

Vysoká škola ekonomická v Praze
Fakulta informatiky a statistiky

Bakalářská práce

Vysoká škola ekonomická v Praze
Fakulta informatiky a statistiky

**Analýza současného stavu a vývoje
infrastruktury internetu věcí**

Vypracoval: Daniel Hájek
Vedoucí práce: Ing. Ladislav Luc
Rok vypracování: 2017

Čestné prohlášení:

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Veškeré použité podklady, ze kterých jsem čerpal informace, jsou uvedeny v seznamu použité literatury a citovány v textu podle normy ČSN ISO 690.

V..... dne

Podpis:

Poděkování:

Touto cestou bych rád poděkoval vedoucímu své bakalářské práce, panu Ing. Ladislavu Lucovi, za umožnění zpracovávat toto zajímavé téma a za metodické vedení v průběhu zpracování práce. Dále bych rád poděkoval své rodině a blízkým za rady a podporu nejen během zpracování této práce, ale i během celého studia.

Abstrakt

Práce se v teoretické části věnuje aktuálnímu fenoménu internetu věcí, vysvětluje tento pojem a nabízí pohled do historie tématu. V druhé části sestavuje ucelený přehled používaných bezdrátových technologií pro přenos dat, včetně nově vyvíjených právě pro internet věcí. Dále analyzuje současný stav pokrytí ve vybraných světových státech a v České republice, včetně odhadu jeho budoucího vývoje. V praktické části je práce zaměřená na popsání vize, jak by mohl vypadat ideální chytrý dům a na navrhnutí implementace reálných chytrých zařízení, pro maximální přiblížení se ideální funkčnosti. Při návrhu je kladen důraz na síťovou infrastrukturu, při použití bezdrátové sítě Zigbee.

Klíčová slova: internet, internet věcí, bezdrátové sítě, LoRa, Sigfox, Zigbee

Abstract

This thesis aims to introduce a phenomenon called the Internet of things (IoT) and its wireless networks, it brings short overview about the topic and it's history. In the next part of the thesis, there is presented a list of currently used wireless networks and they are compared to specialized networks developed for the Internet of things. This part also contains a short analysis of the Internet of things' current network's coverage, the analysis focuses on the countries which are the world's leaders in technology development. These countries are also compared with the Czech Republic. In the practical part of the thesis is introduced a vision of ideal smart house. Afterwards, a project of implementation of smart devices is presented. This project aims at reaching the same attributes as the presented vision. The main part of the project is dedicated to designing a wireless network using the Zigbee standard.

Key words: internet, internet of things, iot, wireless networks, LoRa, Sigfox, Zigbee

Obsah

Seznam obrázků.....	9
Seznam tabulek.....	9
1 Úvod	10
2 Internet věcí.....	10
2.1 Obecné pojmy	10
2.2 Historie.....	12
3 Bezdrátové sítě	14
3.1 Obecné požadavky	14
3.2 Používané technologie	14
3.2.1 6LowPAN	14
3.2.2 Bluetooth.....	14
3.2.3 WiFi	15
3.2.4 Mobilní sítě.....	15
3.2.5 NFC	15
3.3 Sítě určené pro Internet věcí.....	16
3.3.1 Sigfox	16
3.3.2 LoRa Technology	18
3.3.3 LTE-M.....	19
3.3.4 Z-Wave	21
3.3.5 Zigbee	23
3.4 Porovnání síťových technologií	26
3.5 Pokrytí ve světě	27
3.5.1 USA	28
3.5.2 Jižní Korea	29
3.5.3 Západní Evropa	29
3.5.4 Porovnání vývoje ve světě	30

3.6	Pokrytí v České republice	31
4	Návrh praktického využití sítě Zigbee pro realizace chytrého domu	33
4.1	Vize ideálního chytrého domu.....	33
4.2	Použitá zařízení a jejich umístění.....	34
4.2.1	O domě.....	34
4.2.2	Zabezpečení	35
4.2.3	Uživatelský komfort	37
4.2.4	Zábava	38
4.3	Umístění chytrých zařízení	39
4.4	Potřebná infrastruktura	40
4.5	Cena	42
5	Závěr	44
6	Seznam použité literatury	45

Seznam obrázků

<i>Obrázek 2-1: Vývoj počtu vyhledávání výrazu "internet of things" službou Google.....</i>	<i>13</i>
<i>Obrázek 3-1: Pokrytí sítě Sigfox v Evropě</i>	<i>17</i>
<i>Obrázek 3-2: Schéma fungování LoRa sítě v podání Českých radiokomunikací.....</i>	<i>19</i>
<i>Obrázek 3-3: Porovnání různých LTE kategorií.....</i>	<i>20</i>
<i>Obrázek 3-4: Princip komunikace v rámci sítě Z-Wave.....</i>	<i>22</i>
<i>Obrázek 3-5: Schéma vrstev protokolu Zigbee.....</i>	<i>23</i>
<i>Obrázek 3-6: Schéma možných topologií sítě Zigbee.....</i>	<i>25</i>
<i>Obrázek 3-7: Celosvětový počet aktivních, testovaných či budovaných sítí pro Internet věcí letech 2015 a 2016.]</i>	<i>27</i>
<i>Obrázek 3-8: Pokrytí USA sítě Sigfox k 13.4.2017.....</i>	<i>28</i>
<i>Obrázek 3-9: Pokrytí USA sítě LoRa k 13.4.2017.....</i>	<i>28</i>
<i>Obrázek 3-10: Aktuální pokrytí ČR sítě Sigfox.....</i>	<i>32</i>
<i>Obrázek 3-11: Pokrytí ČR sítě LoRa k 17.4.2017.....</i>	<i>32</i>
<i>Obrázek 4-1: Půdorys přízemí modelového domu.....</i>	<i>35</i>
<i>Obrázek 4-2: Půdorys 1. patra modelového domu.....</i>	<i>35</i>
<i>Obrázek 4-3: Pohybový senzor podporující bezdrátovou technologii Zigbee.....</i>	<i>36</i>
<i>Obrázek 4-4: Bezdrátový stmívač světel.....</i>	<i>37</i>
<i>Obrázek 4-5: Multifunkční meteorologický senzor.....</i>	<i>38</i>
<i>Obrázek 4-6: Umístění chytrých zařízení v přízemí.....</i>	<i>39</i>
<i>Obrázek 4-7: Umístění chytrých zařízení v 1.patře.....</i>	<i>39</i>
<i>Obrázek 4-8: Příklad využití topologie.....</i>	<i>40</i>
<i>Obrázek 4-9: Síťová infrastruktura v 1.patře.....</i>	<i>41</i>
<i>Obrázek 4-10: Síťová infrastruktura v přízemí.....</i>	<i>42</i>

Seznam tabulek

<i>Tabulka 3-1: Porovnání bezdrátových sítí.....</i>	<i>26</i>
<i>Tabulka 4-1: Ceny koncových zařízení.....</i>	<i>43</i>
<i>Tabulka 4-2: Celková cena.....</i>	<i>43</i>

1 Úvod

Tato bakalářská práce je zaměřena na problematiku tématu: síťové infrastruktury pro Internet věcí. Internet věcí nebo také Internet of Things (IoT) je souhrnně používané označení pro propojení fyzických objektů každodenní potřeby s internetem, toto propojení umožňuje komunikaci mezi všemi připojenými objekty a/nebo jejich uživateli. Existence zmíněného připojení k internetu umožňuje těmto objektům sbírat a sdílet data, pomocí kterých se za předpokladu správného využití může zlepšovat kvalita našich životů. Hlavním předpokladem pro vznik Internetu věcí ovšem není samotné připojení objektů k internetu, již nyní existuje spousta chytrých zařízení, která jsou k internetu připojena. Podmínkou pro opravdovou existenci Internetu věcí je mnohonásobné zvýšení počtu těchto zařízení oproti současnosti. Podrobnější charakteristice zvoleného tématu, včetně definice používaných pojmů a souhrnu historie, je věnována první kapitola.

Hlavním cílem této práce je provést analýzu současné síťové infrastruktury, používané právě pro objekty Internetu věcí, budované v České republice a jejího předpokládaného vývoje. V rámci tohoto cíle je zpracováno souhrnné porovnání nejvýznamnějších současně používaných bezdrátových technologií a jejich porovnání s nově vyvíjenými sítěmi určenými pro internet věcí. Také je sestaven přehled současného pokrytí těmito sítěmi v nejvyspělejších státech světa a odhad budoucího vývoje tohoto pokrytí. Následuje porovnání se současným stavem a vývojem v České republice.

Dalším hlavním cílem této práce je, v návaznosti na předchozí bod, navrhnout soustavu zařízení pro chytrý dům, která bude efektivně využívat jednu či více ze sítí zmíněných v přechozí části práce. Pojmem chytrý dům je označován dům či byt, ve kterém jsou efektivně integrovány chytrá zařízení, která tak vytvářejí jeden funkční celek. Součástí chytrého domu může být také automatizace různých procesů denní potřeby, jako je například osvětlení, vytápění nebo zabezpečení domu.

2 Internet věcí

2.1 Obecné pojmy

Definice Internetu věcí se může lišit podle pohledu, jakým je k tomuto tématu přistupováno. Ovšem nezávisle na odborné definici lze Internet věcí popsat jako globální síť propojující takzvané chytré objekty a jejich uživatele. Jako chytrý objekt se dá označit jakýkoliv běžný objekt, který při modifikování pomocí relativně malého elektronického zařízení, získá vlastnosti chytrého objektu, jako je právě konektivita k internetu a možnost měnit své

chování na základě získaných informací. Koncept chytrých zařízení se postupně vyvinul z jiné podobné technologie: RFID (radio frequency identification). Tato technologie umožňuje dálkovou identifikaci předmětů za pomoci k nim připojených elektronických zařízení. RFID je v podstatě schopen nahradit například čárové kódy sloužící k jednoznačné identifikaci majetku. Rozvoj technologie RFID a potažmo chytrých zařízení je umožněn především neustálým vývojem na poli elektroniky a miniaturizace. [1 s. 307, 2 s. 247, 3]

Příklad: Běžným příkladem chytrého objektu může být například vytápění domácnosti, toto vytápění může zcela bez problému fungovat jako „hloupé“ kdy pouze udržuje stanovenou teplotu, pokud mu ovšem budou poskytnuty data například o předpovědi počasí, může upravit plán vytápění pro zachování stálé teploty, ale s menšími náklady na energii, v tuto chvíli se z „hloupého“ běžného objektu stává objekt chytrý.

