahé v porovnání s předřadníkem nebo podobnými zařízeními. Lze realizovat i zdroje, které budou určeny pro takovéto aplikace [34]. Takto koncipované zdroje by poté byly mnohem levnější. Stále se však musí být v souladu s normou IEC 62386.

Celková cena za tyto čtyři součástky tedy činní 4 583 Kč. K této ceně je ještě nutné připočíst částku, kterou by stály další levnější součástky. Pro účely tohoto finančního přiblížení zvolíme tuto částku 20 % (916 Kč) z předchozí hodnoty (tato částka také zahrnuje část nákladů za různé jednorázové náklady, jako je například pořízení brány do internetu). Nesmí se také zapomenout na cenu za implementace (zaplacení techniků, programátorů apod.), opět tuto částku zvolíme jako 20 % (916 Kč) původní hodnoty. Po těchto úpravách se dostaneme na částku 6 416,20 Kč. Pro zjednodušení dalších propočtů toto číslo zaokrouhlíme na 6500 Kč.

Pro uvedení této částky do perspektivy, bude tento odstavec věnován rozboru ceny nově postaveného sloupu veřejného osvětlení. V praxi je možné se setkat s velkým množstvím druhů sloupů veřejného osvětlení, které se mohou lišit výškou, konstrukcí,

materiálem a designem. Stejně tak to platí i u osvětlovacích těles, kde největším rozdílem je typ. Nejčastěji se setkáme s výbojkovým světlem nebo LED světlem, které je dražší. Podle těchto parametru se jednotlivé finálně sestavené sloupy mohou značně lišit ve svých nákladech na výstavbu. Velkým cenovým rozdílem v závislosti na druhu sloupu (hlavně jeho výšce), je způsob jeho ukotvení do země. Z těchto skutečností není možné generalizovat cenu jednoho sloupu, samotné sloupy podle typu mohou stát od 3 500 až do 10 000 Kč. Světla se poté značně liší podle typu: výbojky od 2 000 do 4000 Kč, LED od 4 500 do 8 500 Kč, světla s regulovatelnými LED od 10 000 do 14 000 Kč. Jelikož se jedná, o velké rozdíly bude využito příkladu z praxe. Samostatný 8 m vysoký stožár, od firmy Amako [35], v provedení JB 10 L stojí kolem 7 000 Kč, k němu cena světla (s regulovatelnými LED) TVO40S-W provedení COBRA 80 W [36] se pohybuje okolo 12 400 Kč. Jedná se o běžně používané součásti, se kterými se lze běžně setkat v praxi. Celkově se pak cena pro vztyčení a zapojení jednoho sloupu pohybuje okolo 25 000 Kč, kde v této částce jsou započítány také zemní práce a mzda pro zaměstnance. Z tohoto porovnání je vidět, cena úpravy pro využití služeb IoT naroste v řádu desítek procent (okolo 20 % pro součásti uvedené v této práci). Další odstavec tedy bude věnován rozboru, ve kterém se pokusí zjistit, za jak dlouho by se částka potřebná na úpravu zaplatila přes úsporu na spotřebu elektrické energie.

Internetový dodavatel LED svítidel ledsviti.cz, který má ve své nabídce také LED světlo se stejným výkonem [37], má na svých internetových stránkách interaktivní graf porovnání nákladů světla s takovýmto výkonem a odpovídající sodíkové výbojky (150 W), viz Obr. 25.



Obr. 25 Porovnání úspor mezi 80 W LED světlem a odpovídající výbojkou (150 W), převzato z [37]

Z tohoto grafu je vidět že při zadaných parametrech samotné LED světlo zaplatí za necelých 12 let. Podle výsledků z praxe [21] se při regulaci LED světla dosáhne další úspory za energie ve výši 40 %, což v našem případě činí roční úsporu dalších 400 Kč.

Zapojení realizované v této práci by se tedy zaplatilo v průběhu 16 let a 3 měsíců (při úpravě LED světla). Pokud bychom ale brali v potaz celkový rozdíl mezi 150 W sodíkovou výbojkou a LED světlem s implementovaným řízením přes IoT, dostáváme se k tomu, že by se modernizace zaplatila v průběhu 13 a půl roku.

