ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta elektrotechnická

Katedra telekomunikační techniky

Inteligentní řízení veřejného osvětlení v koncepci IoT

Leden 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: 9. 1. 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 vlastní minimální spotřebě. V praktické části je popsán způsob realizace jednoduchého ovládání sítě veřejného osvětlení s možností umístění komunikačního modulu do dříku sloupu. Pro tuto konfiguraci byla provedena měření v reálném provozu. Poslední částí práce je finanční analýza tohoto řešení.

Klíčová slova: Internet věcí, IoT, IQRF, 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 placing it in pillar. For this configuration was realised measurement of parameters in running service. Last part of this thesis consist of financial analysis of this solution.

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

Obsah

1. 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 žárovky, která bude měnit svoji svítivost v závislosti na intenzitě okolního osvětlení, až po například pračku, posílající informace o stavu pracího cyklu do aplikace 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 mnoho technologií, díky kterým může zařízení poskytnout služby IoT, například: RFID, Bluetooth (low energy varianta), Zigbee, low power WAN a mnoho dalších. Výběr komunikačních technologií se řídí podle způsobu využití, ekonomické stránky, prostředí, v kterém bude technologie využívána, a jiných preferencí.

Existují dva základní způsoby, jak zrealizovat zařízení využívajícího Internetu věcí. Prvním případem jsou stávající zařízení, která původně nebyla zamýšlena pro Internet věcí. Zde 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 toho 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 = $2^{128} \approx 3x10^{38}$ 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].

1.1 Stručná historie Internetu věcí

Prvním zařízením, které komunikovalo s okolním světem prostřednictvím internetu, byl automat na colu, nacházející se na půdě Carneie Mellon Univerzity v Pittsburghu [4]. Již v roce 1982 toto zařízení bylo schopno oznamovat úroveň svých zásob a jejich stav. Až v roce 1991 byly principy Internetu věcí oprášeny, když vyšel vědecký článek zabývající se budoucností počítačových sítí v 21. století. Mezi lety 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 popularitě a v následnicích letech se články o něm začínají objevovat v publikacích pro širokou veřejnost jako např.: The Guardian, Boston Globe apod. V roce 2005 uveřejnilo ITU první report na téma IoT. Poté v roce 2008 proběhla první Evropská konference na téma Internetu věcí a od této doby opět nabývá celý koncept na popularitě. Posledním velkým milníkem pro internet věcí bylo uvedení protokolu IPv6 do provozu. Od této doby také nastává rychlý rozvoje technologií pro Internet věcí, který bude pokračovat do budoucna.

1.2 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). Co nejnižší spotřeby se snažíme dosáhnout, protože většina zařízení využívající LPWAN technologie využívá baterii jako zdroj energie. Jedním z důvodů, proč je možné docílit takto nízké spotřeby, je

skutečnost, že není potřeba, aby zařízení komunikovaly neustále. Většinu času je zařízení v režimu standby (spánku) a pouze v určitých časových intervalech, které se mohou značně lišit podle aplikace, vysílá data. Dat od zařízení je většinou malé množství, takže využívají se malé přenosové rychlosti 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 jsou 433-434 MHz a 863-870 MHz (ve světě se ještě využívá pásmo 902-928 MHz). Přestože ISM pásmo je volně k použití, musí se dodržovat jistá omezení podle 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.

1.3 IQRF

Obr. 1 IQRF logo

IQRF je první low-power WAN technologie, která bude představena. Tato technologie je vyvíjena českou společností Microrisc, sídlící v Jičíně [6], již od roku 2004. Jedná se o kompletní řešení pro Internet věcí zahrnující jak hardware a software tak i protokoly pro přenos a podpůrné služby.

IQRF pracuje s přenosovou rychlostí 20kb/s. Spotřeba energie 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)

Při odesílání dat se spotřeba pohybuje mezi 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 (nejsou překročeny hranice určené všeobecným oprávněním č. VO-R/10/05.2014-3) a v pásmu 433-434 MHz není překročena úroveň 10 mW (nejsou překročeny hranice

určené všeobecným oprávněním č. VO-R/10/05.2014-3). Hodnota vysílaného výkonu je softwarově nastavitelná v násobcích základní úrovně.

Systém je založený na principu komunikačních modulů s proprietárním operačním systémem, který v současné době je ve verzi 3.08D. Tyto moduly se programují s využitím programovacího jazyka C a s využitím definovaných příkazů v GUI. Dosah jednoho 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]. Druhým způsobem je zapojení do topologie, kdy se nezvyšuje dosah jednotlivých modulů, ale zvyšuje se efektivní plocha sítě, kde mezi dvěma koncovými zařízeními může 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 v sítí není žádný koordinační prvek a vysílané packety jsou určené všem ostatním modulům. V tomto nastavení může síť obsahovat neomezené množství zařízení, a vše se řídí programem od uživatele. Na rozdíl od p2p v MESH topologii nalezneme koordinátor a jsme omezeni počtem zařízení v síti. 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 fungovat jako koncový bod nebo jako router, pokud je to zapotřebí. Pokud by byl počet zařízení v síti nedostačující, existuje možnost škálování sítě pomocí nastavení cílových zařízení jako koordinátory pro sub-sítě. Sub-síť může také maximálně obsahovat 239 zařízení. Doporučuje se však vytvářet méně komplikované sítě z důvodu 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 na přenos packetu bez chyb (dílčí CRC a celkové CRC).

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

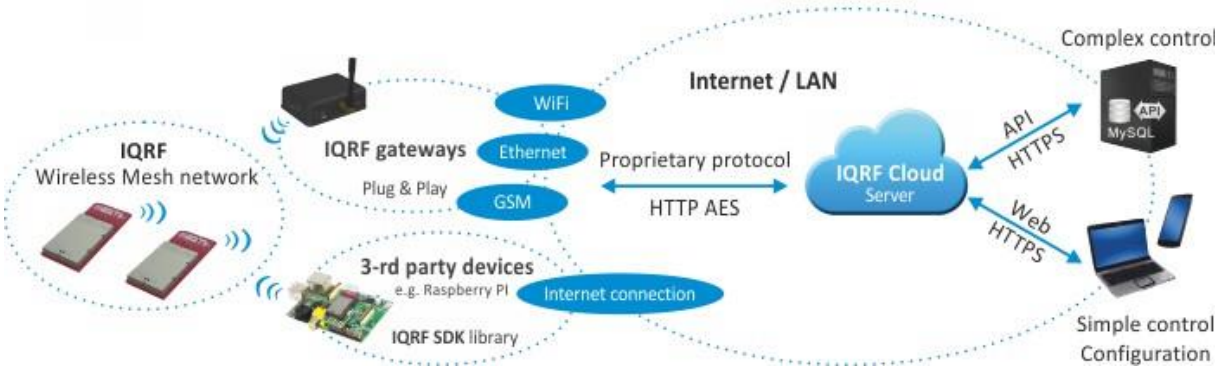
PIN	packet info
DLEN	data lenght
CRCH	header checksum
NTW INFO	networking info
CRCN	NTW INFO checksum
DATA	max 255B of users data (v IQRF OS 2.0 omezeno na 64B)
CRCD	data checksum
CRCS	Security checksum

IQRF moduly 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 také

jako testovací, servisní nástroj a je to také prostředí 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 automatická inicializace modulu v IQRF IDE), který je součástí vývojářského kitu. Mezi podporovaná zařízení ještě patří brány do internetu, které mají port rozhraní USB.

V otázce zabezpečení komunikace využívá technologie vrstev 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 stav jeho úrovně zabezpečení, které poskytuje. 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 od výrobce technologie. 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 také možné posílat příkazy k řízení koncových zařízení. Jediným potřebným hardwarem pro realizaci je brána pro přístup do internetu (Gateway). Další nezbytností je existující účet na stránkách cloudu [9], kde je možné, aby jeden účet spravoval vícero bran, ale také aby jedna brána byla přístupná z více účtů. Pro IQRF existuje množství bran ať už samostatných, které vlastní přístup do internetu realizují za pomocí technologií jako je Ethernet, Wi-fi nebo GSM, tak bran které se připojí do USB rozhraní. Instalace brány probíhá principem plug-and-play, kdy se celé nastavení brány provede přes IQRF IDE.



Obr. 2 IQRF cloud [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, nebo je možné data zanášet do databázových systémů. Na všechny tyto možnosti je cloudová aplikace uzpůsobena. 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 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. Přestože cloud je schopen držet pouze vcelku omezené množství přijatých zpráv, 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, poté je maximální počet záznamů limitován pouze velikostí úložného prostoru, vyhrazeného na logy.

1.4 LoRa

Obr. 3 LoRa logo

LoRa je druhou z představených LPWAN technologií. Na rozdíl od předchozí LPWAN technologie, LoRa je 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.

Jelikož existuje mnoho implementací technologie LoRa do hardwaru, je spotřeba modulů různá. Pro názornost bude uveden příklad modulu od společnosti Four Faith s označením F8L10D-N LoRa Module. 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 IQRF je přenosová rychlost. LoRa využívá změn rychlostí přenosu, pro docílení optimalizace spotřeby a zlepšení škálovatelnosti sítě. Rychlost přenosu se pohybuje mezi 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, zde 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 dorazily beze ztráty. Většina modulů je schopna vysílat s vyšším výkonem, než jsou stanoveny hranice pro vysílání podle všeobecného oprávnění č. VO-R/10/05.2014-3, proto je potřeba 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 žádných mezičlenů na vzdálenosti závisle podle implementace a prostředí, v zástavbě se však pohybujeme v řádu stovek metrů až jednotek kilometrů a jednotek kilometrů až v extrémních případech do 20 kilometrů ve volném prostoru. Maximální počet modulů, které mohou být připojeny k jedné gateway je závislosti 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), toto maximu se pohybuje okolo 1,5 milionů packetů za hodinu. 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 [11]. 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 na trhu 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 – Není otevřený kanál pro příjem zpráv pouze v okamžiku vysílání.

Zabezpečení v inicializace zařízení v síti a poté samotné komunikace je řešena pomocí užití unikátních klíčů a encrypce. Koncový bod si při inicializaci požádá o spárování za použití zprávy 128 b AppKey klíče. 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 jak na obou stranách komunikace (countery by se neměly nikdy opakovat).

1.5 SigFox

Obr. 4 SigFox logo

Technologie SigFox je vyvíjena Francouzskou společností stejného jména od roku 2009. SigFox se zaměřuje jak na hardware, tak software. Infrastruktura pro sítě s technologií SigFox je vlastněna společností SigFox, kde pro obchodní partnery je otevřena část trhu s koncovými zařízeními. SigFox se v tomto ohledu chce stát „celosvětovým operátorem“ pro sítě Internetu věcí.

Spotřeba energie bude opět demonstrována na příkladu koncového bodu. V tomto případe na zařízení Atmel ATA8520D:

- 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 s pokrytím sítě [12] a komunikační modul SigFox. Topologie použitá v síti je peer-to-peer, kdy výrobcem udávané vzdálenosti na, které jsou zařízení schopna 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 maximální velikost dat ve zprávě je 12 B. Celá síť se svým principem více podobá mobilním sítím než konkurenčním řešením sítí LPWAN technologií.