Přínosem Internetu věcí ovšem není samotné propojení objektů s internetem. Již nyní existuje mnoho zařízení, která získávají dodatečná data pro své fungování ze sítě internet. Tímto přínosem je vytvoření sítě, která bude zahrnovat desítky až stovky milionů podobných zařízení, případně i více, a umožní velkoplošný sběr dat i jejich přímé sdílení mezi propojenými subjekty. Tyto data bude možno zpracovávat v mnoha různých odvětvích, jako je například meteorologie nebo zdravotnictví. Současně s takto masivním rozvojem sběru dat nastanou komplikace v jejich přenosu, ukládání a dostatečně rychlém zpracování, rozvoj tzv. Big Data (viz s. 12). [1 s. 308, 3]

Dalším pojmem vyskytujícím se v souvislosti s Internetem věcí se stává označení chytrý dům (nebo též chytrá domácnost). V současnosti se jedná o velmi volně používaný termín, který může označovat od domu s pouhým jednoduchým propojením audiovizuální techniky až po inteligentní domy budoucnosti, které zatím slouží pouze jako vědecké laboratoře. V dnešní době jsou takto nejčastěji označovány domy, kde jsou propojeny elektronické systémy jako je například zabezpečení, vytápění, osvětlení a senzory rozmístěnými v domě a případně na zahradě. Toto propojení umožňuje zavést jednotné ovládání všech součástí chytrého domu. Dále by měla být splněna podmínka propojení domu s venkovním světem a tím umožněné dálkové ovládání některých jeho součástí, výhodou propojení s vnějším světem je také možnost získávání informací například o předpovědi počasí a na základě těchto informací upravit činnost zavlažování na zahradě nebo jiné funkce domu. [4 s. 1-2]

Pro využití Internetu věcí v průmyslu se mnohdy používá označení jako 4. průmyslová revoluce, nebo také Průmysl 4.0. V praxi to znamená, že se nynější automatizovaná výroba

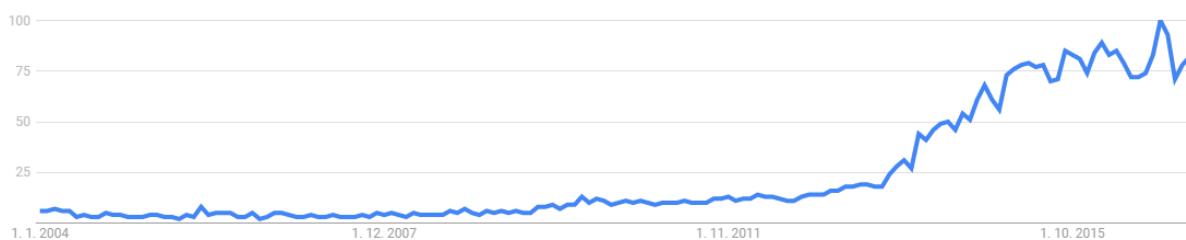
stane plně integrovaná a sama sebe optimalizující na základě údajů z propojených výrobních strojů a senzorů, velice pravděpodobně se hranice sdílených dat neomezí pouze na jednu konkrétní firmu, ale budou sdíleny minimálně v rámci celých koncernů. Pod Průmyslem 4.0 je také zahrnuto implementování chytrých funkcí do běžných výrobků a celková jejich příprava pro propojení se zbytkem Internetu věcí. [5 s. 16]

V souvislosti s rozvojem Internetu věcí a internetu obecně, a samozřejmě nejenom díky tomu, získává na popularitě také fenomén známý jako Big Data. Jedná se o tak velká data, které není možno zpracovávat pomocí běžných databázových nástrojů. Hlavními kritérii pro označení běžných dat jako Big Data je velikost v desítkách až stovkách terabytů a nízká strukturovanost dat. Big Data fungují jako podpůrná data podniku pro rozhodování vedle běžných dat, pro jejich zpracování se dají využít nestrukturované databáze (NoSQL) a specializované programy využívající distribuované výpočty, jako je například aplikace Apache Hadoop. Využití distribuovaného výpočtu znamená rozdělení velkého množství dat na menší snáze zpracovatelné části a jejich následné zpracování na více různých počítačích. [6, 7]

2.2 Historie

Již od vzniku předchůdce dnešního Internetu, ARPANETu (Advanced Research Projects Agency NETwork) v roce 1969, který původně vznikl jako experimentální síť americké agentury DARPA (Defense Advanced Research Projects Agency), jejímž cílem bylo zajistit funkční počítačovou síť i v případě vojenského útoku a vyřazení některého z přenosových uzlů. V následujících letech stále stoupal počet připojených zařízení do této sítě, aby v roce 1990 při ukončení projektu ARPANET již přesahoval sto tisíc připojených počítačů. V roce 1991 byla v laboratoři CERN (Conseil Européen pour la recherche nucléaire) spuštěna první webová stránka, a tím vznikl internet v podobě v jaké ho známe nyní. Během následujících let byly postupně připojovány jednotlivé země, Československo v roce 1992, aby v roce 1996 dosahoval již 55 miliónů připojených zařízení na celém světě. V dalších letech Internet dosahoval téměř exponenciální expanze a v roce 2010, i za pomoci rozvoje chytrých zařízení, přesahoval počet připojených zařízení 2 miliardy. Za první chytré zařízení a součást Internetu věcí, ačkoliv toto pojmenování vzniklo až o několik let později, je považován toustovač, který v roce 1990 vytvořil John Romkey. Po připojení toustovače k počítači pomocí TCP/IP dokázal Romkey vzdáleným ovládáním toustovač zapnout. Samotný pojem Internet věcí vznikl v roce 1999, kdy jeden ze zakladatelů Auto-ID Center Kevin Ashton tento pojem použil jako název své prezentace. Ve stejném roce došlo také k zavedení EPC (Electronic Product Code), který slouží jako jednoznačný elektronický

identifikátor fyzického objektu, založený na technologii RFID. V roce 2000 společnost LG představila první chytré zařízení do domácnosti. Jednalo se o chytrou ledničku, která měla sledovat zásoby potravin a rozhodovat, zda je potřeba danou potravinu koupit nebo ne. Tento výrobek se ovšem nestal populárním mezi zákazníky především z důvodu vysoké ceny a příliš malého přínosu. V letech 2003 a 2004 došlo k prvním markantnějším zmínkám o Internetu věcí v mainstreamových médiích a vědeckých publikacích, zároveň společnost Walmart poprvé ve velké míře nasadila technologii RFID. V roce 2005 byl Internet věcí poprvé zmíněn ve zprávě Mezinárodní komunikační unie a mezi lety 2006 až 2008 se k tomuto připojila také Evropská unie uspořádáním první evropské konference zaměřené na Internet věcí. V letech 2008 až 2009 překročilo množství připojených zařízení počet uživatelů, do roku 2010 dokonce dosáhl počet připojených zařízení 12,5 miliardy, ve stejném roce počet obyvatel Země dosahoval pouze 6,8 miliardy lidí, tedy na jednoho člověka připadala téměř dvě připojená zařízení. Podle společnosti Cisco lze toto pokládat za zrození Internetu věcí, tomuto odpovídá i rostoucí zájem veřejnosti o vyhledávání pojmu Internet věcí (viz. obrázek 2-1). Ve stejném roce byla také oblast Internetu věcí označena čínským premiérem za klíčovou a byl připraven plán investic do jejího rozvoje. Dalším technologickým milníkem umožňujícím rozvoj Internetu věcí, bylo veřejné spuštění IPv6 adres, které nastalo v roce 2011. Ve stejném roce došlo totiž k přidělení posledních volných bloků IPv4 adres, které byly využívány od roku 1981 a bylo je třeba nahradit. Nastupující IPv6 nabízí 2^{128} možných kombinací, oproti pouhým 2^{32} v případě IPv4 adres, lze tedy předpokládat, že zásoba adres bude dostatečná i pro budoucí prudký rozvoj Internetu věcí. [8, 9]



Obrázek 2-1: Vývoj počtu vyhledávání výrazu "internet of things" službou Google. [8]

3 Bezdrátové sítě

3.1 Obecné požadavky

Pro využití v oblasti Internetu věcí se hodí některé již běžně používané technologie jako je například WiFi, Bluetooth nebo GSM. Ovšem k vzhledem ke specifickým požadavkům, které klade Internet věcí na tyto sítě, vznikají také zcela nové standardy. Mezi tyto požadavky lze zařadit například snahu o snížení energetické náročnosti na připojená zařízení, zvyšování dosahu jednotlivých sítí nebo naopak zde není taková náročnost na rychlost datového přenosu.

3.2 Používané technologie

3.2.1 6LowPAN

6LowPAN (IPv6 over Low-power wireless Personal Area Network) je síťový protokol definující zapouzdření a kompresy hlavičky, které umožňuje přijímání a odesílání IPv6 paketů přes IEEE 802.15.4 (standard definující nízko energetické osobní sítě). Největší výhodou 6LowPAN je možnost využití tohoto standardu na různých platformách od WiFi (5 GHz) až po sítě fungujících na frekvencích pod 1 GHz. [10, 11]

Standard: RFC6282

Frekvence: od méně jak 1GHz až po 2,4GHz

3.2.2 Bluetooth

Jedná se o běžně používaný protokol rozšířený především u mobilních telefonů a nositelné elektroniky, lze předpokládat, že toto využití bude převažovat i v budoucnu. Nejnovější verze Bluetooth je označována jako Bluetooth Low Energy (BLE) nebo také Bluetooth Smart, tato verze se vyznačuje podobnými vlastnostmi jako původní Bluetooth, ale s mnohem menší energetickou náročností, tedy s lepšími vlastnostmi pro využití v rámci Internetu věcí. V nejnovější verzi (5.0) je zde také umožněn přímý přístup do sítě internet pomocí 6LowPAN. [10, 12]

Frekvence: 2.4GHz

Dosah: max. 150m

Přenosová rychlost: 1Mb/s

3.2.3 WiFi

WiFi je momentálně nejrozšířenější řešení pro bezdrátové sítě přenášející velké objemy dat, proto je také jednou z nejčastějších voleb při připojování chytrých zařízení k internetu. WiFi momentálně nabízí největší přenosové rychlosti, ale je velmi limitována svým dosahem a energetickou náročností. I přes tyto nedostatky je WiFi nejpoužívanější volbou při tvorbě chytrých domácností, protože se zde nemusí složitě řešit energetická výdrž zařízení, drtivá část dnešních chytrých domácností je totiž připojena do elektrické sítě. Momentálně používaným standardem pro WiFi je 802.11ac, ale nejrozšířenější je zatím stále starší 802.11n. [10]

Frekvence: 2.4GHz/5GHz

Dosah: cca 50m

Přenosová rychlost: 150-200MB/s (802.11n), až 1GB/s (802.11ac)

3.2.4 Mobilní sítě

Díky svému vysokému dosahu se mobilní sítě nabízejí jako ideální řešení pro připojení chytrých zařízení na velkou vzdálenost. U nejmodernějších sítí čtvrté generace (LTE) také nabízejí přenosové rychlosti srovnatelné se staršími WiFi standardy. I přes tyto výhody se ovšem ukazuje, že připojení pomocí mobilních sítí je příliš nákladné jak po energetické, tak finanční stránce. [10]

Standardy: GSM/GPRS/EDGE (2G), HSPA (3G), LTE (4G)

Frekvence: 900/1800/1900/2100MHz

Dosah: 35 km(GSM), 5 km (LTE)

Přenosová rychlost: 35-170 kb/s (GPRS), 120-384 kb/s (EDGE), 384 Kb/s -2 Mb/s (UMTS), 600 kb/s-10 Mb/s (HSPA), 3-100 Mb/s (LTE)

3.2.5 NFC

NFC (Near Field Communication) umožňuje jednoduchou komunikaci mezi dvěma zařízeními na krátkou vzdálenost, vzhledem k malému dosahu NFC nelze tuto komunikaci jednoduše zachytit a zneužít. Hlavní využití této technologie nachází především v bezkontaktních platbách, například pomocí chytrého telefonu, nebo ve sdílení digitálního obsahu mezi dvěma zařízeními. [10, 13]

Standard: ISO/IEC 18000-3

Frekvence: 13.56 MHz

Dosah: 10 cm

Přenosová rychlost: 100–420 kb/s

3.3 Sítě určené pro Internet věcí

Následující sítě jsou vyvíjeny přímo pro využití v rámci Internetu věcí, neznámá to, že by výše zmíněné standardy nebyly využitelné pro Internet věcí, ale specializované sítě je budou postupně vytlačovat.