Z tohoto rozboru je vidět, že finanční návratnost investice je již jen při zahrnutí úspory na energiích vcelku dobrá. Musíme také ale počítat s dalšími úsporami, které se ale nedají jednoduše vyčíslit. Ať už se jedná o zkvalitnění služeb veřejného osvětlení, úspory za správu veřejného osvětlení nebo také ekologický přínos spojený s nižší spotřebou energií. Dalším významným faktorem, který zde bude hrát roli je stav vývoje cen LED světel a energií. S dalším poklesem cen LED světel a zdražením energií se přechod na modernější technologie stává ještě výhodnějším. Svou roli také hraje fakt, že ceny uvedené v tomto rozboru jsou internetové ceny, které jsou vyšší, než s čím se můžeme setkat v praxi (množstevní slevy, odečet DPH, věrnostní slevy mezi společnostmi atd.).

9 Závěr

Teoretická část této diplomová práce je zaměřena na průzkum technologií, které spadají pod jednotný název Internet věcí. Hlavní oblastí pak jsou takzvané low-power WAN technologie, které se vyznačují nízkou spotřebou a schopností přenášet informace na vzdálenosti vyšší než několik stovek metrů. Mezi hlavní zástupce takovýchto technologií patří SigFox, LoRa a IQRF, se kterou byla realizována praktická část této práce.

Při realizaci teoretické části jsem dospěl ke dvěma hlavním zjištěním o Internetu věcí. U obou těchto problémů je hlavním důvodem jejich existence fakt, že zařízení využívající principů Internet věcí jsou stále ještě v počátcích svého rozšíření mezi koncové uživatele. Prvním z těchto problémů je neexistence jednotných standardů, kdy velké množství organizací usiluje o prosazení svých standardů do praxe. Druhým velkým problémem v Internetu věcí, je nedostatečná úroveň zabezpečení napříč různými zařízeními. Některé v současné době nabízené zařízení na trhu nesplňují ani minimální bezpečnostní standarty. Z tohoto důvodu probíhá velké množství kybernetických útoků zaměřených na takováto zařízení, ať už se jedná o útoky na zařízení vlastněná jednotlivcem nebo na celé sítě. Největším úskalím zde je možné zneužití zařízení pro další možné útoky na klasické počítačové sítě. Oba popsané problémy kopírují stav z doby rozvoje klasického internetu, největším rozdílem je však úroveň znalostí odborné veřejnosti. Nízká úroveň bezpečnosti je velkým problémem v současné době, kdy rychlost jejího rozvoje bohužel nekopíruje rychlost rozšiřování zařízení Internetu věcí na trh.

V praktické části práce jsem se zabýval konstrukcí jednoduchého systému na ovládání sloupu veřejného osvětlení, s využitím hardwaru a softwaru technologií IQRF a DALI. Největším úskalím realizace toho úkolu bylo naprogramování a zapojení IQRF modulu tak aby byl schopen generovat signály přenášející data pro DALI předřadník, podle příslušných norem. Generování signálu bylo vyřešeno použitím čekání, které generuje PIC, na kterém je IQRF modul postaven. Pomocí tohoto časování se měnila hodnota výstupního pinu na IQRF modulu v závislosti na vysílané zprávě. Na výstupu IQRF modulu je maximálně možné mít +3 V, kdy pro potřeby IQRF je nutné mít alespoň + 9,5 V. Pro přechod mezi těmito úrovněmi bylo navrženo zapojení tranzistoru ve spínacím režimu. Výstup z tohoto tranzistoru vede na DALI sběrnici, ke které je připojen DALI světelný předřadník, který ovládá regulovatelný LED pásek.

Součástí této práce také byl návrh několika modelových situací, kde by bylo možné takto vytvoření zapojení použít. Nejpodrobnější z těchto návrhů byla představena situace implementace zapojení ve sportovním areálu. V této ukázce jsou představeny jednotlivé IoT služby, které by se dali v takovémto prostředí nabízet. V neposlední řadě tato ukázka také popisuje jednotlivé úkony, které je potřeba provést pro bezproblémovou implantaci tohoto řešení.