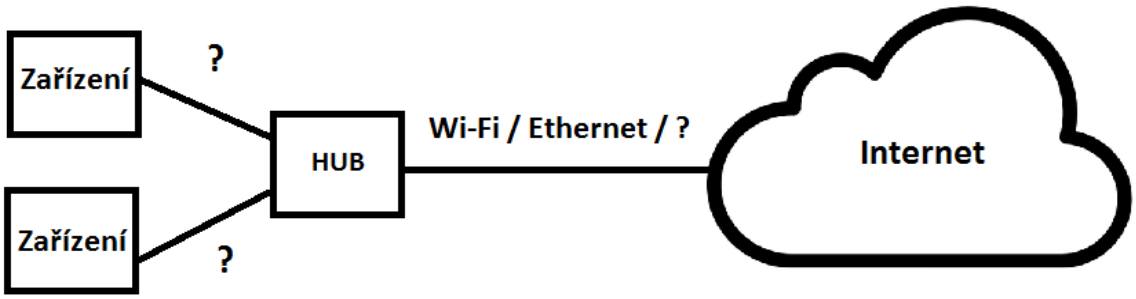
Stejně jako u technologie LoRa, způsob programování komunikačních modulů pro koncová zařízení se liší podle výrobce. V kontrastu k tomu infrastruktura je plně v péči společnosti SigFox a není dostupná zvenčí.

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 SigFox je způsob chodu koncových zařízení, většinu času tyto zařízení nevysílají a jsou v režimu spánku, takže je obtížné na ně útočit.

2 Bezpečnost v prostředí Internetu věcí

S masovým rozšířením Internetu věcí nastává otázka ohledně bezpečnosti v této oblasti. Jak již bylo zmíněno v kapitole 1.2 jedním z největších problému v této oblasti je neexistence standardů 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 pozměněný chod přístrojů povede k újmám na zdraví uživatele. Dalším problémem, který se zde vyskytuje je zabezpečení přístupu k datům.

V různých oblastech využití zařízení Internetu věcí jsou potřebné různé stupně zabezpečení proti odchytu a manipulaci s daty. 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 wi-fi. U systémů s centrálním prvkem existují různá řešení komunikace zařízení-hub a hub-internet, kde tyto řešení se budou lišit podle výrobce. Propojení zařízení-hub bude 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 Hub k internetu je méně, dva hlavní způsoby jsou přes wi-fi nebo ethernet 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 drahé 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 bylo zmíněno výše, protože sítě wi-fi jsou na trhu delší dobu je existuje větší skupina lidí, kteří se vyznají v slabých stránkách těchto sítí.



Obr. 5 Vizualizace přístupu zařízení do internetu v síti s centrálním prvkem

Mezi nejpravděpodobnější důvody útoku na chytré domácnosti bude získání informací o stavu domácnosti, zvycích jejich obyvatelů a dalších informací, které mohou být zneužity za pomocí social engineeringu. Manipulace se zařízeními v tomto prostředí může zahrnovat drobné nepříjemnosti jako je změna teploty ovlivněním termostatu, ale častěji se bohužel bude jednat o větší útoky vedené na vypnutí chytrého alarmu. Dohromady tyto útoky mohou například vést k loupežím kdy pachatelé vědí, že majitel domácnosti není přítomen a s vypnutým alarmem provést loupež beze svědků.

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 sít v této kategorii má na starosti jiné zařízení, z tohoto důvodu se u každé bude lišit cíl útoku, kde 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 lamp ale informace, které získá většinou je schopen získat i jiným způsobem a kdy nejchoulostivější data, která jsou přenášena jsou ve většině případů (jednotlivé řešení tohoto problému se mohou lišit), jsou informace o interním označení lamp. Na druhou stranu v této aplikaci, stejně jako u všech ostatních, aby útočník nebyl schopen se dostat k ovládání veřejného osvětlení – jeho vypnutí v době kdy by mělo svítit a podobným manipulacím. Dalším hypotetickým příkladem podobné infrastrukturní aplikace mohou být boxy pro vyzvednutí balíčků nacházející se na veřejných místech. Pro takovouto aplikaci není vhodné ani aby útočník byl schopen zjistit stav jednotlivých boxů, jestli v danou chvíli obsahují zásilku nebo jsou prázdné.

V průmyslové sféře je situace ochrany dat a správné funkčnosti sítě nekompromisní. Jakékoliv zásahy do systému mohou znamenat finanční ztráty v závislost 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 tohoto důvodu byl zde měl být kladen velký důraz na kvalitní a bezpečné zařízení. 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.

2.1 Současný stav zabezpečení

Internet věcí je v době vzniku toho dokumentu stále ještě v začátcích svého rozšíření pro využití širokou 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 zaobírají dopodrobna např.: odborné články od BitDefenderu [13] a Veracode [14].

Většina bezpečnostních mezer, které je v současné době možné nalézt v prostředí IoT, se již v minulost 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 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 vše bez výjimky potřebuje být zabezpečeno oproti útokům, což je jeden z hlavních důvodů proč se v současné upozorňuje na nezbytnost rozvoje této oblasti. Proto je nejprve zapotřebné si vymezit oblasti zabezpečení, které budou zkoumány. Hlavní oblasti, ve kterých je potřeba se zaměřit na bezpečnost, jsou přístup k zařízení, přenos dat a systém cloudových služeb. V každé z těchto oblastí by se měli dodržovat alespoň minimální úrovně zabezpečení. Cloudové služby na rozdíl od ostatních dvou oblastí dosahují stejných bezpečnostních standartu jako ostatní podobné serverové struktury. Důvodem pro tuto skutečnost je, že bezpečnost a spolehlivost nezbytnou skutečností pro funkčnost celé sítě. Poskytovatel těchto služeb si proto nemůže dovolit žádné zanedbání bezpečnosti v tomto ohledu. Dalším důvodem pro tuto skutečnost je samotná podstata cloudových služeb. Pro některé výrobce IoT zařízení není výhodné si vytvářet vlastní infrastrukturu jakou jsou serverové struktury a datová uložiště, takže si projímají potřebné prostředky od třetích stran, pro které je bezpečnost jedním z prodejních bodů.

Tento odstavec se popíše některé z bezpečnostních mezer se kterými byly schopny výrobky vstoupit na trh a byly odhaleny až v analýzách zmíněných na začátku této podkapitoly. Pravděpodobně nejzávažnějším nedostatkem se kterým se lze setkat (a který se vyskytl u výrobku uvedeném na trh) byl přenos zpráv ve formě volného textu. Tento problém se vyskytl jak u přenosu zpráv mezi zařízením a přístupovým bodem pro zařízení do internetu tak i v samotné komunikaci v něm. 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, ale musí se použít dostatečně robustních algoritmů a musí být správně implementovány. Na trhu byl objeven produkt, který komunikoval s klientskou aplikaci zprávami ve volném textu a heslem zašifrovaným 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 vyskytuje u 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 současný 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 (které mohou prosakovat data ven ze systému), atd.

Jedním z největších bezpečnostních rizik v 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 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), průzkum trhu se zaměřením na bezpečnost zařízení před koupí apod. Současné trendy naštěstí spějí k omezení možností, kde je uživatel schopen zanechat slabá místa.

2.2 Možné útoky

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.

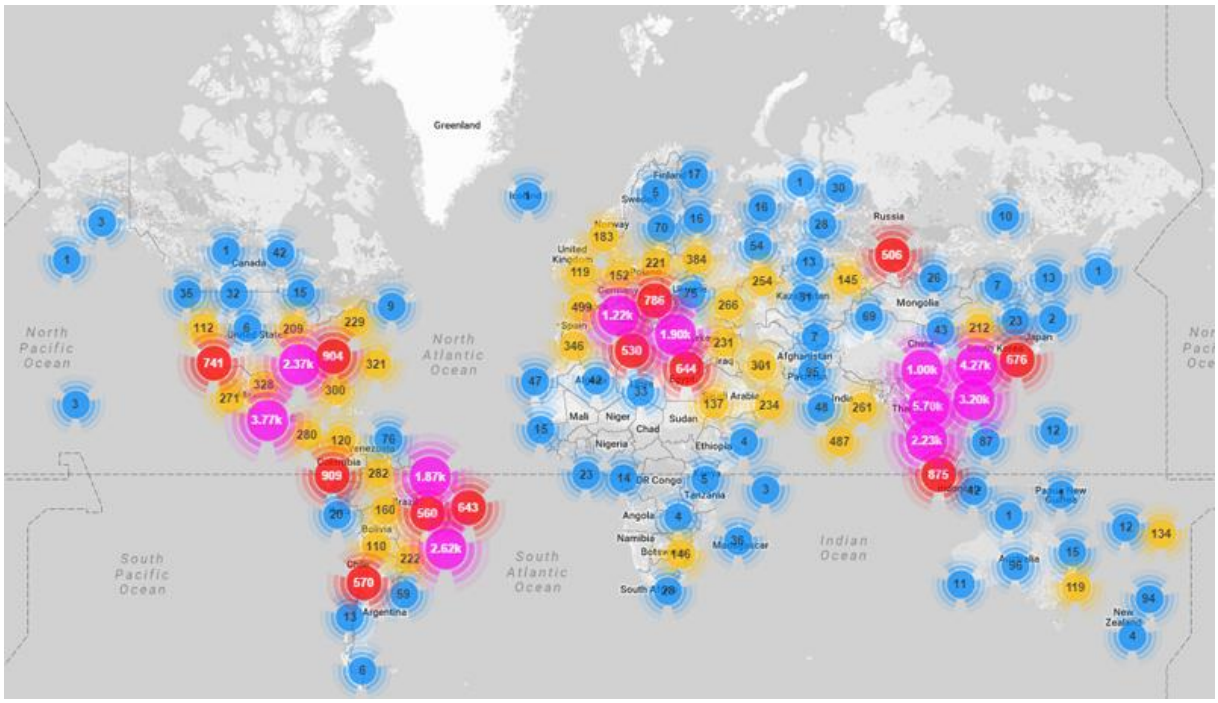
Man-in-the-middle attack – V tomto druhu útoku, narušitel odposlouchává a manipuluje s komunikací mezi dvěma zařízeními. Principem je přesvědčit obě strany spojení, že stále komunikují napřímo mezi sebou. Pro tento účel musí být útočník schopen vytvářet falešné zprávy, se kterými je schopen překonat 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 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.

Malware – Termín malware je zkratkou pro malicious software, tedy pro software k narušení chodu postiženého 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 rozšíření slabých hesel, jak se tomu stalo v případě malwaru Mirai [15]. 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. 6 je vidět mapa rozšíření zařízení infikovaných malwarem Mirai.