3.3.1 Sigfox

Sigfox je síť vyvinutá stejnojmennou francouzskou společností, prvotním cílem této společnosti bylo se stát světovou jedničkou v nabízení připojení pro chytrá zařízení. Avšak po čase společnost od tohoto cíle upustila a mimo domovskou Francii, kde síť sama provozuje, se vydala cestou partnerství se stávajícími mobilními operátory (např. i s českým T-Mobilem). Síť Sigfox se řadí mezi LPWAN (Low Power Wide Area Network), tedy sítě určené na velkou vzdálenost s nízkými energetickými nároky. A v rámci této kategorie lze Sigfox zařadit do podkategorie využívající velmi úzkého frekvenčního pásma. Konkrétně v Evropě jde o bezlicenční pásmo 868Mhz oproti v USA využívanému pásmu 915MHz. Celá síť je velmi výrazně přizpůsobena nízké energetické náročnosti, nejprve byla dokonce vyvíjena jako jednosměrná síť, umožňující koncovým zařízením pouze odesílání dat, avšak v průběhu vývoje byla síť upravena na obousměrnou. Vedle využitého frekvenčního pásma jsou nárokům na nízkou spotřebu energie přizpůsobena také koncová zařízení, tedy konkrétně chování těchto zařízení. Pomocí sítě Sigfox je umožněno přenášet pouze velmi malé objemy dat (do 12 bytů při jednom odeslání) maximálně 144x za den a zprávy jsou přenášeny velmi pomalu, tímto způsobem je umožněn přenos na vysokou vzdálenost (až 80 km). Dále musí být koncová zařízení přizpůsobena specifickému přijímání dat ze sítě, zařízení totiž obvykle nejsou připojena trvale, ale pouze v určitých časových blocích, většinou po odeslání zprávy ze samotného zařízení. Jeden přístupový bod může za den odeslat maximálně 9 000 000 zpráv, což je dáno regulací využívaného pásma, a disponuje vysílacím výkonem 25 mW / 14 dBm. [14, 15, 16, 17]

Identifikace zařízení v síti Sigfox neprobíhá pomocí klasických IP adres nebo SIM karet, ale každé zařízení, či jeho síťový modul, má přidělený unikátní identifikátor, pomocí kterého je adresovatelné v rámci sítě. Samotná komunikace se zařízením probíhá pomocí aplikace výrobce, které se k nim připojuje pomocí rozhraní (API) Sigfoxu. Zabezpečení přenášených

dat je možné rozdělit do několika různých fází. Samotný přenos mezi koncovými zařízeními a přístupovými body je zabezpečen pomocí unikátního klíče, kterým každé zařízení podepisuje odeslaná data. Pomocí tohoto podpisu lze odhalit případné pozměnění informace třetí osobou (Man in the Middle Attack). Zabezpečení informace proti ztrátě při přenosu či rušení je provedeno pomocí odesílání každé informace třikrát na náhodné frekvenci a její přijetí pomocí všech přístupových bodů v dosahu. Následující přenos mezi přístupovými body a cloudem Sigfoxu je realizován pomocí zabezpečené VPN, samotné připojení koncového uživatele ke cloudu probíhá přes HTTPS. V současné době síť Sigfoxu pokrývá, či se buduje, ve 32 zemích na rozloze 1.9 miliónů čtverečních kilometrů a na tomto území žije přes 512 miliónů obyvatel (viz. obrázek 3-1). [15, 17,18]

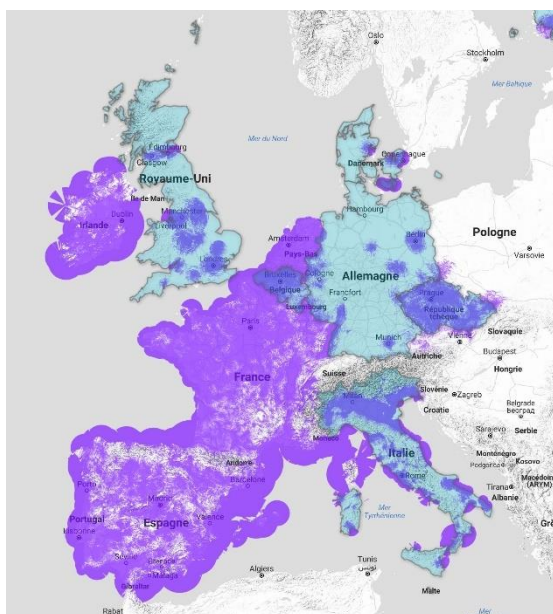
Zařízení kompatibilní se sítí Sigfox vyrábí spousta různých výrobců a cena za Sigfox modul se pohybuje velmi nízko, maximálně v jednotkách euro. Při využití současných technologií v oblasti baterií mohou tato zařízení vydržet v provozu zhruba 5 až 15 let bez připojení do elektrické sítě, spotřeba zařízení při vysílání se totiž pohybuje většinou mezi 5mA až 45mA. Cena za připojené zařízení je řešena pomocí ročního předplatného a podle počtu zařízení vychází na 0,1 až 1 euro za rok a zařízení. [15, 17]

Standard: Sigfox

Frekvence: 900MHz

Dosah: 30-50 km (ve volném terénu), 3-10 km (ve městě)

Přenosová rychlost: 100 b/s



Obrázek 3-1: Pokrytí sítě Sigfox v Evropě. [19]

3.3.2 LoRa Technology

LoRa Technology označuje dvě technologie, které jsou vyvíjené LoRa Alliance. První z nich je LoRa (long range) modulace signálu, patentovaná firmou Semtech. Tato modulace rozprostírá signál podobně jako jiné po celém kanálu. Hlavním rozdílem oproti jiným modulacím signálu je ovšem lineární změna kmitočtu na místo skokové, toto zvyšuje odolnost oproti Dopplerovu jevu a snižuje nároky na vysílač. Dopplerův jev označuje změnu vlnové délky na základě vzájemného pohybu vysílače a přijímače. LoRa modulace umožňuje využít automatického nastavení přenosové rychlosti, kdy je automaticky zvolena nejvyšší přenosová rychlost na základě naměřeného signálu, je to vhodné především pro stacionární aplikace. [20]

Druhou vyvíjenou technologií je LoRaWAN, jedná se o obousměrný síťový protokol vhodný pro použití především pro Internet věcí. Stejně jako Sigfox využívá LoRaWAN nelicencované přenosové pásmo pod 1 GHz konkrétně v Evropě tedy 868 MHz a ve Spojených státech 915 MHz. V Evropě je typicky používáno 8 přenosových kanálů, z toho 3 hlavní, oproti tomu v USA je používáno až 72 kanálů pro odesílání a 8 kanálů pro přijímání dat. Zabezpečení je realizováno pomocí symetrické šifry AES, kdy každé zařízení disponuje dvěma klíči o délce 128 bitů. Jeden z klíčů je určen pro šifrování v rámci přenosu mezi zařízením a přístupovým bodem, druhý je určen pro zabezpečení samotného přenosu mezi sítí a uživatelskou aplikací. [20, 21]

Zařízení připojená do sítě LoRa jsou rozdělena do tří kategorií - A, B a C. Kategorie A označuje zařízení napájená pomocí baterie, je u nich tedy kladen velký důraz na šetření energie. Z těchto důvodů nemůže server iniciovat přenos dat do nebo z koncového zařízení. Přenos je vždy iniciován z koncového zařízení a zprávy jsou odesílány pouze jednou a v poměrně dlouhých časových prodlevách. Příjem zpráv do koncového zařízení probíhá pouze v předem stanovených intervalech. Zařízení kategorie B se podobně, jako kategorie A, vyznačují snahou o úsporu energie, ale oproti kategorii A mohou tato zařízení odesílat každou zprávu vícekrát, pro minimalizaci možnosti ztráty dat, a příjem dat koncovým zařízením probíhá v častějších intervalech než u kategorie A. Některá zařízení také podporují probuzení pro přenos dat pomocí pingu ze serveru. Zařízení kategorie C disponují neustálým připojením k síti (vhodné pouze pro zařízení s trvalým napájením), je u nich tedy možné kdykoliv iniciovat přenos pokynem ze serveru. Každé zařízení, z jakékoliv kategorie, musí pro připojení do sítě LoRa disponovat unikátním 32 bitovým identifikátorem a dvojicí 128 bitových klíčů. Zařízení může být těmito informacemi vybaveno již při výrobě, nebo musí proběhnout vzdálená aktivace, kdy server tyto informace zařízení přidělí. Vzdálená

aktivace probíhá na základě zaslání informace, k jaké aplikaci dané zařízení patří a ověření pomocí AES klíče dané aplikace. Na základě těchto informací server zařízení přidělí v rámci sítě unikátní identifikátor a dvojici klíčů, které bude využívat při komunikaci s přístupovými body potažmo serverem. [21, 22]

Data ze zařízení v síti LoRa se odesílají na cloudové úložiště provozovatele sítě, ke kterému mají uživatelé přístup pomocí zákaznické aplikace. Zákaznická aplikace k datům přistupuje přes API provozovatele sítě, takže zákazník není zatížen nutností ukládat všechna data z koncových zařízení, ta zůstávají na serverech provozovatele (viz. obrázek 3-2). [23]

Standard: LoRaWAN

Frekvence: 868 MHz (Evropa), 915 MHz (USA)

Dosah: 15 km (ve volném terénu), 2-5 km (ve městě)

Rychlost: 100 kb/s



Obrázek 3-2: Schéma fungování LoRa sítě v podání Českých radiokomunikací. [23]

3.3.3 LTE-M

LTE-M je obecné označení LPWAN sítí fungujících na základě klasického LTE, jedná se ale o mnohem méně komplexní síť než výchozí LTE. LTE Cat-0 (Release 12) využívající šířku pásma 20 MHz, LTE Cat-M1 (Release 13), která funguje v pásmu o šíři již jen 1,4 MHz, případně přímo úzkopásmová NB-IoT síť využívající pásmo o šířce pouze 180 KHz. (viz. obrázek 3-3) Využívání užších přenosových pásem umožňuje snížit energetickou náročnost a celkovou technologickou náročnost na koncová zařízení, jelikož využívají právě užší přenosové pásmo a nejsou závislé na neustálé obousměrné komunikaci. Odhady

předpokládají až 90% pokles nákladů na koncová zařízení oproti klasickému širokopásmému LTE. Za další velkou výhodu můžeme považovat skutečnost, že úzkopásmovou síť lze provozovat i na dosud nevyužívaných hraničních frekvencích, neubírá tedy prostor z vyhrazené frekvence pro provoz běžných mobilních sítí. [24, 25]

	LTE Rel-8 Cat-1	LTE Rel-12 Cat-0	LTE Rel-13 Cat-M1	NB-IoT Rel-13
DL peak rate	10 Mbps	1 Mbps	1 Mbps	~0.2 Mbps
UL peak rate	5 Mbps	1 Mbps	1 Mbps	~0.2 Mbps
Duplex mode	Full	Half or full	Half or full	Half
UE bandwidth	20 MHz	20 MHz	1.4 MHz	0.18 MHz
Maximum transmit power	23 dBm	23 dBm	20 or 23 dBm	23 dBm
Relative modem complexity	100%	50%	20-25%	10%
Note: peak data rates refer to full duplex operation for Cat-0 and Cat-M1				