Z důvodu velkého zájmu společností o tuto problematik jsem se také zabýval dalšími úskalími tohoto problému. Většina komerčních řešení ovládání veřejného osvětlení pracuje s myšlenkou umístění komunikačních modulů do krytu osvětlovacího tělesa. Velkou nevýhodou tohoto řešení je ztížený přístup do této části sloupu a většinou je zapotřebí využít montážní plošinu pro jakoukoliv manipulaci se zařízením. Druhou možností je uložení komunikačního modulu do dříku sloupu, kde je k němu jednoduchý přístup. Výsledek dvou měření v takovéto konfiguraci však ukázal, že stěny dříku sloupu utlumí signál do takové míry, že přenos na potřebnou vzdálenost není možný. Jedním, z možných řešení tohoto problému je připojení externí antény ke komunikačnímu modulu.

Poslední částí celé práce byla zjednodušená finanční analýza, při níž bylo zjištěno, přechod ze světla se sodíkovou výbojkou na regulovatelné LED světlo se sám zaplatí za 13,5 roku. S tím že vybraný druh světla je má průměrnou životnost okolo 14 let při 10 hodinách svícení denně. Tato skutečnost dokazuje, že pouze při uvážení cen energií, tak je tato investice výhodná. Jak bylo ale zmíněno na konci kapitoly 8 celková návratnost je vyšší, ale nedá se takto předem propočítat.

10 Literatura

[1] iot-portal. Definice IoT. [online]. 8.8.2016 [cit. 2016-08-08]. Dostupné z: http://www.iot-portal.cz/

[2] Gartner. Růst IoT. [online]. 10.7.2016 Dostupné z: http://www.gartner.com/newsroom/id/3165317

[3] The best smart home hub. BGR. [online]. 28.8.2016 [cit. 2017-01-02]. Dostupné z: http://bgr.com/2016/10/28/best-smart-home-hub-2016-amazon-alexa-echo/

[4] The only Coke machine on the internet. Carnegie Mellon University. [online]. [cit. 2017-01-02]. Dostupné z: https://www.cs.cmu.edu/~coke/history_long.txt

[5] Český telekomunikační úřad. Všeobecné oprávnění č. VO-R/10/05.2014-3 k využívání rádiových kmitočtů a k provozování zařízení krátkého dosahu. 24.8.2016 Dostupné z: https://www.ctu.cz/cs/download/oop/rok_2014/vo-r_10-05_2014-03.pdf

[6] About Us. Microrisc. [online]. [cit. 2017-01-02]. Dostupné z: http://www.microrisc.com/en/about-us

[7] Anthennas. IQRF. [online]. [cit. 2017-01-02]. Dostupné z: http://www.iqrf.org/products/accessories/antennas

[8] Security. IQRF Alliance. [online]. 25.5.2016 [cit. 2017-01-02]. Dostupné z: http://www.iqrfalliance.org/data_files/news/iqrf-security.pdf

[9] Prihlaseni. IQRF Cloud. [online]. [cit. 2017-01-02]. Dostupné z: https://cloud.iqrf.org/en/prihlasit/

[10] IQRF Cloud. IQRF. [online]. [cit. 2017-01-02]. Dostupné z: http://iqrf.org/technology/iqrf-cloud

[11] Datasheet: F8L10D [online]. 2017 [cit. 2017-05-22]. Dostupné z: http://en.four-faith.com/uploadfile/2017/0329/20170329090616378.pdf

[12] LoRa FAX. SEMTECH. [online]. [cit. 2017-01-02]. Dostupné z: http://www.semtech.com/wireless-rf/lora/LoRa-FAQs.pdf

[13] Datasheet: ATA8520 [online]. 2015 [cit. 2017-05-22]. Dostupné z: http://www.atmel.com/Images/Atmel-9372-Smart-RF-ATA8520_Datasheet.pdf

[14] SigFox coverage. SigFox. [online]. [cit. 2017-01-02]. Dostupné z: http://www.sigfox.com/en/coverage

[15] IoT Research Paper. Bitdefender. [online]. 1.2.2016 [cit. 2017-01-02]. Dostupné z: http://download.bitdefender.com/resources/files/News/CaseStudies/study/87/Bitdefender-2016-IoT-A4-en-EN-web.pdf

[16] IoT whitepaper. Veracode. [online]. [cit. 2017-01-02]. Dostupné z: https://www.veracode.com/sites/default/files/Resources/Whitepapers/internet-of-things-whitepaper.pdf

[17] Mallware Mirai. Motherboard. [online]. 11.8.2016 [cit. 2017-01-02]. Dostupné z: http://motherboard.vice.com/read/internet-of-things-mirai-malware-reached-almost-all-countries-on-earth

[18] Insecurity in IoT. Symantec. [online]. 12.5.2015 [cit. 2017-01-02]. Dostupné z: https://www.symantec.com/content/dam/symantec/docs/white-papers/insecurity-in-the-internet-of-things-en.pdf

[19] Popis lampy veřejného osvětlení. In: Kooperativa [online]. [cit. 2017-05-22]. Dostupné z: http://www.kooperativa-vod.cz/ocelove-stozary/obecny-popis-stozaru/

[20] IEC 62386. Digital addressable lighting interface. 2. IEC, 2014.