Obr. 6 Rozšíření malwaru Mirai

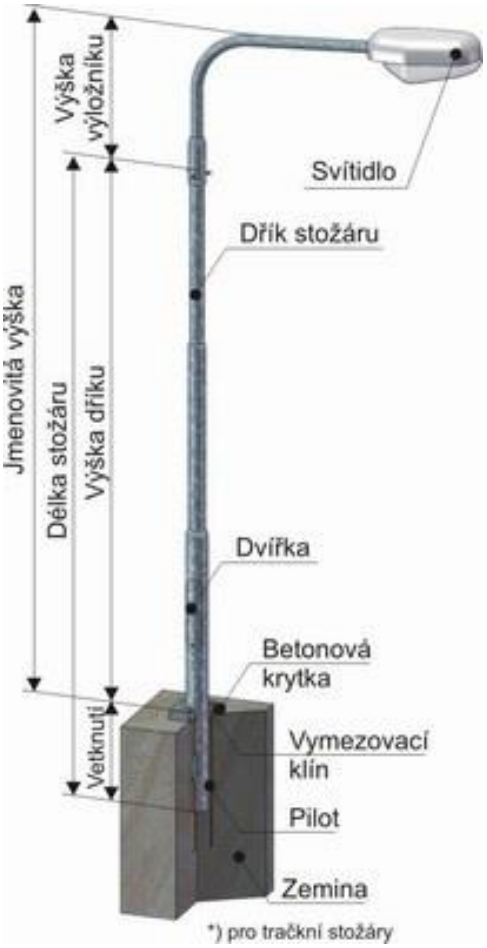
Útoky na lokální sítě – Pokud se povede útočníkovy nabourat do lokální sítě (nejčastěji získáním hesla od špatně zabezpečené wi-fi) obsahující inteligentní zařízení, tak může ve velké části případů převzít plnou kontrolu nad těmito zařízeními. Tohoto je možné dosáhnout, protože jedním z rozšířených nedostatků je přenos zpráv v místní síti ve volném textu. Některá zařízení komunikují pouze s cloudovou službou. V tom případě musí útoční ještě provést Man-in-the-Middle útok, pro získání kontroly nad 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 [16]. 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 vést i 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.

3 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. 7 a je vidět popis moderního sloupu veřejného osvětlení.

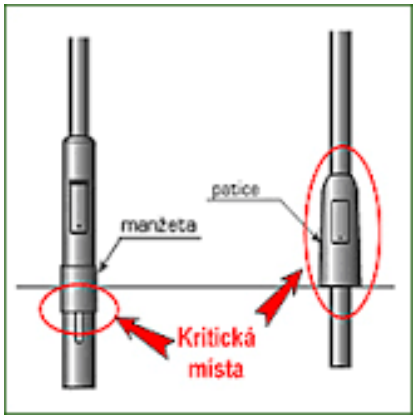


Obr. 7 Popis sloupu veřejného osvětlení

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 jako z litiny. 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). Na Obr. 8 jsou vidět oba typy stožárů.



Obr. 8 Ukázka sloupu bez patice a s paticí

Osvětlovací tělesa (Svítidla podle Obr. 7) používaná v současné době se dělí převážně do dvou kategorií výbojky a LED světla. V současné se hlavně využívá výbojek plněných 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. Jedná se o souhrnný termín pro nezbytné zařízení, které zajišťují provoz sloupu. Jedná se hlavně o svorky umožňující propojit silové obvody v trase stožárů a dále napojení a jištění svítidla ve stožáru.

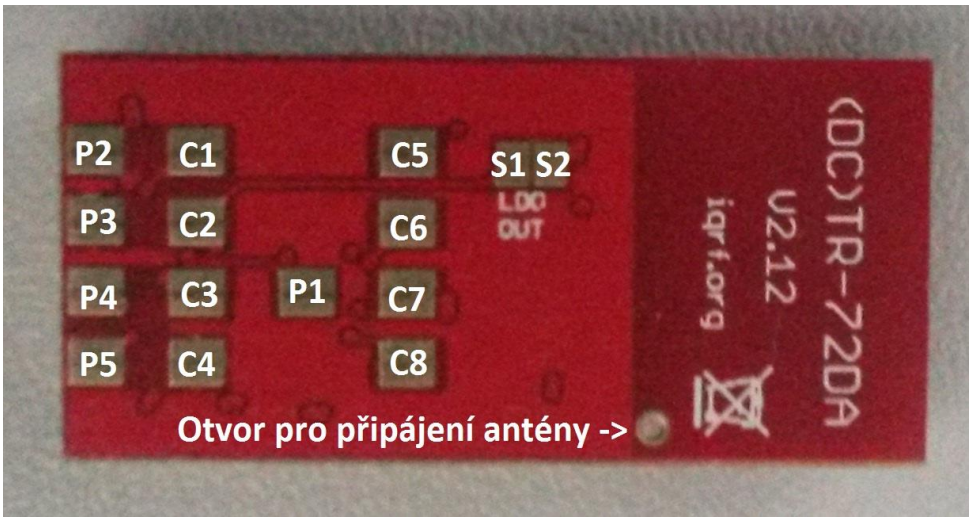
4 Realizace Demo aplikace ovládání veřejného osvětlení

Praktickou ukázkou využití zařízení Internetu věcí bude realizace demo aplikace ovládání veřejného osvětlení. Ovládání bude prováděno manuálně dálkově nebo automatizovaně za pomocí soumrakového spínače. Realizace bude provedena s využitím technologie IQRF a jejího vývojářského kitu DS-START-04.

4.1 Obsah vývojářského kitu DS-START-04

Development kit pro IQRF obsahuje následující komponenty, které jsou zobrazeny na Obr. 9 - Obr. 11:

- 3x IQRF komunikační modul TR-72DA, Obr. 9
- 1x Programátor CK-USB-04A, Obr. 10
- 2x Univerzální přenosový koncový modul DK-EVAL-04A, Obr. 11
- 1x USB to Micro USB kabel
- 1x USB flash disk se softwarem, dokumentací a příklady pro IQRF moduly

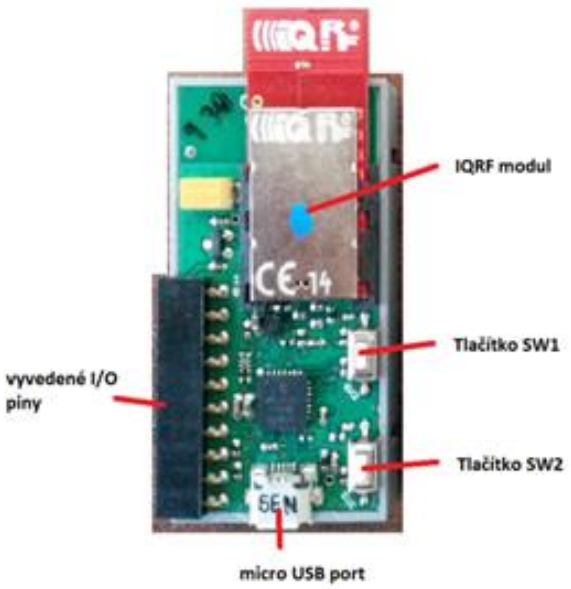


Obr. 9 Zadní strana komunikačního modulu TR72-DA

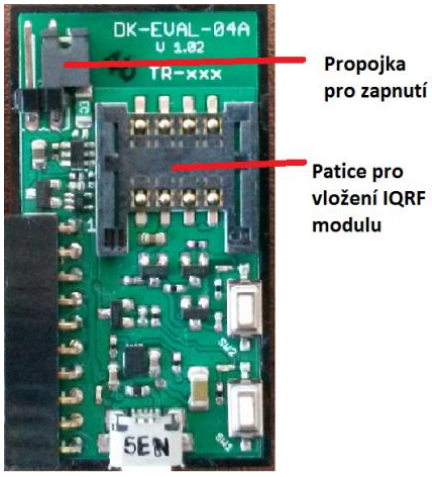
Popis jednotlivých vývodů z komunikačního moduluTR-72DA:

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



Obr. 11 Popis rozdílných součástí DK-EVAK-04A (oproti CK-USB-04A) bez komunikačního modulu

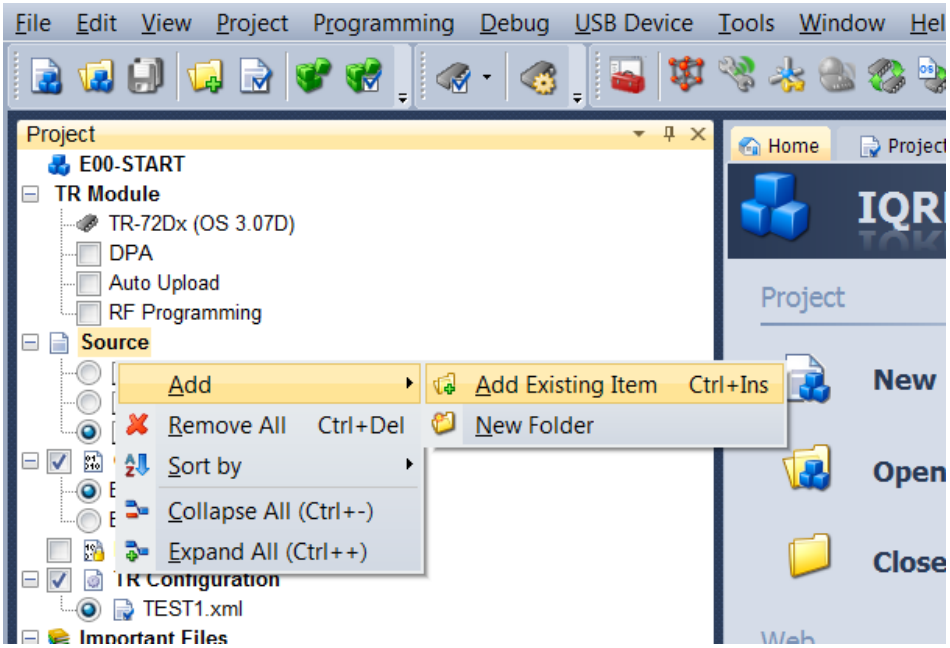
4.2 Příprava vývojářského prostředí

Pro naprogramování jednotlivých komunikačních modulů bude použit program IQRF IDE, který je v současné době ve verzi 4.36. 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 [17]. 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 .hex verze. 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. 12). V tuto chvíli se otevře nové okno s průzkumníkem, ve kterém se postupně vyberou oba soubory se zdrojovými kódy.

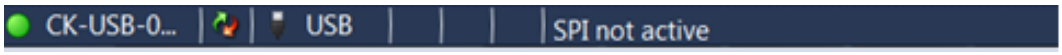
Před přesunem k samotnému programování je potřebné vysvětlit některé často opakující se úkony – kontrola stavu připojení zařízení k počítači, kompilace zdrojových kódů a jejich nahrání do komunikačního modulu:



Obr. 12 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. 13, respektive na Obr. 14.