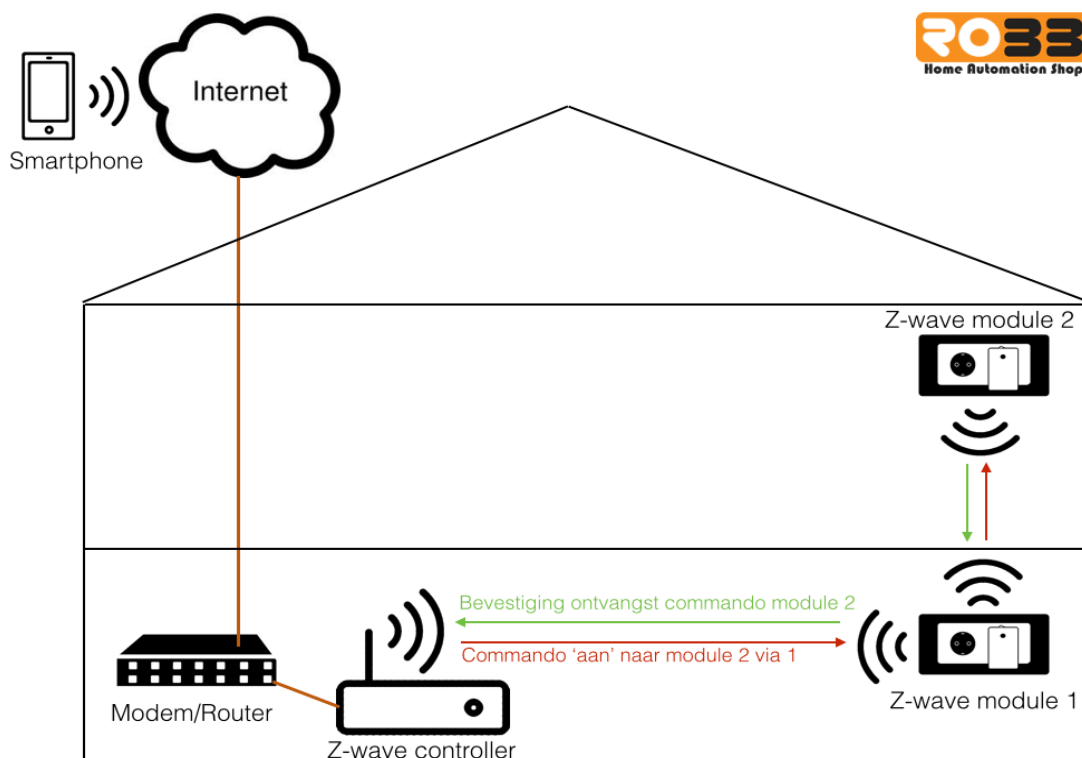
Obrázek 3-3: Porovnání různých LTE kategorií. [25]

Vývoj LTE-M lze označit jako reakci některých klasických mobilních operátorů na rozvoj nových sítí (Sigfox, LoRa a dalších), především z důvodu poměrně snadné modernizace stávající mobilní infrastruktury na LTE-M. Nynější LTE síť totiž není možné příliš efektivně využít pro připojení velkého množství zařízení Internet věcí, protože většina z těchto zařízení nepotřebuje přenášet příliš velké objemy dat, což je hlavní přednost LTE. Hlavní nevýhodou LTE je naopak velká energetická náročnost pro koncová zařízení a relativně vysoké poplatky za připojené zařízení, tedy zbytečná platba za nevyužitelnou rychlost připojení. LTE-M tedy operátorům umožní nabídnout ceny schopné konkurovat i jiným sítím Internetu věcí. 3GPP (The 3rd Generation Partnership Project), sdružení technologických firem pracujících na vývoji nových telekomunikačních standardů, si ve specifikacích LTE Cat-M1 (Release 13) dalo za úkol dosáhnout následujících cílů: snížit energetické nároky natolik, aby zařízení s 5WH baterií vydrželo v provozu zhruba 10 let, snížit cenu koncových zařízení na porovnatelnou s cenou zařízení pro GPRS, dosáhnout vyššího pokrytí z jednoho koncového bodu, než nabízejí jiné sítě (> 156dB), umožnit zařízením variabilní přenosovou rychlost. Nicméně prozatím je možné LTE-M považovat za stále se rozvíjející technologii, která se dočká svého masivnějšího nasazení v průběhu roku 2017. [24, 25]

3.3.4 Z-Wave

Z-Wave je dalším síťovým protokolem, určeným především pro připojení chytrých zařízení v rámci domácnosti. Na rozdíl od sítí Sigfox, LoRaWAN či LTE-M, se ale nejedná o síť typu WAN (Wide Area Network) ale typu PAN (Personal area network), oproti těmto sítím nabízí několika násobně nižší dosah, maximálně cca 40 m (dokonce pouze zhruba 30 m u starší generace čipů). V ohledu dosahu je Z-Wave srovnatelný tedy například s Bluetooth nebo WiFi. Z-Wave funguje, obdobně jako Sigfox nebo LoRaWAN, na nelicencovaném vysílacím pásmě, v Evropě, Číně a Jižní Koreji je to konkrétně 868,4 MHz a v USA 908,4 MHz, není tedy rušen například domácími Wi-Fi sítěmi, které fungují na frekvenci 2,4 GHz. [26, 27, 28]

Síť Z-Wave využívá smíšenou (MESH) topologii, která umožňuje všem zařízením komunikovat jak s routerem, tak mezi zařízeními samotnými, tímto lze dosáhnout navýšení efektivního dosahu sítě až zhruba na 150 m (viz. obrázek 3-4). Maximální přenosová rychlost může dosáhnout až 100 kbit/s, ale běžně dosahované rychlosti se pohybují zhruba jen kolem 40 kbit/s (dokonce pouze necelých 10 kbit/s u starší řady čipů). Ovšem pro posílání dat z koncových senzorů a řídicích informací pro chytrá zařízení je tato rychlost dostačující. Pomocí jednoho routeru může být do sítě připojeno maximálně 232 zařízení, v případě potřeby lze propojit více routerů a tím dosáhnout většího množství připojených zařízení. Každému řídicímu prvku sítě je výrobcem přidělen 32 bitový identifikátor (není možné jej změnit) a v rámci sítě je každému zařízení přidělen také 8 bitový identifikátor (musí být unikátní v rámci jedné sítě). Zařízení jsou schopna komunikovat pouze s dalšími zařízení se shodným síťovým identifikátorem. Pro spojení mezi sítěmi je potřeba připojit speciální modul, který to umožní. [26, 27, 28]



Obrázek 3-4: Princip komunikace v rámci sítě Z-Wave. [31]

Zabezpečení sítě Z-Wave se obecně zakládá pouze na unikátním síťovém 32 bitovém identifikátoru a 8 bitovém identifikátoru koncových zařízení, bez kterých se nelze k daným zařízením připojit. Ovšem tyto identifikátory se dají poměrně snadno zjistit odposloucháváním síťového provozu. Jednotlivá koncová zařízení totiž poměrně často komunikují s řídicí jednotkou (například hlásí stav baterií). V minulosti už se také vyskytlo několik případů, naštěstí zatím jen v testovacím prostředí, kdy se pomocí napadení sítě podařilo fyzicky poškodit koncová zařízení. Například zničení dálkově ovládaného světla pomocí neustálého vypínání a zapínání zabralo při pokusu mezi čtyřmi až devíti hodinami. Další možností pro zabezpečení přenosu mezi zařízeními je využití symetrického šifrování standardu AES. Využití šifrování ale není v síti vynuceno a záleží pouze na tvůrci samotného zařízení, zda se šifrování rozhodne využít a velká část zařízení ho bohužel tedy nepodporuje. V případě použití šifrovaného spojení je potřeba, aby při prvotní instalaci zařízení do sítě proběhla výměna 128 bitových klíčů mezi řídicí jednotkou a daným zařízením. Tato výměna klíčů se sice jeví poměrně zranitelná, ale klíč je při přenosu šifrován pomocí dočasného kódu nastaveného výrobcem řídicí jednotky. Ačkoliv by se toto dočasné šifrování dalo prolomit a tím získat přístup k šifrovacímu klíči, nejeví se tento fakt jako příliš rizikový, protože k přenosu klíče dochází pouze při prvotní instalaci zařízení (nebo při obnovení řídicí jednotky do továrního nastavení) a útočník by musel v daný okamžik

odposlouchávat síťovou komunikaci. Pro ochranu při výměně klíče umožňují také Z-Wave zařízení dočasně snížit vysílací výkon a tím útočnickovi znesnadnit potencionální odchycení klíče. [29, 30]

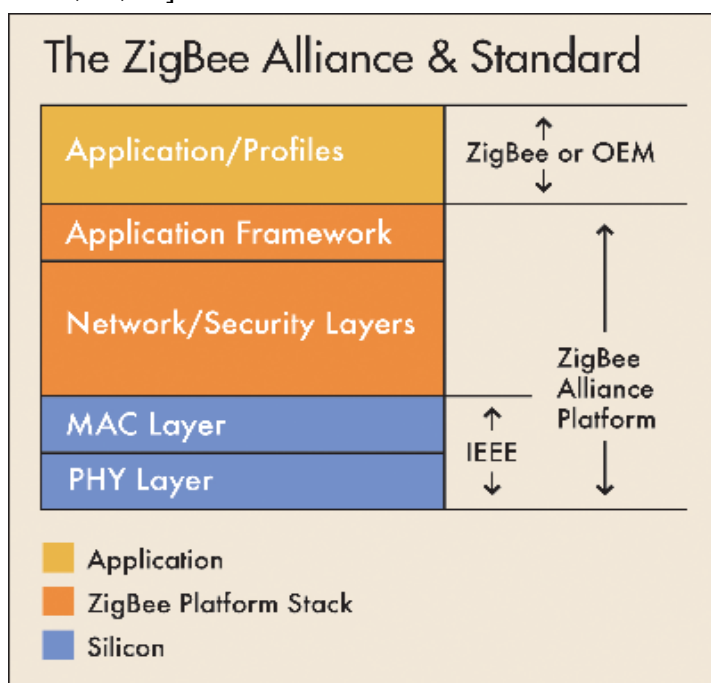
Frekvence: 868 - 910 MHz

Dosah: 40 m

Rychlost: 100 kb/s

3.3.5 Zigbee

Zigbee lze označit za potencionálně nejhlavnějšího konkurenta k výše zmíněné Z-Wave. Je vyvíjen uskupením předních technologických firem (Samsung, Phillips, Cisco a mnoho dalších) sdružených do Zigbee Alliance založené v roce 2002 a podobně jako Z-Wave funguje na nelicencovaných pásmech 868 MHz, 915 MHz ale také 2,4 GHz. Standard Zigbee je postaven na základech protokolu IEEE 802.15.4 (fyzická vrstva) a všechna Zigbee zařízení jsou tedy kompatibilní i s tímto protokolem. V porovnání s jinými sítěmi fungujícími na frekvenci 2,4 GHz jako je třeba Bluetooth nebo WiFi (IEEE 802.11b) nabízí Zigbee mnohem menší nároky na koncová zařízení, jak v oblasti energetické náročnosti, tak výpočetních nároků na použitý čip, tímto se vyrovná sítím fungujícím na frekvencích do 1 GHz (LoRa, Sigfox). Pro zpracování přenosu přes síť Zigbee stačí již velice jednoduchý 8-bitový čip s 30 kB pamětí a předpokládaná výdrž při provozu na baterie se odhaduje na jednotky let. [32 s. 1-3, 33, 34]