[21] Smart cities [online]. 23.3.2016 [cit. 2017-05-22]. Dostupné z: http://www.proelektrotechniky.cz/osvetleni/51.php

[22] Chytré lampy PRE [online].18.2 2016 [cit. 2017-05-22]. Dostupné z: http://www.odbornecasopisy.cz/svetlo/aktualita/chytre-lampy-pre-potvrdily-zhorsenou-smogovou-situaci-v-praze--2274

[23] Smart city Wipperfürth [online]. 31.1.2016 [cit. 2017-05-22]. Dostupné z: http://www.proelektrotechniky.cz/osvetleni/58.php

[24] TR-72D datasheet. IQRF. [online]. [cit. 2017-01-02]. Dostupné z: http://www.iqrf.org/support/download&kat=37&ids=337

[25] IQRF IDE. IQRF. [online]. [cit. 2017-01-02]. Dostupné z: http://iqrf.org/technology/iqrf-ide

[26] IQRF OS Ref. Guide. IQRF. [online]. 21.7.2016 [cit. 2017-01-02]. Dostupné z: http://www.iqrf.org/support/download&kat=35&ids=156

[27] BPW34 datasheet. ECOM. [online]. 12.3.2012 [cit. 2017-01-02]. Dostupné z: https://www.ecom.cz/open_sheet/sheet_name=D28599

[28] IQRF Development tools. IQRF. [online]. [cit. 2017-01-02]. Dostupné z: http://www.iqrf.org/products/development-tools

[29] PIC16F877 Timer Modules tutorials: Timer2 [online]. [cit. 2017-05-22]. Dostupné z: http://www.microcontrollerboard.com/pic-timer2-tutorial.html

[30] Datasheet: BSY34 [online]. [cit. 2017-05-22]. Dostupné z: http://teslakatalog.cz/io0/210.gif

[31] Foxtron [online]. [cit. 2017-05-22]. Dostupné z: http://www.foxtron.cz/cz

[32] Transceiver TR-72DA. IQRF. [online]. [cit. 2017-01-02]. Dostupné z: http://iqrf.org/products/transceivers/tr-72d

[33] Zdroj pro měnič napětí: 15 W, 12V DC [online]. [cit. 2017-05-22]. Dostupné z: https://www.smdledzarovky.cz/napajeci.zdroje.led/napajeci.zdroj.na.din.listu.15w.12v.dc.125a?utm_source=seznam&utm_medium=cpc&utm_campaign=Dynamick%C3%BD+remarketing&utm_content=PremiumLED+Nap%C3%A1jec%C3%AD+zdroj+na+DIN+li%C5%A1tu+15W+12V+DC+1,25A&utm_term=

[34] Levnější zdroje DALI konzultace se zástupcem firmy Foxtron

[35] Stožár bezpaticový. Amako. [online]. [cit. 2017-01-02]. Dostupné z: http://www.amako.cz/produkty/stozar-bezpaticovy-tristupnovy-silnicni-typ-jb

[36] Regulovatelné LED světlo cobra: Katalog LED osvětlení [online]. 2017 [cit. 2017-05-22]. Dostupné z: http://www.ledprogram.cz/uploads/download/LED-Program-2017-I.pdf

[37] Graf spotřeby [online]. 2017 [cit. 2017-05-22]. Dostupné z: https://www.ledsviti.cz/led-verejne-osvetleni-80w-5000k/