Obr. 13 Stav připojení programátoru k *PC – nepřipojeno*



Obr. 14 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 souborům, ve kterých se nachází základní funkce, které bude program využívat. Knihovna, která bude využívána, se jmenuje template-basic.h. Na přenosném flash disku, který je součástí vývojářského kitu, je cesta k této knihovně:

.../Development/include/IQRF_OS/template-basic.h. 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 (ve tvaru, který je použit v ukázkách kódu) *#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 [18]). 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).

4.3 Komunikace mezi zařízeními

V této části bude popsán postup naprogramování vysílací a přijímací části komunikačního řetězce a nastavení síťového protokolu IQMESH. Zatím bude funkčnost programu zaměřena na manuální ovládání stavu žárovky (testování funkčnosti kódu probíhalo s využitím LED diody místo žárovky veřejného osvětlení).

Programování koncentrátoru:

Požadovanou funkčnosti vysílací strany je v tomto bodě možnost manuálního ovládání centralizovaného ovládání všech lamp veřejného osvětlení a monitoring stavu rozsvícení jednotlivých lamp. Základem pro jednotlivé zdrojové kódy jsou příslušné ukázky kódu pro programování IQRF zařízení. Základem pro část vysílací strany je ukázkový kód E01-TX.c z tohoto jednoduchého programu byla použita programová kostra, která obsahuje všechny základní náležitosti pro požadovanou aplikaci. Z původního kódu byla ponechána pouze základní struktura, a ještě funkce pro odeslání zprávy po stisknutí tlačítka. Zmíněná část kódu je k vidění na ukázce 1.

Ukázka 1:

```
if (buttonPressed)
{
        pulseLEDG();            //    LED indication
        PIN = 0;
        DLEN = 4;               //    Nastavení délky packetu (počet bytu, které budou
odeslány)
        RFTXpacket();           //    Odeslání požadované zprávy
        waitDelay(25);
}
```

Data určená k odeslání se dají nastavit dvěma způsoby. Prvním způsobem je nahrání dat do paměti EEPROM. Použitý příkaz pro nahrání dat do paměti je #pragma cdata[__EEAPPINFO] = "0123", kde v uvozovkách jsou příslušná data. Délka přenesených dat je poté určena příkazem DLEN, jak je vidět v předchozí ukázce kódu.

Druhým způsobem, kterým je možno manipulovat s daty k odeslání je, pokud k práci s nimi přistupuje jako k práci s polem. Tímto způsobem je možné přistupovat k datům jednotlivě a je také možné s daty jednoduše manipulovat. Takto vytvořená data, jsou uložena v jedno z bufferů modulu a pro další manipulaci s nimi je nutné je zkopírovat do jiného bufferu nebo uložit do paměti. Příkaz pro načtení dat do RF bufferu (buffer pro data, která budou modulem odeslána přes radiovou frekvenci) je bufferRF[0]=0; (číslo v [] určuje pořadí jednotlivého bytu v bufferu). Data se poté ukládají do jiných bufferů / pamětí příkazem Copy, kde plná syntaxe obsahuje počáteční lokaci dat a cílovou např.: copyBufferRF2COM(); (viz. Reference guide). V kódu je využito druhého způsobu kdy do RF bufferu nahrajeme hodnotu 0x30 hexa pro zhasnutí a 0x31 pro rozsvícení. Jelikož se jedná o centralizované ovládání sítě vyslaný packet způsobí rozsvícení nebo zhasnutí všech lamp veřejného osvětlení. Při realizaci sítě s přístupem do cloudu by dalším krokem bylo ovládání jednotlivých lamp z webového prostředí.

Ukázka 2:

```
if(o_s==1)                  // Kontrola minulého stavu rozsvícení
{
        bufferRF[0]=0x30;   // Zhasnutí
        o_s= 0;             // Nastavení příštího stavu - další stisk tlačítka rozsvítí
}
else
{
        bufferRF[0]=0x31;   // Rozsvícení
        o_s = 1;            // Nastavení příštího stavu - další stisk tlačítka zhasne
}
```

Další funkční 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 3.

Ukázka 3:

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

Finální částí programu pro koncentrátor je nastavení síťového protokolu IQMESH. Tohoto se docílí použitím metod pro nastavení koordinátoru, zapnutí směrování, nastavení filtrování sítě atd. (viz. Reference guide). Nejprve je nutné do programu zahrnout hlavičky metod a poté je znovu zavolat v programu. Dokončený program je v k nalezení v přílohách k této práci.

Programování koncového modulu:

Než se přejde k rozboru zdrojového kódu, je nejprve nutné popsat požadovanou funkčnost modulu. Účelem koncového modulu je ovládat stav veřejného osvětlení v závislosti na ovládání centrálně přes koncentrátor nebo lokálně s využitím světelného senzoru (viz následující kapitola 4.4). Vždy poté co se změní stav rozsvícení modul, vyšle zprávu, ve které informuje koncentrátor a o této změně. Pro ovládání relé, které bude vykonávat spínání, bude použito pinu C5 (dle Obr. 9 z kap 4.1), dalším pinem který bude zapojený je pin GND.

Realizace kódu pro přijímací moduly jednotlivých sloupů je poté opět založena na ukázkovém příkladu pro IQRF. Tentokrát bylo využito souboru E02-RX.c, ze kterého byla ponechána kostra programu obsahující podmínku kontrolující přijetí zprávy. Do této podmínky se poté vnoří další podmínka, která kontroluje obsah zprávy. Podle obsahu zprávy od koncentrátoru se poté vybere příslušná možnost podle, které se změní stav rozsvícení. Změny stavu jsou provedeny nastavením RE5_IO do 0 pro zhasnuté světlo a do 1 pro rozsvícené. Tuto hardwarovou proměnou je potřebné také inicializovat mimo prostor funkce APPLICATION a poté nastavit počáteční hodnotu.

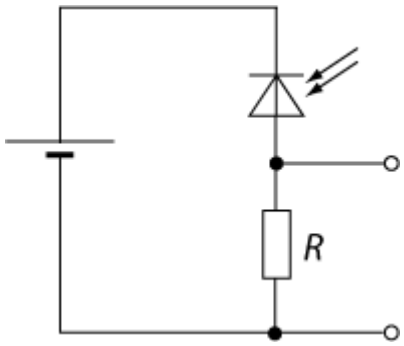
Ukázka 4:

```
copyBufferRF2COM();
if((bufferCOM[0]==0x30)        // Podmínka kontrolující příkaz od koncentrátoru
{
        RE5_IO = 0;            //Zhasnutí
}
else
{
        RE5_IO = 1;            // Rozvícení
}
```

V tomto okamžiku je ještě nutné nastavit odesílání současného stavu rozsvícení zpátky na koncentrátor. Tohoto docílíme tím, že dočasně nahrajeme do RF bufferu hodnotu 0 a 1 v závislosti na stavu proměnné RE5_IO. Posledním krokem stejně jako v případě programu pro koncentrátor je nutné nastavit protokol IQMESH.

4.4 Realizace ovládání za pomocí soumrakového senzoru

Další funkcí, kterou aplikace bude vykonávat je ovládání rozsvícení za pomocí světelného senzoru. Realizace senzoru je provedena s využitím fotodiody a odporu v zapojení diody jako spotřebiče.



Obr. 15 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 [19]) 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.

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. O propojení mezi fotodiodou a IQRF modulem se stará trojlinka H03VVH2-F.

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.

Programování koncového modulu s komparátorem:

Nyní se bude pokračovat v práci se zdrojovým kódem pro koncové zařízení z minulé kapitoly. Pro naprogramování požadované funkce je hlavně zapotřebí analogového komparátoru. K tomuto účelu se opět využije jednoho z ukázkových zdrojových kódů. Tentokrát se jedná o soubor z adresáře s pokročilými ukázkami (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 5. 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 5:

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

Kontrola rozsvícení pomocí v závislosti na úrovni vnějšího osvětlení se dá realizovat i jinými způsoby. Prvním z nich je vzít několik IQRF modulů a dedikovat je pro rozhodování pro monitoring úrovně osvětlení. Kde každý modul by měl na starosti části 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 [20]. Na trhu, jíž 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.

4.5 Možnost připojení do Cloudového řešení

Dalším krokem v realizaci celkového aplikace by bylo připojení sítě do cloudu. Bohužel jednou z nevýhod vývojového kitu, je nemožnost jeho využití jako brány pro přístup do internetu / cloudového řešení IQRF. V tomto případě by se ještě muselo dokoupit zařízení brány pro přístup do internetu. Pro IQRF existuje více možností realizace internetové gateway – od malých kompaktních, které se dají připojit přes rozhraní USB do počítače, až po samostatné gateway, které k internetu přistupují pomocí technologií wi-fi, ethernet nebo GSM.

V následujícím textu bude zjednodušeně popsána instalace IQRF gateway a jejího propojení s cloudem, celý detailně vysvětlený postup lze nalézt na stránkách IQRF [21].

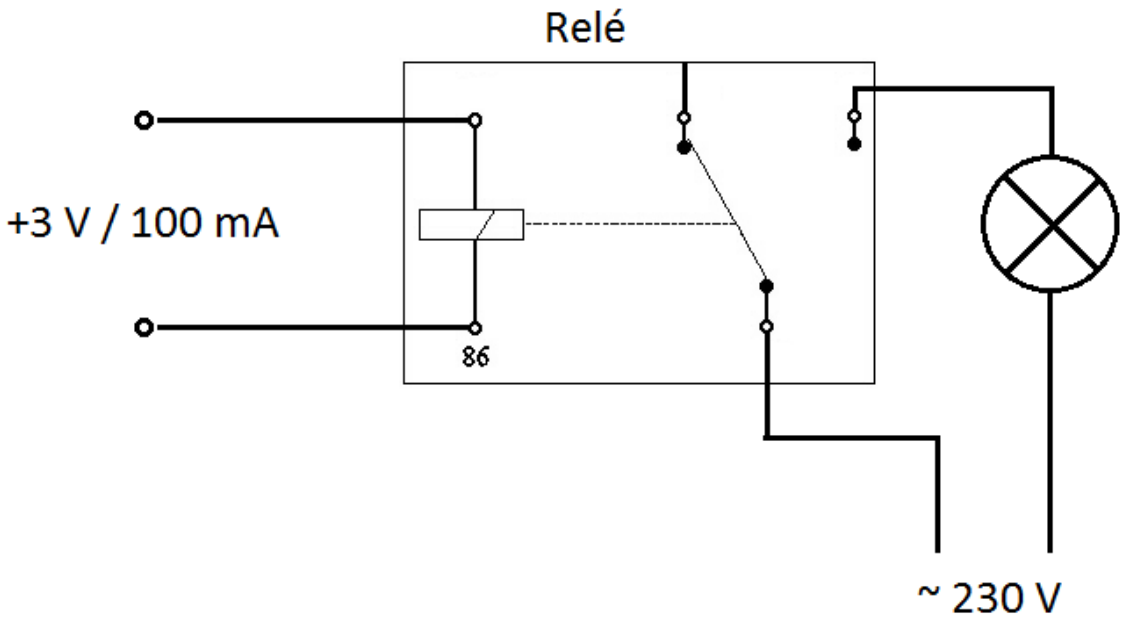
- Připojení brány k počítači a její rozpoznání v IQRF IDE
- Prvotní přihlášení do brány, defaultní přihlašovací jméno/heslo – iqrf/iqrf (lišta Tools -> GW Tool)
- Otevření záložky Basic v okně, které se otevře a vybrání použití brány společně s IQRF cloudem a nastavení parametrů přenosu
- Změna hesla v záložce Administration
- Vytvoření účtu na stránkách IQRF: https://cloud.iqrf.org
- Spárování Gateway a účtu na stránkách Cloudu – záložka Gateway registration / editing, kde Gateway ID se získá přes IQRF IDE, kde v okně pro spravování brány přejde do záložky Status a dole v okně se zvolí tlačítko Copy ID, přes které se ID zkopíruje do schránky
- Po spárování a inicializaci je možné nahlédnout na data, která se updatují v uživatelsky nastavených cyklech

Poté co je síť připojená do cloudu, dalším krokem, který v této práci není realizovaný z důvodu nemožnosti použití vývojového kitu jako brány, by byla realizace webové aplikace (realizované za pomocí JavaScriptu nebo PHP) pro přístup a zprávu dat ze sítě.