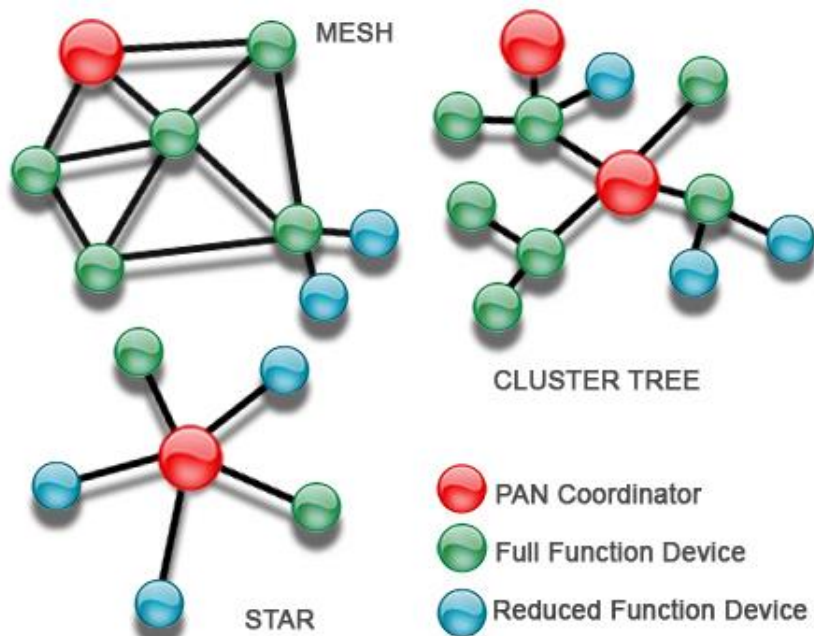


Obrázek 3-5: Schéma vrstev protokolu Zigbee. [35]

Standard Zigbee je rozdělen do několika vrstev, kde každá vrstva zajišťuje specifickou část přenosu, při změně v požadavcích na protokol, tedy není třeba upravovat celý protokol ale stačí upravit příslušnou vrstvu. Konkrétně je zde využito tří vrstev (viz. obrázek 3-5), kdy první vrstva je definována přímo standardem IEEE 802.11b, který určuje fyzickou a MAC (Medium Acces Layer) část. Fyzická část je zodpovědná za samotný způsob vysílání, modulaci signálu a užití frekvenční pásmo. MAC část zajišťuje komunikaci mezi fyzickou vrstvou a sítíovou (NWK) vrstvou. NWK vrstva, tentokrát už samotného Zigbee, odpovídá za zabezpečení sítě a směrování signálu, koncové zařízení nemůže zjistit ideální cestu signálu a je to tedy v režii routeru. Při zakládání nové sítě je NWK vrstva hlavního routeru (koordinátoru) odpovědná za zvolení topologie a přidělení NWK adresy ostatním zařízením. Nejvyšší vrstva, označována jako aplikační, na této vrstvě jsou spuštěny samotné aplikace definující chování daného zařízení. Na jedné aplikační vrstvě může být spuštěno až 240 různých aplikací. Zigbee nabízí pro vývoj zařízení také takzvané aplikační profily, tyto profily umožňují kompatibilitu zařízení jiných výrobců, používajících stejný aplikační profil. [32 s. 5-6 a 17-22, 33]

Zigbee zařízení se dělí na dva typy, prvním je takzvané zařízení s plnou funkcionalitou, které může komunikovat jak s routerem, tak s ostatními zařízeními. Druhá kategorie zařízení je označována jako zařízení s omezenou funkcionalitou, tato zařízení mohou komunikovat pouze se zařízeními s plnou funkcionalitou, ale je výrazně snížena náročnost na jejich výpočetní výkon a spotřebu energie. Zařízení s plnou funkcionalitou je tedy v rámci Zigbee sítě možné využít jako hlavní router, koncové zařízení s funkcionalitou routeru nebo pouhé koncové zařízení, zatímco zařízení s omezenou funkcionalitou lze využít pouze jako koncové zařízení. V závislosti na tomto rozdělení zařízení, je možné využít různých topologií při vytváření Zigbee sítě (viz. obrázek 3-6). První z těchto topologií je hvězda, kde jedno zařízení slouží jako řídicí router a ostatní zařízení komunikují pouze s tímto zařízením. Další možnou topologií je takzvaná smíšená topologie, která je tvořena pouze zařízeními s plnou funkcionalitou a umožňuje tedy všem zařízením v síti komunikovat mezi sebou. Při využití pouze menšího počtu zařízení s plnou funkcionalitou, je také možné vytvořit topologii typu strom, kde řídicí router komunikuje s dalšími routery a ty pak komunikují s koncovými zařízeními, tímto lze efektivně zvýšit dosah sítě oproti hvězdě, za využití méně výkonných zařízení než u smíšené topologie. Také je možné tyto topologie kombinovat a vytvořit síť, kde některá zařízení komunikují mezi sebou a některá slouží jako pouhé koncové body. Tato rozmanitost umožňuje využít síť Zigbee například v rozmanitém prostředí s velkým množstvím překážek, které nepropouští signál, pomocí předávání dat mezi jednotlivými zařízeními můžeme překážky jednoduše obejít správným umístěním zařízení. Zařízení

s plnou funkcí mohou totiž sloužit jako jednoduché opakovače, pouze předávající signál dále. Jedinou nevýhodou tohoto postupu je zvyšování prodlevy mezi odesláním signálu a jeho obdržetím cílovým zařízením. [32 s. 9-11, 33, 34]



Obrázek 3-6: Schéma možných topologií sítě Zigbee. [36]

Identifikace zařízení v síti probíhá pomocí unikátního identifikátoru o délce 16 nebo 64 bitů, zvolení požadované délky identifikátoru provádí administrátor při instalaci sítě. Využití 16 bitového identifikátoru umožňuje snížit nároky na paměť zařízení a délku přenášené zprávy, ovšem může být limitujícím faktorem pro připojení velkého počtu zařízení do jedné sítě. Oproti tomu 64 bitový identifikátor umožňuje v podstatě neomezenou velikost sítě (2^{64} potenciálních zařízení). Komunikace se zařízením v jiné síti je možné pomocí spojení identifikátoru zařízení a identifikátoru samotné sítě, které je přidělena řídicímu routeru při založení sítě. Zabezpečení přenášených zpráv je realizováno pomocí symetrického AES šifrování s délkou klíče 128 bitů. Samotné šifrování může být prováděno na dvou vrstvách protokolu Zigbee, základní zabezpečení je uskutečňováno přímo na síťové vrstvě za využití 128 bitů dlouhého klíče, který je společný všem zařízením v síti a je obvykle přidělen zařízením již při instalaci sítě. Toto slouží jako primární zabezpečení proti odposlouchávání síťové komunikace. Většina Zigbee zařízení umožňuje držet v paměti více těchto klíčů, ale pouze jeden může být v daný okamžik aktivní. Další část zabezpečení je realizována v aplikační vrstvě zařízení, tento klíč je většinou sdílený pouze mezi dvěma zařízeními a k jeho ustanovení dochází obvykle přenosem při prvotním připojení zařízení do sítě. Hlavním předpokladem zabezpečení Zigbee sítě, je bezpečné uložení samotných klíčů a šifrování veškerého přenosu. Ovšem při připojení nového zařízení do sítě může dojít ke

krátkodobému nezašifrovanému přenosu samotného klíče do nového zařízení, toto je potencionálně velmi rizikové, protože zachycení klíče útočníkem může poskytnout přístup k veškeré komunikaci v této síti. Tento okamžik nezašifrovaného přenosu klíče je relativně krátký, ale útočník může za pomoci různých metod (např. rušení daného zařízení a tím simulovat špatnou funkčnost zařízení) přimět uživatele k obnovení zařízení do továrního nastavení a tím vynutit tento přenos. Dalším riziko je pokud se útočník fyzicky zmocní některého ze zařízení připojených do sítě. Podstata většiny těchto zařízení totiž neumožňuje poskytnout dostatečnou odolnost proti získání klíče ze samotného zařízení a toto může vyústit ve stejný problém jako je odchycení klíče při přenosu. [32 s. 22-23, 37 s. 2-3]

Frekvence: 868 - 915 MHz / 2,4 GHz

Dosah: 75 m

Rychlost: 250 kb/s

3.4 Porovnání síťových technologií

Tabulka 3-1: Porovnání bezdrátových sítí. [zdroj: autor]

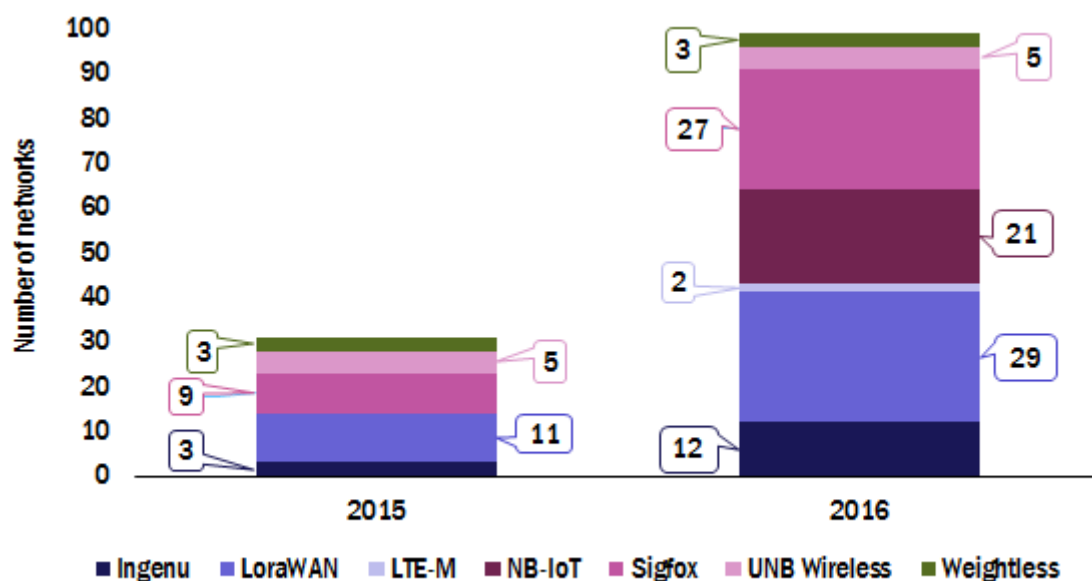
Název	Frekvence	Max. dosah	Max. rychlost
Bluetooth	2,4 GHz	150 m	1 Mb/s
WiFi	2,4 GHz / 5 GHz	50 m	1 GB/s
Cellular	900–2100 MHz	35 km	100 Mb/s
NFC	13.56 MHz	10 cm	400 kb/s
Sigfox	900 MHz	50 km	100 b/s
LoRa	900 MHz	15 km	100 kb/s
LTE Cat-M1	900–2100 MHz	5 km	1 Mb/s
NB-IoT	900–2100 MHz	5 km	200 kb/s
Z-Wave	868–910 MHz	40 m	100 kb/s
Zigbee	868–915 MHz / 2,4 GHz	75 m	250 kb/s

V současnosti nelze určit která z bezdrátových sítí bude dominantní během budoucího vývoje Internetu věcí, je ovšem jasné že se bude jednat o jednu ze specializovaných sítí (Sigfox, LoRa, LTE-M, NB-IoT), protože ostatní sítě nenabízejí dostatečný dosah spojený s energetickou nenáročností. Pro technologie na bázi LTE hraje významný fakt již existující infrastruktura, kterou stačí modernizovat. Naopak sítě Sigfox a LoRa mají momentálně navrch ve většině států budujících sítě pro Internet věcí, díky brzkému nástupu těchto technologií. Dle mého názoru bude v budoucnosti nejúspěšnější technologie LoRa, protože nabízí dostatečný dosah pokrytí a zároveň mnohem vyšší rychlost než Sigfox, ovšem může se nakonec ukázat opak. Mezi standardy Z-Wave a Zigbee, které slouží pro sítě malého

dosahu, nelze jednoznačně určit, který se v budoucnu stane dominantním. Již nyní velká část zařízení podporuje připojení přes oba standardy, lze tedy očekávat že oba standardy budou nadále existovat vedle sebe.