11 Seznam obrázků

12 Seznam zkratek

Zkratka	Anglický název	Český ekvivalent
ABS	Acrylonitrile Butadiene Styrene	Akrylonitrilbutadienstyren
ADR	Adaptive Datarate Algorytm	Algoritmus adaptivní rychlosti přenosu dat
AES	Advanced Encryption Standard	Standard pokročilého šifrování
CRC	Cyclic Redundancy Check	Cyklický redundantní součet
DALI	Digital Addressable Lighting Interface	Digitální adresovatelné světelné rozhraní
DBPSK	Differential Binary Phase-Shift Keying	Diferenciální binární fázově klíčovaný posuv
DoS	Denial of Service	Odepření služby
EEPROM	Electrically Erasable Programmable Read-Only Memory	Elektronicky vymazatelná paměť pouze pro čtení
GFSK	Gaussian Frequency Shift Keying	Gaussovské klíčování frekvenčním posuvem
GSM	Global System for Mobile communications	Globální systém pro mobilní komunikaci
GUI	Graphical User Interface	Grafické uživatelské rozhraní
IDE	Integrated Development Environment	Vývojové prostředí
IoT	Internet of Things	Internet věcí
ITU	International Telecommunication Union	Mezinárodní telekomunikační unie
ISM	Industrial, Scientific and Medical	Průmyslové, vědecké a zdravotnické (pásmo)
I/O	Input/Output	Vstupně výstupní
LDO	Low-Dropout	Low-Dropout
LED	Light-Emitting Diode	Dioda emitující světlo
LPWAN	Low-Power Wide Area Network	Nízko výkonová rozsáhlá síť
MAC	Media Access Control address	Fyzická adresa
M2M	Machine-to-Machine	Rozhraní Stroj-Stroj
PIC	Peripheral Interface Controller	Mikrokontroler PIC
PHP	Hypertext Preprocessor	Hypertextový preprocesor
PLA	Polylactide acid	Polymléčná kyselina
p2p	peer-to-peer	Rozhraní Klient-Klient
RFID	Radio-Frequency IDentification	Identifikace na rádiové frekvenci
SPI	Serial Peripheral Interface	Sériové periferijní rozhraní
USB	Universal Serial Bus	Universální sériová sběrnice
WAN	Wide Area Network	Rozsáhlá síť
WEP	Wired Equivalent Privacy	Soukromí ekvivalentní drátovým sítím
WPA2-PSK	Wi-Fi Protected Access 2 – pre-shared Key	Chráněný přístup k Wi-Fi 2 s přesídleným heslem

13 Přílohy

Zdrojový kód pro měření – modul A

```
// ******************************************************************************
// Zdrojový kód pro testovací modul A - periodicky odesílá zprávy v intervalu 2,5
#include "D:\Plocha\DP_proj\Development\include\IQRF_OS\template-basic.h"
// ******************************************************************************

void APPLICATION()
{

appInfo();
copyBufferINFO2RF();

while (1)        // nekonečný cyklus
{
        startLongDelay(250);    //              2,5s delay
        PIN = 0;
        DLEN = 4;
        RFTXpacket();           //    Odeslání testovací zprávy
        waitDelay(25);          //    and wait 250ms (25*10ms)
}
}
// ******************************************************************************
#pragma packedCdataStrings 0
#pragma cdata[__EEAPPINFO] =  "1000"
```

Zdrojový kód pro měření – modul B

```
// ******************************************************************************
// Zdrojový kód pro testovací modul B - Po přijetí zprávy od modulu A odešle testovací zprávu
#include "D:\Plocha\DP_proj\Development\include\IQRF_OS\template-basic.h"
#define RX_FILTER                       0
// ******************************************************************************

void APPLICATION()
{
enableSPI();
setRFmode(_WPE | _RX_STD | _TX_STD);
toutRF = 1;

while (1)
```

```
{
        if (RFRXpacket())          // Kontrola přijetí zprávy
        {
                waitDelay(25);
                bufferRF[0]=0x30;                  // Obsah zprávy – Identifikátor
                PIN = 0;
                DLEN = 1;
                RFTXpacket();              //     Odeslání zprávy
                waitDelay(25);
        }
}
}
```

Zdrojový kód pro měření – modul C

```
// *************************************************************************
// Zdrojový kód pro testovací modul C - Přijímání zpráv a jejich výpis
#include "D:\Plocha\DP_proj\Development\include\IQRF_OS\template-basic.h"
// *************************************************************************

void APPLICATION()
{
enableSPI();                // Enable SPI

while (1)
{
        if (RFRXpacket())          // Kontrola přijetí zprávy
        {
                copyBufferRF2COM();
                startSPI(DLEN);
        }
}
}
```