Aplikace by hlavně monitorovala stav jednotlivých lamp veřejného osvětlení - jejich stav v závislosti na světelném senzoru. Další funkcí, která by byla implementována je možnost ovládání stavu světel nezávisle na světelném senzoru, ať už by se jednalo o jednotlivá světla nebo o všechna naráz. Tohoto lze docílit díky skutečnosti zmíněné v kapitole 4.2, a to že každé světlo (každý komunikační modul) má svůj vlastní unikátní identifikátor, který posílá ve v zprávách pro koncentrátor, ale podle kterého se také rozhoduje při přijímání zpráv, jestli jsou určeny pro něj nebo ne.

5 Hardwarová řešení

Veškeré testování kódu a jeho funkčnosti prozatím probíhalo na integrovaných LED diodách koncového modulu DK-EVAK-04A nebo na externě připojené LED diodě. V reálném prostředí se však bude ovládat osvětlovací těleso s mnohem vyšším příkonem. Většina lamp pouličního osvětlení pracuje s příkonem 50–150 W, u zřizování nového osvětlení je výjimečně zapotřebí vyššího příkonu. V této práci se věnujeme situacím, kdy je využíváno maximálního příkonu 150 W, kde již v takovémto případě se jedná o velká světelná tělesa. Pro spínání světla bude použito spínací výkonové relé. Finální zapojení spínacího relé je na obr. 16.



Obr. 16 Zapojení relé

Z datasheetu pro komunikační modul TR-72DA [22] lze vyčíst hodnoty výstupního napětí a maximálního možného odebíraného proudu. Tyto hodnoty jsou U_{out} = +3 V ± 60 mV, I_{max} = 100 mA. Na výstupu relé se bude pracovat s napětím 230 V a jak již bylo zmíněno příkon pro světelné těleso bude maximálně 150 W. Podle těchto parametrů je potřebné zvolit vhodné spínací relé. Po průzkumu trhu bylo vybráno relé G6RL-1 DC3 od společnosti Omron, které splňuje potřebné parametry. Podle datasheetu výrobce [23], může relé spínat při 3 V stejnosměrného napětí na cívce a proudu 73,3 mA a je schopné spínat napětí až 400 V střídavých (300 V stejnosměrných), maximální spínaný proud může dosahovat až 10 A (doporučuje se nepřekračovat 8 A) a maximální spínaný výkon je 150 W. Při výběru relé je potřebné se řídit hlavně podle parametrů spínací cívky a hodnoty maximálního spínaného výkonu na výstupu. Pokud by nebylo na trhu k nalezení relé těchto parametrů, je možné vybrat relé s jinými parametry cívky a použít

zapojení se zesilovačem. Nejčastěji se pak bude jednat o relé s potřebným napětím na cívce 5 V. Další výhodou zvoleného relé je realizace pouzdra. Jedná se o kompaktní nízko-profilové pouzdro vysoké pouze 12,3 mm (rozměry V/Š/D: 12,3/10/28,5 mm). Z tohoto důvodu je možné relé vložit do krytu našeho zařízení viz. další podkapitola. Existují také relé s podobnými parametry, které jsou rozměrově mnohem větší a v takovém případě se většinou jedná o produkty, které se dají přichytit na některou z normovaných lišt (například na DIN lištu, která se používá na přichycení elektrické výzbroje v sloupech věřeného osvětlení).

5.1 Návrh ochranného krytu

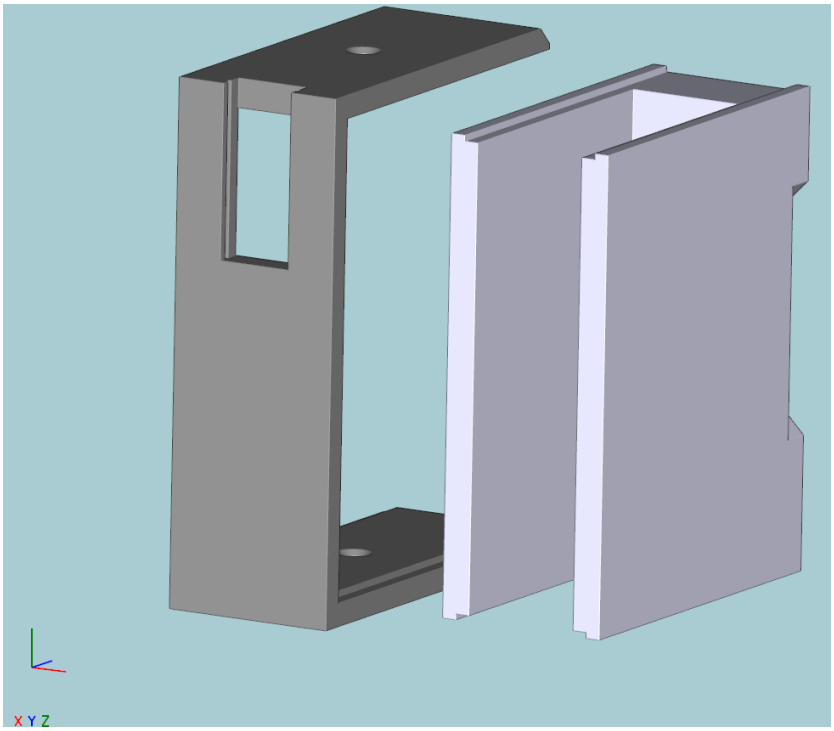
Jelikož nemůžeme umístit komunikační modul do dříku sloupu veřejného osvětlení samostatně, je zapotřebí navrhnout kryt. Tento kryt musí být mýt dostatečné vnitřní rozměry, aby byl schopen pojmout komunikační modul, spínací relé a zdroj energie (baterii). Při návrhu krytu je také nutné dbát na vnější 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.

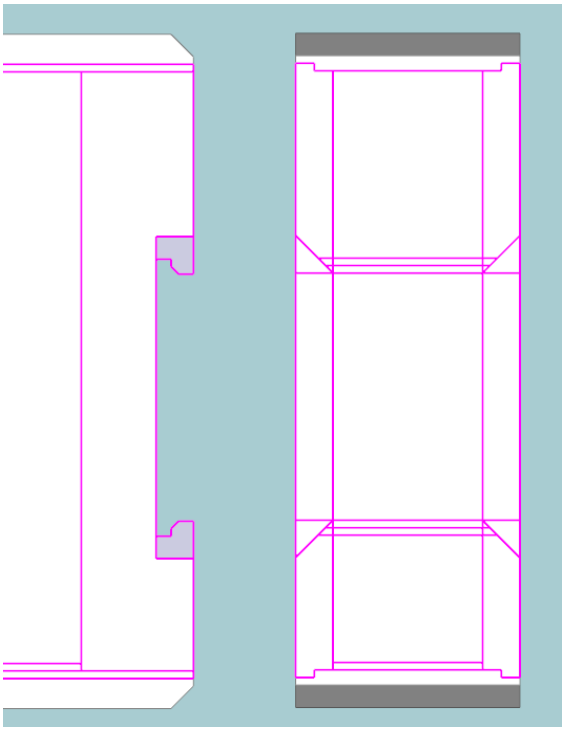
Maximální rozměry pro ochranný obal pro zařízení jsou 90x30x70 mm (V/Š/D). Tyto rozměry byly zvoleny s ohledem na vnitřní prostor sloupu veřejného osvětlení (rozměry byly inspirovány podle v současné době instalovaných modulů do sloupů veřejného osvětlení [24]) a na velikosti komunikační modulu a relé. Samotný kryt se skládá ze dvou částí, které se do sebe zasunou, kde finální podoba výrobku je vidět na Obr. 17.

Všechny stěny, kromě zad druhého části krytu, jsou široké 5 mm. Díky tomu nám na šířku zbývá 20 mm, kde dva ze tří rozměrů použitého relé jsou menší než tato hodnota, takže se relé bez problému vejde dovnitř. 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. 18, kde je zobrazena část pohledu z boku a na zadní stranu, v obrázku jsou také zvýrazněny vnitřní hrany zadního dílu.



Obr. 17 Ochraný kryt



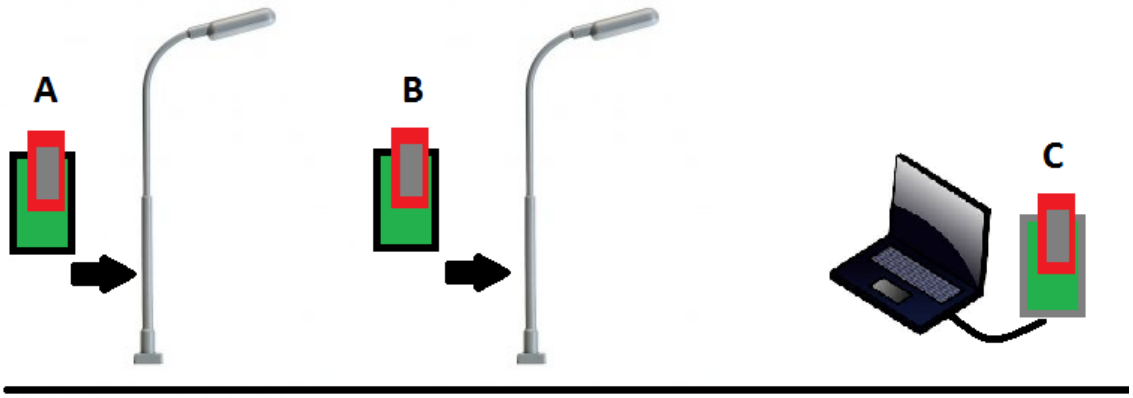
Obr. 18 Zadní strana ochranného krytu

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 ^{o}C (např.: materiál PLA se může začít deformovat již při teplotách překračujících 60 ^{o}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.