3.5 Pokrytí ve světě

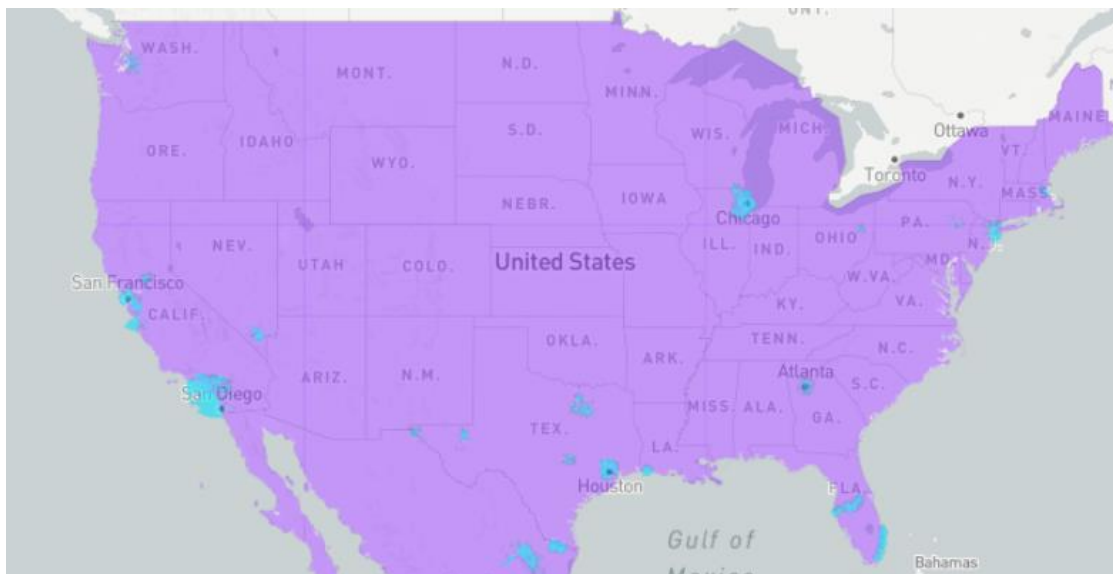
V této kapitole je provedeno shrnutí aktuálního vývoje pokrytí a využitých technologií ve vybraných státech ve světě. V celosvětovém měřítku, došlo v roce 2016 ke ztrojnásobení počtu aktivních, testovaných nebo budovaných sítí pro Internet věcí oproti roku 2015 (viz. obrázek 3-7), lze očekávat, že toto číslo v následujících letech ještě poroste. [38]



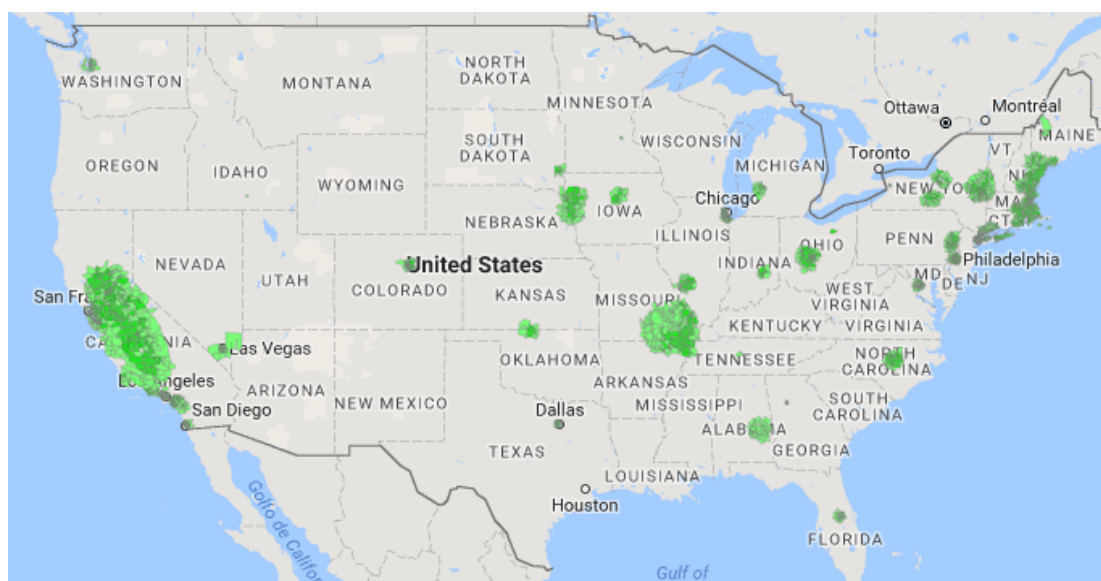
Source: Analysys Mason

Obrázek 3-7: Celosvětový počet aktivních, testovaných či budovaných sítí pro Internet věcí letech 2015 a 2016. [38]

3.5.1 USA



Obrázek 3-8: Pokrytí USA sítí Sigfox k 13.4.2017. [19] (pokryté území je zvýrazněno světle modrou barvou)



Obrázek 3-9: Pokrytí USA sítí LoRa k 13.4.2017. [42]

Vzhledem k velké rozloze Spojených států Amerických nelze zatím mluvit o žádném celoplošném pokrytí, jednotliví provozovatelé tedy v současnosti cílí na pokrytí největších měst a tím i na největší části populace. Momentálně ve Spojených státech, tak jako ve většině států na světě, probíhá souboj mezi technologií Sigfox reprezentovanou stejnojmennou francouzskou společností a technologií LoRa, kterou využívá společnost Senet. V současnosti jsou oba standardy ve Spojených státech zastoupeny téměř srovnatelně. Sigfox dosáhl koncem roku 2016 svého cíle pokrýt 100 měst ve Spojených státech, mezi těmito městy ovšem nejsou zastoupeny pouze největší města, ale i spousta menších. Vychází to z faktu, že Sigfox přednostně vedle velkých měst pokrýval také ta, kde byl o tuto

technologii projeven zájem některým z významnějších uživatelů (např. místní továrna). Ve výsledku tedy Sigfox nyní pokrývá 20 % populace Spojených států (viz. obrázek 3-8). Senet se svou sítí dosáhl podobného milníku jako Sigfox, tedy 100 pokrytých měst, již o pár měsíců dříve, lze tedy říci, že se momentálně jedná o vedoucího poskytovatele připojení pro Internet věcí ve Spojených státech (viz. obrázek 3-9). Senet dále nabízí, že v případě dostatečného zájmu je do 60 dní schopen nabídnout pokrytí i v dosud nepokrytých oblastech, čímž se může mapa pokrytí měnit velice rychle i mimo plánované lokality. Další podstatní hráči na Severoamerickém trhu jsou současní mobilní operátoři, především Verizon a AT&T. Tito poskytovatelé již pracují na zavádění svých vlastních sítí pro Internet věcí, které využívají standard LTE-M, to jim umožní dosáhnout rychle vysokého pokrytí za pomoci úpravy současné mobilní infrastruktury. Obě společnosti plánují dosáhnout masivního pokrytí již během roku 2017. Celkově jsou zatím Spojené státy spíše hůře pokrytou zemí, například oproti západní Evropě, ale v tomto hodnocení je potřeba zohlednit několika násobně větší rozlohu Spojených států. [39, 40, 41]

3.5.2 Jižní Korea

Jižní Korea, společně s Nizozemskem (viz. dále), patří mezi první dva státy, kteří mají celostátní síť pro zařízení Internetu věcí. V Jižní Koreji jsou momentálně ve velkém provozovány dva standardy sítí pro Internet věcí. Největší jihokorejský telefonní operátor SK Telecom cílí svou snahu na poskytnutí kompletního připojení pro různé typy koncových zařízení. Tato zařízení dělí do tří kategorií: první kategorie obsahuje zařízení vyžadující vysoké přenosové rychlosti a neustálé připojení k internetu (např. CCTV kamery), pro tyto zařízení je určena stávající LTE síť. Pro zařízení druhé kategorie, která vyžadují neustálé připojení ale ne tak vysoké přenosové rychlosti jako v první kategorii (např. senzory pohybu), byla v březnu roku 2016 spuštěna síť na standardu LTE-M. Do poslední kategorie jsou zařazena zařízení nevyžadující neustálé připojení a ani nepřenášejí velké objemy dat, pro tyto zařízení byla koncem června spuštěna roku 2016 spuštěna síť na standardu LoRa. Toto dokazuje, že jednotlivé síťové technologie nemusí sloužit pouze jako konkurence mezi sebou, ale při využití jednou společností mohou doplňovat svou funkcionalitu. V Jižní Koreji je momentálně pokryto již 99 % všech obyvatel a tím se řadí mezi špičku zemí v rozvoji infrastruktury pro Internet věcí. [43, 44, 45, 46]

3.5.3 Západní Evropa

V západní Evropě je momentálně velice rozšířená síť využívající standard Sigfox stejnojmenné francouzské společnosti, nabízí pokrytí většiny území ve státech jako je Francie, Španělsko, Irsko, Dánsko a země Beneluxu. A alespoň pokrytí největších měst ve

Velké Británii a Německu. Momentálně se z celkových 10 miliónů aktivních zařízení v síti Sigfox většina nachází v západní Evropě. Současně s rozvojem těchto sítí dochází i k masivnímu nasazování dalších technologií na území Západní Evropy. V podstatě v každé zemi dochází k implementaci LoRa sítí minimálně na území velkých měst a jejich postupnému rozvoji k celoplošnému pokrytí těchto států. Nizozemsko bylo dokonce první zemí plně pokrytou pomocí sítě LoRa společnosti KPN, síť byla ale spuštěna jen o pár dní dříve než v Jižní Koreji, k této síti je již nyní připojeno více jak 1.5 miliónu zařízení. Mimo tyto dva standardy (LoRa a Sigfox), ale dochází k výstavbě také sítí fungujících na základech stávajících LTE sítí. Za největší společnost využívající právě LTE-M standard, je považována skupina Vodafone, která v letošním roce plánuje spuštění celostátních sítí v Německu, Irsku, Nizozemsku a Španělsku. Další takovéto sítě už jsou v Evropě funkční, alespoň podle vyjádření operátorů, ale žádná zatím není v komerčním provozu.

Západní Evropa bude zaujímat i do budoucna vedoucí roli v rozvoji sítí Internetu věcí především díky velkému konkurenčnímu boji mezi jednotlivými poskytovateli a také díky požadavkům Evropských úřadů na zavádění nových technologií do různých odvětví. Tyto technologie budou potřebovat příslušnou infrastrukturu a operátorům nabízí v podstatě jistotu dostatku zákazníků. Příkladem může být třeba zavedení automatického tísňového volání z vozidla, kterým budou povinně vybavena všechna vozidla vyrobená od roku 2018. Další velikou motivací budovat nové sítě, je pro jejich provozovatele prognóza, že do roku 2021 dojde na Evropském trhu ke čtyřnásobení počtu připojených zařízení. [47, 48, 49, 50]

3.5.4 Porovnání vývoje ve světě

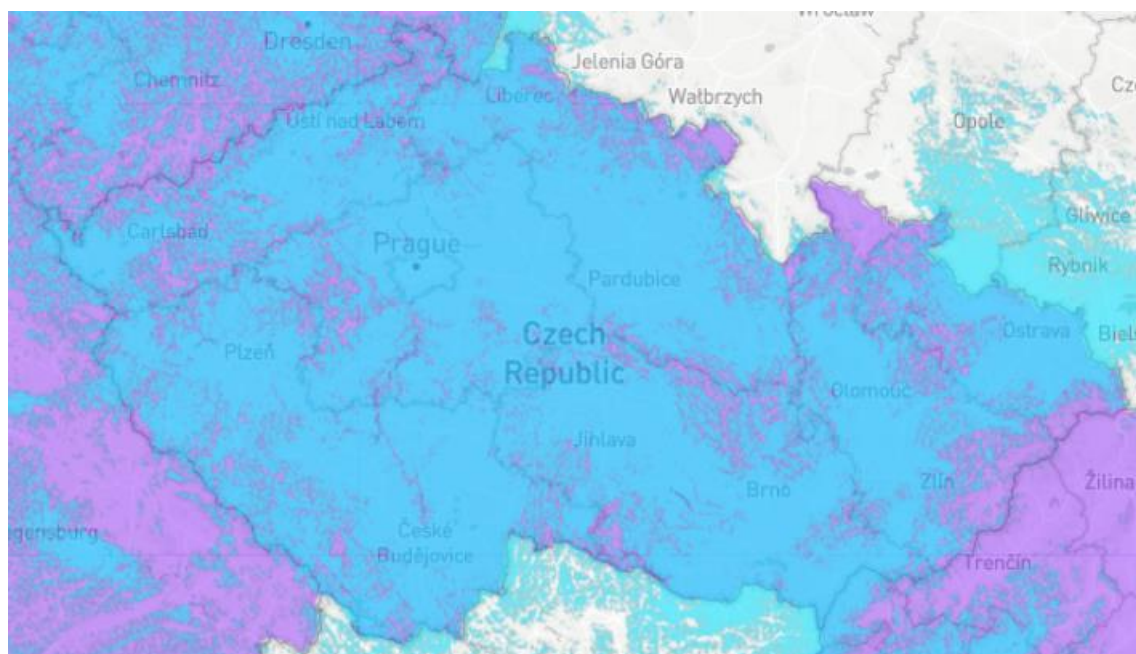
V současné době dochází k budování infrastruktury pro Internet věcí v mnoha dalších zemích po celém světě, ale vedoucími zeměmi tohoto pokroku jsou a nadále budou především státy v západní Evropě a Jižní Korea. Spojené státy Americké v tomto směru zatím poněkud zaostávají, což je zapříčiněno především jejich velikou rozlohou a rozčleněním na jednotlivé státy, ve kterých může být rozdílná podpora a regulace těchto sítí. V budoucnu bude velmi zajímavé sledovat různý vývoj trhu s připojením pro zařízení Internetu věcí v Evropě a právě Jižní Koreji, protože v každé oblasti se rozvíjí naprosto odlišný přístup k použitým technologiím. Na jedné straně stojí nabídka více různých technologií jednou společností v Jižní Koreji, oproti konkurenci mnoha společností využívajících každá jinou technologii v Evropě. Až v budoucnu bude možné posoudit, jaký model poskytování konektivity pro Internet věcí se stane úspěšnějším. Dalším zajímavým faktem ke sledování bude samotný vývoj v Evropě, kde dochází k přímé konkurenci mezi jednotlivými technologiemi, zda některá z použitých technologií dokáže získat převahu na

úkor ostatních, nebo zda společnosti ve výsledku sáhnout po Jihokorejském modelu, který nabízí více různých sítí pod hlavičkou jednoho operátora.

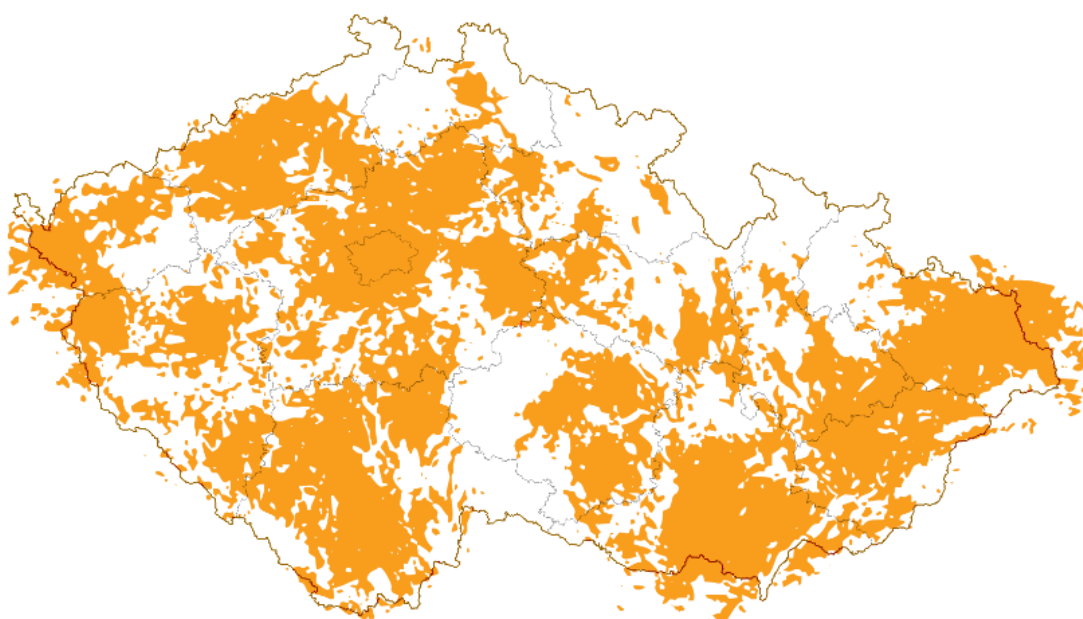
3.6 Pokrytí v České republice

V České republice, podobně jako v zemích západní Evropy, dochází k souboji několika různých technologií. Hlavními soupeři v budování síťové infrastruktury momentálně jsou České Radiokomunikace s technologií LoRa a Simplecell, který ve spolupráci se společností T-Mobile buduje síť na standardu Sigfox. Dalším hráčem, který oznámil příchod na trh během letošního roku je společnost Vodafone s technologií LTE-M (NB-IoT). Podle předpokladů společností T-Mobile a Simplecell bude pro kompletní pokrytí České republiky potřeba zhruba 350 základnových stanic. Momentálně tato síť pokrývá 86 % našeho území (viz. obrázek 3-10) a více jak 90 % populace České republiky a společnost dále plánuje do září letošního roku pokrýt přes 97 % populace a pokračovat v rozvoji sítě v sousední Slovenské republice. Konkurenční síť Českých Radiokomunikací využívající technologii LoRa je momentálně dostupná především v krajských městech a jejich okolí, dále jsou pokryta některá další větší města (Benešov, Kladno, Znojmo, Vsetín a další) (viz. obrázek 3-11). České radiokomunikace plánují do konce letošního roku ve spolupráci se společností Actility (jeden ze zakladatelů LoRa Alliance) spustit plošné pokrytí po celém území České republiky. Vedle toho je další činností Českých radiokomunikací například podpora společností vyvíjejícím koncová zařízení. Společnost, která na trh poskytování konektivity pro Internet věcí vstoupila jako poslední, Vodafone, sází na implementaci technologie LTE-M, konkrétně její verze NB-IoT. První testování této sítě započalo na podzim roku 2016 a Vodafone slibuje komerční spuštění v průběhu roku 2017. [51, 52, 53, 54, 55, 56]

Česká republika může být v současnosti zařazena mezi nejrychleji se rozvíjející země v odvětví Internetu věcí. Dosáhla toho především díky investicím ze strany Českých Radiokomunikací a Simplecellu (potažmo T-Mobilu), protože budování síťové infrastruktury je pro tyto společnosti poměrně snadnou záležitostí a předpokládaný nárůst počtu připojených zařízení slibuje rychlou návratnost investic. Na druhou stranu případná volba špatného standardu nebude pro společnosti likvidační, protože mohou snadno předělat stávající infrastrukturu na jiný standard. Do budoucna bude zajímavé sledovat vývoj využití jednotlivých sítí a jeho porovnání se státy západní Evropy, kde je momentálně velice podobná situace na tomto poli jako u nás. Z porovnání těchto vývojů budeme moci říci, jak velkou roli hrají v konkurenčním boji samotné technologie, a co závisí na ostatních faktorech, jako je cena, marketing a další. [51]



Obrázek 3-10: Aktuální pokrytí ČR sítě Sigfox. [19] (pokrytá místa jsou vyznačena světle modrou barvou)



Obrázek 3-11: Pokrytí ČR sítě LoRa k 17.4.2017. [23]

4 Návrh praktického využití sítě Zigbee pro realizace chytrého domu

Tato kapitola je věnována návrhu praktického využití Internetu věcí v ideálním chytrém domě, za využití bezdrátového připojení pomocí technologie Zigbee. Kapitola je rozdělena do tří částí. V první části se nachází vize, jakou funkčnost by měl nabízet ideální chytrý dům. Tato úvodní část nijak nereflektuje aktuální stav chytrých domů, je to pouze stav, ke kterému se za použití reálných technologií bude tento návrh snažit přiblížit. V následující části je popis, která zařízení budou potřeba pro co největší přiblížení funkcionalitě ideálního domu, za použití moderních bezdrátových technologií a bez stavebních úprav v samotném domě, a jejich umístění. Ve třetí, poslední části této kapitoly, se nachází popis, jaká síťová infrastruktura je použita pro propojení všech zařízení nacházejících se v domě.

4.1 Vize ideálního chytrého domu

Představy o chytrém domě může mít každý člověk rozdílné a nelze tedy jednoduše říci, co je v této oblasti považováno za ideál. Tato vize představuje chytrý dům na hranici momentálních technologických možností, nabízející uživatelům maximální usnadnění jeho každodenního využití a zároveň stále poskytuje dostatek soukromí a útulnosti, aby se dal stále využívat k běžnému bydlení.

Hlavními kritérii, která by měl takový ideální chytrý dům splňovat, je ale aspoň částečné pokrytí následujících oblastí: bezpečnost, pohodlí a zábava. Zajištění bezpečnosti se týká jak aktivních bezpečnostních prvků, kterými jsou dnešní domy již běžně vybaveny, tak pasivní bezpečnosti. Mezi aktivní bezpečnostní prvky se řadí například různé kamery a čidla. V chytrém domě se tato zařízení nevyužívají jen k jejich prvotnímu účelu, ale jsou propojeny s dalšími systémy domu, jako je například osvětlení nebo centrála bezpečnostní agentury.

Příklad: Při spuštění poplachu narušením některého čidla je automaticky rozsvíceno osvětlení v dané části domu a obraz z příslušné kamery či kamer je přenášen například na mobilní telefon majitele nebo televize v domě. V takovýto okamžik má majitel časový limit na vypnutí v případě, že se jedná o falešný poplach, jinak je automaticky informována bezpečnostní agentura.

Pasivní bezpečnostní se v tomto případě rozumí automatická aktivace aktivních bezpečnostních systémů, například pokud telefon majitele opustí dosah připojení k domácí síti nebo při zamknutí vchodových dveří, případně může být manuálně zapnut v celém domě nebo jeho části (např. v noci). Další součástí pasivní bezpečnosti je automatické

zavření oken, nebo alespoň indikace, která okna nejsou zavřena při odchodu z domu. Součástí tohoto systému je i automatické zhasnutí všech světel a případné ztlumení topení, pokud si to majitel přeje. Tímto se funkcionalita chytrého domu přelévá do další zmíněné kategorie a je zajištěno maximální pohodlí pro majitele. Toho je dosaženo, mimo již zmíněného automatického chování, především pomocí centrálního ovládání domu, například z tabletu nebo z mobilního telefonu. Pomocí tohoto centrálního ovládání může majitel ovládat například světla, topení, žaluzie či audiovizuální techniku. Mezi další schopnosti ideálního chytrého domu patří schopnost realizovat rutinní činnosti nezávisle na majiteli, například každý večer ztlumit topení a vyvětrat v ložnici, nebo při zaznamenání deště naopak bezpečně zavřít všechna okna. Tyto automatické činnosti musí být lehce nastavitelné, a ještě jednodušeji přerušitelné při případné výjimečné situaci, majitel se nesmí cítit jako otrok vlastního domu. Pro případ výpadku proudou nebo jiné poruchy musí být všechny systémy v domě stále ovládatelné manuálně. Další možnosti zvyšování komfortu pro majitele se nachází na příklad v kuchyni, kde lednička dokáže sledovat množství potravin a při poklesu pod určenou hranici pošle uživateli zprávu na telefon, co je potřeba dokoupit, nebo přímo sama zadá objednávku do online obchodu. V ideálním případě také lednička na integrovaném displeji zobrazuje, například to co je možné z aktuálně dostupných potravin uvařit.