6 Měření parametrů vysílače při umístění v dříku sloupu

Jedním z cílů této práce je 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. V těchto případech je nejčastějším zdrojem rušení, rušení vzniklé na osvětlovacím tělesu. Na druhou stranu zde nenastává problém s odstíněním signálu, protože komunikační moduly jsou umístěny v místě pro ně uzpůsobeném. 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. 19, bude popsána funkce kódů nahraných do jednotlivých modulů, kde celé zdrojové kódy jsou k nalezení v příloze.



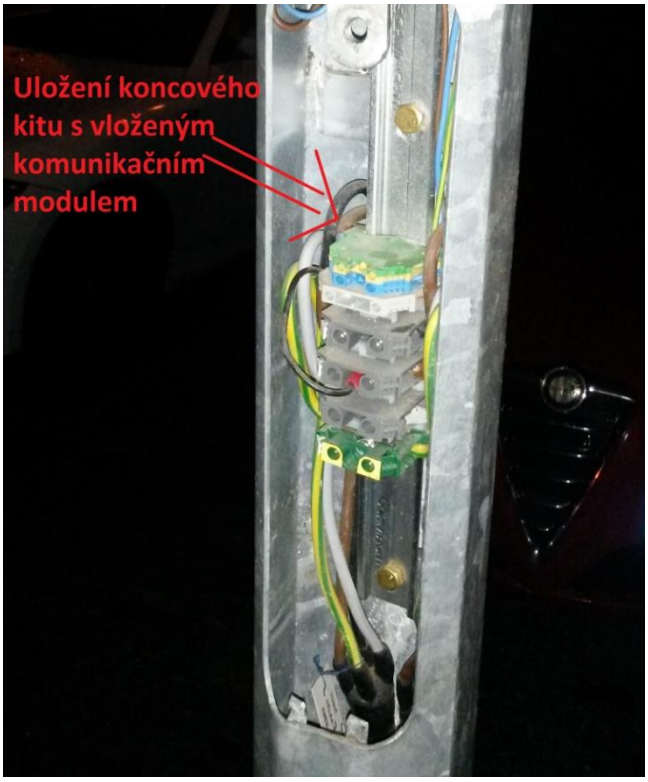
Obr. 19 Měřící pracoviště

Kód nahraný do modulu A (označení modulů podle Obr. 19) 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. 20)
- Venkovní teplota: okolo +5 °C
- Uložení komunikačního modulu dle Obr. 20.



Obr. 20 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. 21)
- Venkovní teplota: okolo -5 ^{o}C

Obr. 21 Patice sloupu použitá ve 2. měření

6.1 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 22 (měření na 25 m) a 23 (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. 22 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. 23 Výpis z IQRF IDE – měření na 50 m

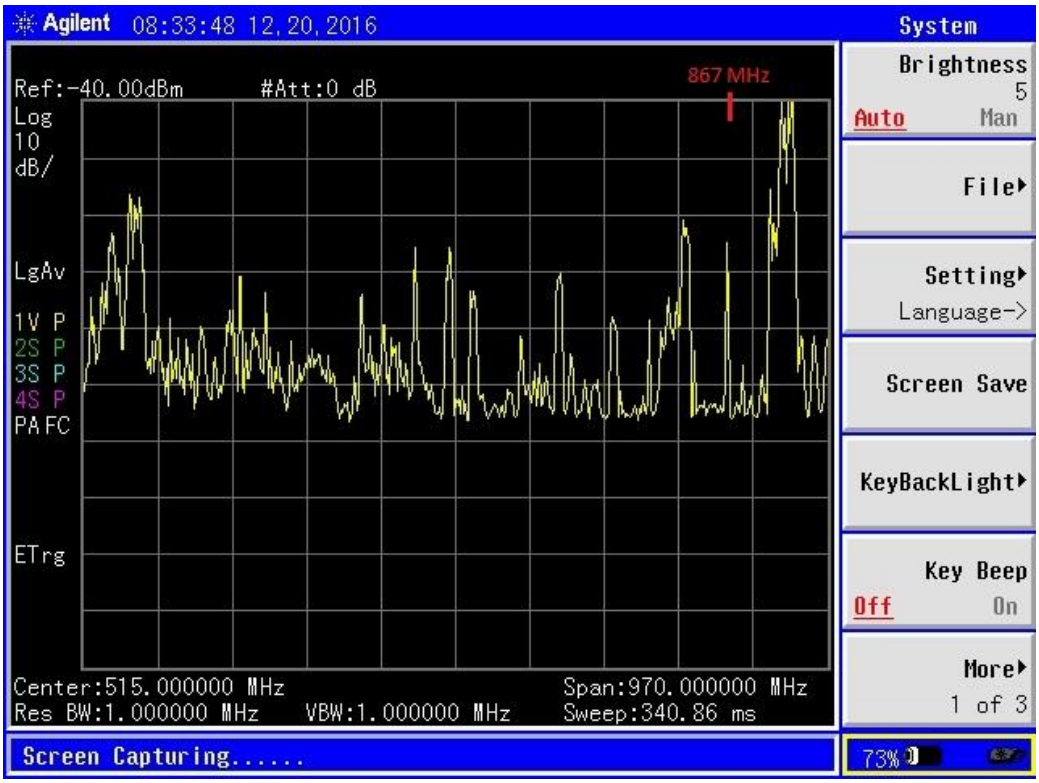
Měření na 50 m proběhlo hlavně z důvodu využití protokolu IQMESH ve finální aplikaci. Protože při zapnutém směrování v síti je možné, aby síť stále fungoval i při výpadku jednoho z modulů, a proto je nutné otestovat kvalitu přenosu i na vyšší vzdálenost (ob jeden sloup).

6.2 Důsledky výsledku měření

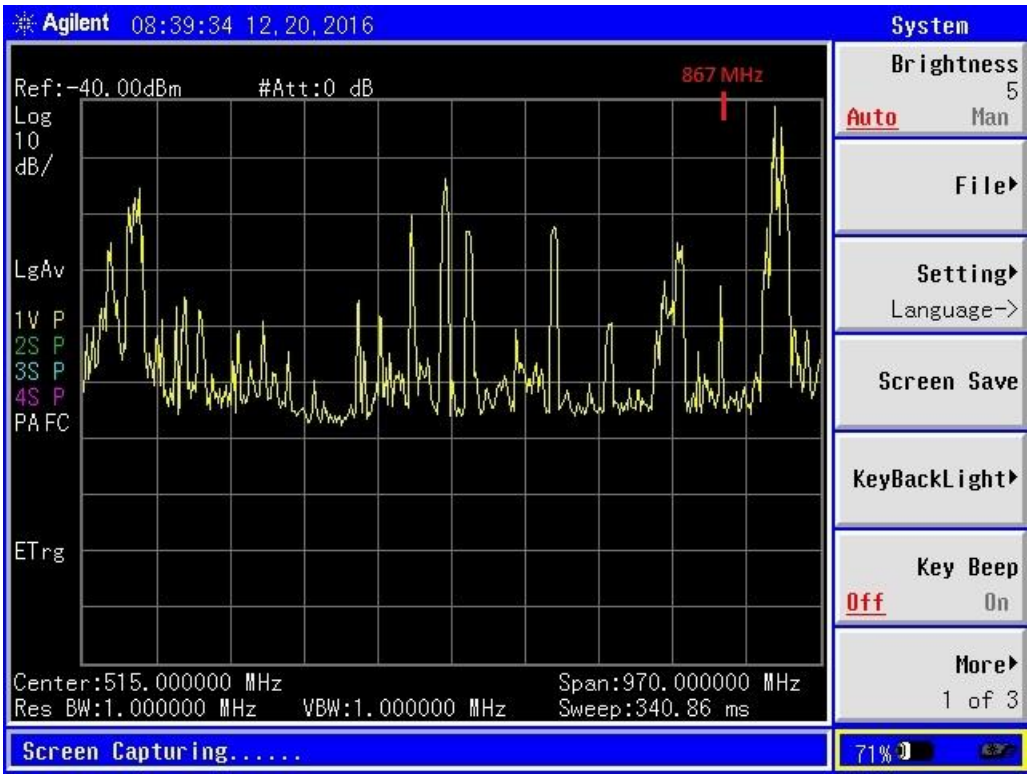
Jelikož Druhé měření provedeno na starších sloupech veřejného osvětlení ještě využívajícího konstrukce s betonovou paticí, které se v praxi téměř do nových projektů nenasazuje, je nutné spíše pracovat s výsledky prvního měření. Z výsledků prvního měření (a částečně i z druhého) se došlo k závěru, že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

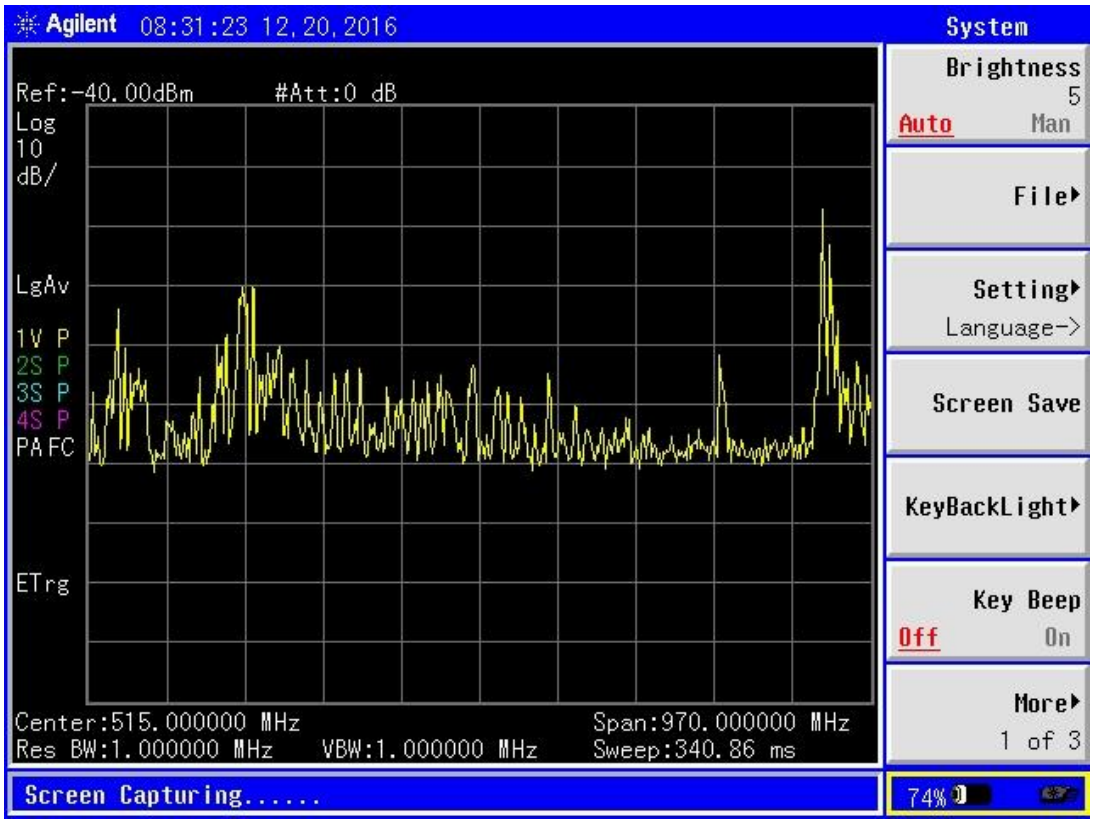
Druhou možností řešení problémy je využití již v praxi implementovaného konceptu umístění komunikačních modulů k osvětlovacímu tělesu. Velkou nevýhodou tohoto řešení je omezený přístup k zařízení. Výška stožárů veřejného osvětlení se pohybuje v rozmezí 4–6 m pro parkové osvětlení, 8–12 m pro uliční a 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. Na následujících obrázcích jsou vidět průběhy rušení od sodíkové výbojky (Obr. 24) a LED světla (Obr. 25) + referenční měření rušení v pozadí (Obr. 26). Měření bylo provedeno spektrálním analyzátorem N9340B výrobce Agilent a prutovou anténou RH799, výrobce DIAMOND. V průbězích je poté vidět že na kmitočtech okolo 865–870 MHz je rušení vyšší v průměru o 25 dB v případě sodíkové výbojky a o 15 dB v případě LED světla oproti referenční hodnotě. Přestože tyto hodnoty nejsou příliš vysoké, bylo by nutné s nimi počítat z důvodu vzdálenosti mez osvětlovacím tělesem a komunikačním modulem.



Obr. 24 Průběh rušení na sodíkové výbojce



Obr. 25 Průběh rušení na LED světle



Obr. 26 Průběh rušení na pozadí

7 Finanční analýza řešení

Jedním z důležitých aspektů celého řešení je finanční přínos jeho implementace. Pokud nebude řešení finančně výhodné v dlouhodobém výhledu, je jeho přínos nejistý. Proto je tato část práce zaměřená na zjednodušenou finanční analýzu problému. Finanční analýzu pro navrhnuté řešení provedeme pro sto lamp. Tento počet byl zvolen z důvodu toho, že některé součástky se nedají nakoupit v menším množství, než je právě sto (většina modelů komunikačních modulů technologie IQRF se dá objednat až od zmíněného počtu). Další velkou výhodou tohoto přístupu jsou množstevní slevy téměř na všechny součástky v případě nákupu sta kusů. Celkový rozpočet na vybavení sta sloupů veřejného osvětlení bude vypadat podle následující tabulky:

součástka	model	cena / kus	počet	celková cena	reference	pozn.
		Kč/kus	-	Kč		
Komunikační modul	TR-72DA	323,00	100	32 300,00	[25]	
Brána do internetu	GW-ETH-02A	2 900,00	1	2 900,00	[26]	(a)
Anténa	AN-DO1-U.FL	93,80	100	9 380,00	[27]	
Baterie	BK-CR 2032	8,10	100	810,00	[28]	
Uchycení baterie	BK883	7,50	100	750,00	[29]	
Relé	G6RL	74,10	100	7 410,00	[30]	
Optický senzor	BPW 34	13,90	100	1 390,00	[31]	(b)
Rezistor 15 kW	25EP51415K0	4,14	100	414,00	[32]	
Kabel k senzoru	H03VVH2-F	4,42	500	2 210,00	[33]	(c)(d)
Ochraný obal	F6 IP55	10,10	100	1 010,00	[34]	(e)
				58 584,00		

Ještě, než se text bude zabývat důsledkem celkových nákladů, je potřebné si vysvětlit některé položky z tabulky:

- (a): V případě brány do internetu, je možné, že podle topologie sítě bude zapotřebí více než jednoho zařízení, pro další úvahy se ale bude počítat pouze s jedním kusem.
- (b): U optického senzoru, v tomto případě fotodiody (v zapojení s odporem dle Obr.15) můžeme zvolit z širokého množství druhů součástek a podle toho se může lišit finální cena položek optického senzoru a rezistoru.
- (c): Přívodní kabel pro optický senzor je dvoužilový a jeho celková délka byla určena, za předpokladu instalace zařízení do sloupu veřejného osvětlení s výškou 5 m.
- (d): Kabel je uveden jako Cena/m a počet je brán v metrech.

- (e): V otázce ochranného obalu nastala největší změna oproti předpokládanému postupu. Původně zamýšlený obal, který byl navrhnut v kapitole 5.1, byl nahrazen již existujícím krytem. Tato změna byla provedena z finančních důvodů. Levnější varianta, která splňuje všechny naše požadavky, se dá sehnat za cenu kolem 10 Kč / kus (hlavní rozdíly – jiný způsob uchycení, vše je uzavřeno uvnitř krytu). Naproti tomu ceny 3D tisku se odvozují v závislosti na objemu finálního výrobku, kvůli ceně materiálu, který by byl použit pro tisk. Objem krytu z kapitoly 4.2 se pohybuje okolo 101 cm^2, kdy cena za jeden 1 cm^2 se při použití ABS plastu pohybuje okolo 0,25 dolaru [35], což je v přepočtu kolem 6,46 Kč. Z tohoto je vidět, že i při úpravách krabičky s cílem snížit objem, nebo najití lepší ceny / dosažení množstevní slevy je stále nevýhodné ji využívat. Využití takto navrhnutého obalu se vyplatí pouze pro velmi malé série, nebo naopak pro velkovýrobce, který má prostředky a technologie na minimalizaci výrobních nákladů.

Pro další úvahy ještě vhodné navýšit finální částku. Zatím nebyla započítána cena montáže. Je také dobré započítat rezervu, v případě, že některé součástky budou muset být koupeny za jinou cenu, nebo pokud by bylo zapotřebí hledat jiné varianty potřebných součástek. Započítat rezervu je tedy vhodné v jakémkoliv případě. Rezerva bude zvolena na 20 % ze současné celkové ceny realizace, a to činní kolem 11 700 Kč a celkově se po zaokrouhlení dostaneme na částku 70 000 Kč. Pro zpřehlednění situace se bude v dalším textu pracovat se situací, kdy všechny ceny budou vztaženy k jednomu kusu, v případě instalace našeho zařízení se jedná o částku 700 Kč.

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 jsou od 2 000 do 4 500 Kč), proto bude využito příkladu z praxe. Samostatný 8 m vysoký stožár, od firmy Amako [36], v provedení JB 10 L stojí kolem 7 000 Kč, k němu cena výbojkového světla TRITON S od společnosti OBS [37] se pohybuje okolo 2 200 Kč. Jedná se o běžně používané součásti od Českých a Slovenských výrobců, se kterými mi se lze běžně setkat v praxi. Celkově se pak cena pro vztyčení a zapojení jednoho sloupu pohybuje okolo 15 000 Kč, kde v této částce jsou započítány také zemní práce a mzda pro zaměstnance. Z těchto čísel je zřejmé, že cena tohoto řešení využívajícího IQRF jednotek procent ať už se jedná o levnější nebo dražší konfiguraci sloupu veřejného osvětlení. V ukázkovém případě je celková cena vyšší o 4,67 %.

Dalším finančním kritériem, které je potřeba zohlednit je návratnost investice. Veřejné osvětlení je služba pro obyvatele příslušných oblastí, takže jediná oblast, kde se dá tímto způsobem ušetřit, je spotřeba energie. Jak již bylo v textu zmíněno, osvětlovací tělesa mají výkon mezi 50–150 W. V případě zmíněného osvětlovacího tělesa se jedná o 70 W výkon. Ceny energií se v České republice značně liší podle dodavatele, průměrně se však pohybují okolo 4 Kč/kWh za plnou sazbu a 2,5 Kč/kWh za sníženou sazbu. Jakožto parametr návratnosti se bude brát v úvahu, o kolik hodin méně se musí denně svítit, aby zařízení zaplatilo v průběhu 10 let. Nejprve je nutné si spočítat kilowat se dá koupit za 700 Kč (ceny energií porostou, ale pro tyto účely budeme brát v úvahu pouze současné ceny). Dělením nám vyšlo, že za 700 Kč se dá pořídit 280 kWh. Druhým krokem je určení kolik hodin potřebuje osvětlovací těleso k spotřebování 1kWh. Při spotřebě 70 W nám vyjde 1000 kWh / 70 W = 14,15 h. Celkový počet hodin, kdy se nebude svítit tedy je 280 x 14,15 = 3968 h. Při rozpočítání na 10 let se dospěje k tomu, že osvětlovací těleso by denně muselo svítit o 1,08 hodiny méně.

Jak je tedy vidět finanční návratnost je mizivá, ale stále v kontextu s celkovou cenou vztyčení sloupu veřejného osvětlení se investice pohybuje v řádu jednotek procent. V tento okamžik je tedy opět nutné vzít potaz hlavní funkci veřejného osvětlení, a tou je služba pro občany. Zkvalitněním služeb pro občany, díky využití chytrého systému obsluhy veřejného osvětlení se dosáhne návratnosti v jiném směru. Tímto je myšleno nejen zlepšení doby provozu osvětlení ale také možnost lepšího monitoringu poruch apod. Je také potřeba vzít do úvahy možnost budoucí implementace dalších funkcionalit, které dále ještě zkvalitní úroveň poskytovaných služeb.

7.1 Možná alternativní řešení

Jak již vyplynulo z předchozího textu, popsaný způsob přístupu k problému neřeší všechny úskalí, se kterými je možné se zde setkat. Z tohoto důvodu je dobré zmínit další možná řešení, jejich výhody a nevýhody.

Jedním z takovýchto potencionálních řešení je takové, kde by se neovládali jednotlivé sloupy ale celé větve. Větví se v tomto případě myslí spojení několika sloupů dohromady přes svorky, kdy pak toto spojení připojeno do rozvaděče jako celek. Pokud by se tedy ovládaly jednotlivé větve z rozvaděče jako celek, bylo by možné ušetřit velkou část nákladů za realizaci. V takovémto případě by stačilo mít pouze několik komunikačních modulů, kde na každou větvi by připadaly maximálně 2 moduly. Jeden z modulů by byl umístěn v rozvaděči a zajišťoval by ovládání větve systému veřejného osvětlení a druhý modul by měl k sobě připojen světelný senzor. Kromě již zmíněné výhody jednoduchosti tohoto řešení, tak se také zachovává největší výhodu původního řešení, kterou je jednoduchost přístupu k ovládacím prvkům. Při tomto řešení je také vyšší konsistence při rozšiřování jednotlivých. Tímto je hlavně myšleno, že celá větev se rozsvítí naráz a kompletní plocha, kterou má určená větev na starost, bude osvětlena.

Efekt kdy se každé světlo rozhoduje samostatně, se může uplatnit hlavně v parcích nebo podobných místech kde je inkonsistentní rozložení světla. Tento postup však není vhodný pro plochy, jako jsou například parkoviště nebo ulice. Nevýhodou ovládání celých větví je velmi omezená možnost vývoje budoucích služeb, kdy u ovládání jednotlivých sloupů je možné postupně rozšířit služby např.: o monitoring poruch světel apod.

Význam této krátké podkapitoly je poukázat na to kolik způsobů řešení tohoto problému existuje. Přestože v současné době nastává vysoká úroveň rozvoje v této oblasti, tak se zatím stále ale většinou jedná o podobné způsoby přístupu k problému. V budoucnu se budeme setkávat s mnohem sofistikovanějšími způsoby řešení, které budou upraveny na míru požadavkům daného projektu.

8 Závěr

Tato 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 jednotlivých standardů, kdy existuje velké množství těles, která se snaží vytvořit vlastní standardy. Z tohoto důvodu existuje velký zmatek v tomto směru. Druhým velkým problémem v Internetu věcí, je nedostatečná úroveň zabezpečení napříč různými zařízeními. Některé z v současné době nabízených 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. Z tohoto důvodu 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 technologie IQRF. Ovládání stavu rozsvícení je realizováno dvěma způsoby. Prvním z nich je možnost centrálního ovládání za využití jednoho komunikačního modulu, kdy se ovládá celá síť (soustava osvětlení) najednou. Druhý způsob je realizován s pomocí světelného senzoru (fotodioda). Každý sloup veřejného osvětlení obsahuje senzor, který s pomocí komparátoru rozhoduje o rozsvícení a zhasnutí v závislosti na úrovni venkovního osvětlení. Jedním z problémů, který nastal při řešení této části práce, bylo zjištění, že vývojářský kit pro technologii IQRF nelze použít jako bránu do internetu a z toho důvodu nelze otestovat nabízené služby cloudového řešení pro tuto technologii.

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 rampy pro jakoukoliv manipulaci se zařízením. Z tohoto důvodu jsem prozkoumal možnost 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. Řešením tohoto problému je instalace přídavné antény, se kterou by vše mělo fungovat. Nevýhodou však je vyšší složitost instalace celého zařízení do dříku sloupu a vyšší cena kompletního řešení.

Poslední částí celé práce byla zjednodušená finanční analýza, jejímž hlavním zjištěním nakonec bylo, že celé zařízení se vyplatí pouze díky svému účelu – zkvalitnění služeb veřejného osvětlení. Z uvedené finanční analýzy vyplynulo, že návratnost této investice by závisela na hromadném využití a sofistikovaném řízení osvětlení v různých oblastech využití. Tímto by došlo ke snížení finančních nákladů, které by souvisely s platbami za spotřebovanou elektrickou energii. Po finanční stránce totiž návratnost může nastat pouze ušetřením za energie.

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

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

[13] 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

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

[15] 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

[16] 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

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

[18] 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

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

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

[21] IQRF Cloud Tech guide. *IQRF.* [online]. [cit. 2017-01-02]. Dostupné z: http://iqrf.org/weben/downloads.php?id=389

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

[23] G6RL datasheet. *Omron.* [online]. [cit. 2017-01-02]. Dostupné z: https://www.omron.com/ecb/products/pdf/en-g6rl.pdf

[24] TWILIGHT SWITCH 2-15.000 LX. *ABB.* [online]. [cit. 2017-01-02]. Dostupné z: https://library.e.abb.com/public/8ca5ef20cb445090c1257c9b003fa8d6/2CSM441034D5601%20-%20T1%20PLUS%20-%20IP65.pdf

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

[26] Gateway GW-ETH-02A. *IQRF.* [online]. [cit. 2017-01-02]. Dostupné z: http://iqrf.org/products/gateways/gw-eth-02a

[27] Anthenna AN-D01.ufl. *IQRF.* [online]. [cit. 2017-01-02]. Dostupné z: http://iqrf.org/products/accessories/antennas/an-d01-ufl

[28] Knoflíková baterie BK-CR2032. *wobchod.* [online]. [cit. 2017-01-02]. Dostupné z: http://www.wobchod.cz/products/detail/BK-CR2032

[29] Držák baterie BK-883. *Battery Holders.* [online]. [cit. 2017-01-02]. Dostupné z: http://www.batteryholders.com/part.php?pn=BK-883&original=CR2032&override=CR2032

[30] Power Relay G6RL-1A DC3. *Digi-Key.* [online]. [cit. 2017-01-02]. Dostupné z: http://www.digikey.com/product-detail/en/omron-electronics-inc-emc-div/G6RL-1A-DC3/Z2762-ND/1679836

[31] BPW34 VISHAY. *GME.* [online]. [cit. 2017-01-02]. Dostupné z: https://www.gme.cz/bpw34-vishay

[32] E-Projects 25EP51415K0 15K Ohm Resistors. *Amazon.* [online]. [cit. 2017-01-02]. Dostupné z: https://www.amazon.com/Projects-25EP51415K0-15K-Resistors-Pack/dp/B01F06T4RS

[33] Kabel H03VVH2-F 2X0,75 bílá. *Sonepar.* [online]. [cit. 2017-01-02]. Dostupné z: http://shop.sonepar.cz/kabel-h03vvh2-f-2×075-bilaplochy/s-1174037/

[34] Krabice F6 IP55. *Sonepar.* [online]. [cit. 2017-01-02]. Dostupné z: http://shop.sonepar.cz/krabice-f6-ip55-rozbocovaci-s-naklapavacim-vickem-90x43x40mm/s-1189024/

[35] 3d print price. *3dprintingpricecheck.* [online]. [cit. 2017-01-02]. Dostupné z: http://3dprintingpricecheck.com/

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

[37] TRITON S. *OMS Lightning.* [online]. [cit. 2017-01-02]. Dostupné z: http://www.omslighting.com/products/type/F23

10 Seznam obrázků

11 Seznam zkratek

ABS	Acrylonitrile Butadiene Styrene
ADR	Adaptive Datarate Algorytm
AES	Advanced Encryption Standard
DBPSK	Differential Binary Phase-Shift Keying
DoS	Denial of Service
EEPROM	Electrically Erasable Programmable Read-Only Memory
GFSK	Gaussian Frequency Shift Keying
GSM	Global System for Mobile communications
GUI	Graphical User Interface
IDE	Integrated Development Environment
IoT	Internet of Things
ITU	International Telecommunication Union
ISM	Industrial, Scientific and Medical
I/O	Input/Output
LDO	Low-Dropout
LED	Light-Emitting Diode
LPWAN	Low-Power Wide Area Network
MAC	Media Access Control address
PHP	Personal Home Page
PLA	Polylactide
p2p	peer-to-peer
RFID	Radio-Frequency IDentification
USB	Universal Serial Bus
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WPA2-PSK	Wi-Fi Protected Access 2 – pre-shared Key

12 Přílohy

Zdrojový kód Koncentrátoru

```
// ******************************************************************************
#include "D:\Plocha\DP_proj\Development\include\IQRF_OS\template-basic.h"
#define RX_FILTER                                   0
// ******************************************************************************


void setCoordinatorMode();
void setNetworkFilteringOn();
void setRoutingOn();

void APPLICATION()
{
        int o_s = 0;
        setCoordinatorMode();
        setNetworkFilteringOn();
        setRoutingOn();

while (1)
{
        sleepWOC();


if (buttonPressed)
{
       PIN = 0;
        DLEN = 4;               //Nastavení délky packetu (počet bytu, které budou odeslány)


        if(o_s==1)                      // Kontrola minulého stavu rozsvícení
        {
                bufferRF[0]=0x30;       // Zhasnutí
                o_s= 0;                 // Nastavení příštího stavu - další stisk tlačítka rozsvítí
        }
        else
        {
                bufferRF[0]=0x31;       // Rozsvícení
                o_s = 1;                // Nastavení příštího stavu - další stisk tlačítka zhasne
        }

                RFTXpacket();           //Odeslání požadované zprávy

                waitDelay(25);

}
```

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

}

}

// *****************************************************************************
#pragma packedCdataStrings 0
#pragma cdata[__EEAPPINFO] =  "0123"
// *****************************************************************************
```

Zdrojový kód pro koncový přijímač

```
// *****************************************************************************
#include "D:\Plocha\DP_proj\Development\include\IQRF_OS\template-basic.h"
#define RX_FILTER                           0
// *****************************************************************************
#define RE5_TRIS            TRISC.5         // C2/IO2 pin connected to the RE2
#define RE5_IO              LATC.5          // Inicializace I/O

void setNodeMode();
void setNetworkFilteringOn();
void setRoutingOn();

void initComparator();
void userIntRoutine(void);

void APPLICATION()
{
        int id_sloup=1;         // ID modulu
        RE5_IO = 0;             // Nastavení počátečních hodnot výstupů pro diodu
        RE5_TRIS = 0;           // Nastavení počátečních hodnot výstupů pro diodu
        setNodeMode();
        setNetworkFilteringOn();
        setRoutingOn();


        initComparator();
        setRFmode(_WPE | _RX_STD | _TX_STD);
        toutRF = 1;             // Wait Packed End active so the toutRF can be set to minimum
        _enableUserInterrupt = 1;
```

```
while (1)                       // Main cycle (perpetually repeated)
{

 if (RFRXpacket())              // If anything was received
{
        copyBufferRF2COM();


        if(bufferCOM[0]==0x30)      // Podmínka kontrolující příkaz od koncentrátoru
                RE5_IO = 0;         // Zhasnutí
        else
                RE5_IO = 1;         // Rozvícení

        PIN = 0;
        DLEN = 2;
        bufferRF[0]= id_sloup;

        if(RE5_IO == 0)
                bufferRF[1]=0;      //návratová hodnota pro koncentrátor - zhasnuto

        else
                bufferRF[1]=1;      //návratová hodnota pro koncentrátor – zhasnuto

        RFTXpacket();           //    Transmit the message
        waitDelay(25);

}
}
}

void initComparator(void)
{
        DACCON0 = 0b10000000;           // DAC on, Vdd, Vss
        DACCON1 = 16;                   // Voltage output (0 - 31), 16 ~ 1,5 V
        TRISA.0 = 1;                    // Pin C1 (RA0) as input
        ANSELA.0 = 1;                   // Pin C1 (AN0) as analog input
        CM2CON0 = 0b10010100;           //Com. on, output internal only, output inverted
        CM2CON1 = 0b11010000;
        C2IF = 0;                       // Clear interrupt flag
        C2IE = 1;                       // Interrupt from Comparator 2 enable
}
// *****************************************************************************
#pragma packedCdataStrings 0
#pragma cdata[__EEAPPINFO] =  "0123"
// *****************************************************************************
```

```
#pragma origin __USER_INTERRUPT
#pragma library 0
void userIntRoutine(void)
{
	if (C2IF)
	{
		C2IF = 0;			// Clear interrupt flag
		if (C2OUT)
		{
			RE5_IO = 0;		// Zhasnutí
		}
		else
		{
			RE5_IO = 1;		// Rozvícení
		}
	}
}
```

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);
        }
}
}
```