V oblasti zábavy musí být jednoduše ovladatelné prvky audiovizuální techniky, aby uživatel nemusel například pro změnu hudby jít do vedlejší místnosti. Chytrý dům také umožňuje, pomocí propojení jednotlivých systémů, při spuštění filmu na televizi automaticky zatáhnout žaluzie, ztlumit světla a uzamknout vchodové dveře.

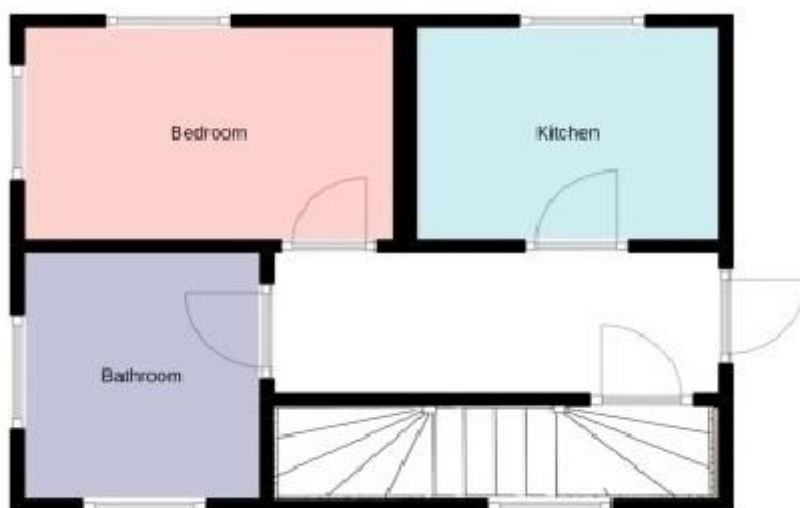
Vzhledem k poměrně vysoké ceně zařízení pro chytrý dům, je potřeba aby chytrá domácnost nabídla alespoň minimální návratnost v podobě ušetřených nákladů na energie. Této úspory je dosaženo především pomocí elektronické regulace topení a osvětlení. Například při odchodu majitele je automaticky snížena intenzita vytápění a zhasnuta všechna světla, toto chování ale musí být snadno vypnutelné pro případ, že majitel odchází jen na pár minut. Opět i zde nastává problém přílišné automatickosti. Další úspora energie je dosáhnuta regulací osvětlení v závislosti na úrovni venkovního světla.

4.2 Použitá zařízení a jejich umístění

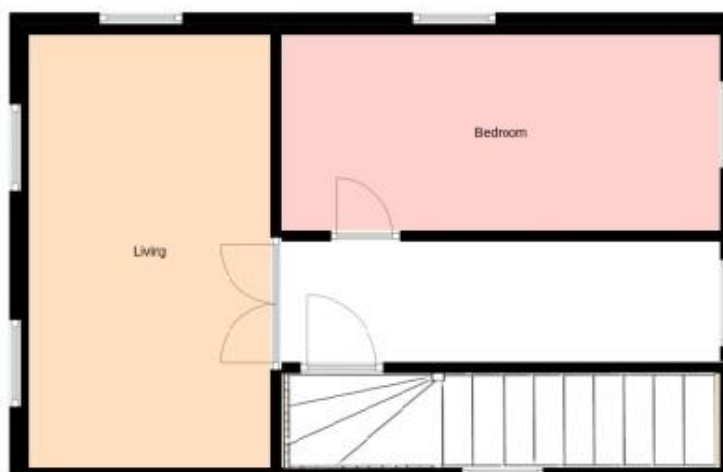
4.2.1 O domě

Modelový dům, na kterém je soustava chytrých zařízení navrhována, je obdélníkového půdorysu. Pokoje jsou v domě rozmístěny ve dvou patrech, v přízemí (viz. obrázek 4-1) se

nachází koupelna, ložnice a vstup do sklepa, který je rozdělen do dvou zvláštních místností a v každé z nich se nachází malé okno. V prvním patře (viz. obrázek 4-2) se dále nachází dětský pokoj, obývací pokoj a terasa. Každý pokoj disponuje v průměru dvěma okny. Celková obytná plocha domu je zhruba 140 m².



Obrázek 4-1: Půdorys přízemí modelového domu. [zdroj: autor]



Obrázek 4-2: Půdorys 1. patra modelového domu. Zdroj: autor

4.2.2 Zabezpečení

Prvotní oblastí pokrytou elektronickými zařízeními, je v dnešní době zabezpečení. Využití elektronického zabezpečovacího systému přináší nejenom lepší zabezpečení objektu, ale u některých pojišťoven může přinést i slevu na pojištění. Pro zabezpečení tohoto objektu byla

využita kombinace venkovních kamer, senzorů pohybu a detektorů otevřených oken. Pro instalaci venku bylo vybráno pět kamer snímajících všechny strany domu a jedna kamera snímá parkovací místo před domem. Všechny kamery jsou vybaveny infračerveným světlem pro bezproblémový provoz v noci. Vzhledem k nutnosti neustálého provozu, a tedy i napájení, nebyly zvoleny kamery podporující bezdrátové připojení. Naopak byly vybrány kamery podporující napájení přes UTP kabel při využití speciálního příslušenství, odpadá tedy potřeba instalovat ke každé kameře více jak jeden kabel.

Senzory pohybu (viz. obrázek 4-3) jsou instalovány u vstupních dveří, na schodišti, na chodbě v každém patře a v každém pokoji. Celkově je tedy umístěno devět snímačů pohybu. Senzory pohybu byly vybrány podle požadavku na podporu bezdrátové technologie Zigbee. Není tedy třeba zavádět žádné nové kabelové rozvody. Podle stejného požadavku byly vybrány i senzory upozorňující na nedovřená okna a dveře. Výrobce obou typů senzorů slibuje u těchto zařízení výdrž až pět let na baterie, takže se jedná o poměrně bezúdržbové vybavení. Vzhledem k umístění těchto senzorů na každé okno a vchodové dveře, včetně sklepních, bylo celkem potřeba umístit patnáct snímačů po celém domě. Dalšími instalovanými senzory jsou detektory kouře. Pro potřeby síťového pokrytí jsou použity detektory kouře podporující funkci opakovače. Detektory kouře jsou umístěny v každé místnosti, z bezpečnostních i síťových důvodů. Celkem je tedy použito osm detektorů kouře.



Obrázek 4-3: Pohybový senzor podporující bezdrátovou technologii Zigbee. [57]

Dále jsou instalovány také bezdrátově ovládané zámky všech venkovních dveří, u chytrých zámků je třeba vybírat velice pečlivě, protože se jedná o největší potencionální bezpečnostní problém. Při instalaci bezdrátového zámku je důležitá volba takového řešení, které podporuje manuální ovládání ať již původním nebo novým klíčem. Toto eliminuje problémy při vybití baterií v zámku. Další podmínkou pro výběr bezdrátového zámku je

podpora šifrování na aplikační úrovni, pro dodatečné zabezpečení ovládání zámku. V tomto návrhu je použit jeden zámek od společnosti Kwikset umístěný na vchodových dveřích.

4.2.3 Uživatelský komfort

V této části je zahrnuto veškeré technické vybavení, usnadňující běžné využívání domácnosti, jako jsou dálkově ovládané vypínače, rolety, vytápění a podobně. Prvotním instalovaným zařízením z této kategorie byly bezdrátové stmívače světla. Pro instalaci byla vybrána dvě zařízení od společnosti Trust, prvním zařízením je bezdrátový stmívač světla (viz. obrázek 4-4), který se instaluje mezi vypínač a samotné světlo. Dalším instalovaným zařízením je bezdrátový vypínač světla, ten se instaluje namísto klasického vypínače, vypínač je možné stále manuálně ovládat stisknutím. Jednou z nevýhod takového vypínače je absence fyzického přerušení přívodu proudu do světla, takže v případě poruchy nemusí fungovat ani manuálně. Ovšem není potřeba předpokládat, že nemožnost vypnout světlo by vedla k nějakým potencionálně nebezpečným situacím. Bezdrátové stmívače je třeba instalovat ke každému světlu v každé místnosti včetně terasy, takže je potřeba použít dvanáct stmívačů, u vypínačů je potřeba o něco nižší počet. Díky možnosti ovládaní dvou světla jedním vypínačem stačí do každé místnosti umístit jeden, tedy v součtu devět vypínačů, všechna tato zařízení jsou opět plně kompatibilní s bezdrátovou technologií Zigbee.



Obrázek 4-4: Bezdrátový stmívač světla. [58]

V případě potřeby dálkově ovládat vytápění domu, je obvykle s tímto požadavkem třeba počítat již při koupi samotných topných těles. Ovšem k běžnému radiátoru je možné připojit digitální hlavici s vlastním termostatem a připojením k bezdrátové síti. V tomto případě se opět jedná o síť na standardu Zigbee. Tyto hlavice je potřeba umístit na všechna topení v domě pro zajištění optimálního nastavení všech topných jednotek (všechna topení v jedné místnosti musí mít stejná data). Výhodou těchto hlavice je možnost rozpoznat otevřené okno, takže není potřeba řešit komunikaci mezi termostaty a senzory na oknech. Hlavice je potřeba

celkem šest, protože v koupelně a na chodbách je zavedeno elektrické podlahové vytápění, kde stačí běžný termostat vyměnit za termostat s podporou bezdrátového připojení.

Pro dálkové ovládání oken a žaluzií je potřeba již mít dům vybaven okny a žaluziemi s elektronickým ovládáním. Poté je umístěno příslušné zařízení, v tomto případě opět od společnosti Trust, nahrazující původní řídicí mechanismus. Je potřeba toto zařízení umístit na všechna okna a žaluzie, u kterých se předpokládá nutnost dálkového ovládání. Není tedy třeba jej instalovat na okna ve sklepě a podobně málo exponovaných místech. V tomto návrhu je tedy potřeba připojit celkem dvacet řídicích jednotek, pro zajištění ovládání v celém domě.

V návaznosti na automatické otevírání oken a vytápění, musíme systému poskytnout dostatek informací o venkovním počasí. Chytrý dům může získávat jednak informace ze sítě Internet, je-li připojení k dispozici, toto slouží především pro automatické plánování vytápění do budoucna. Také je možné získávat údaje ze senzorů umístěných v okolí domu, tento systém je ideální pro operativní změny v nastavení domu, například zavření oken při dešti nebo silném větru. Na střechu domu je tedy třeba umístit multifunkční senzor (viz. obrázek 4-5) schopný měřit momentální rychlost a směr větru, množství srážek, vlhkost a teplotu vzduchu. Senzor je opět připojen pomocí Zigbee sítě. Při umístění senzoru je třeba dát pozor, aby byl volně přístupný a nezakrytý (např. stromy).



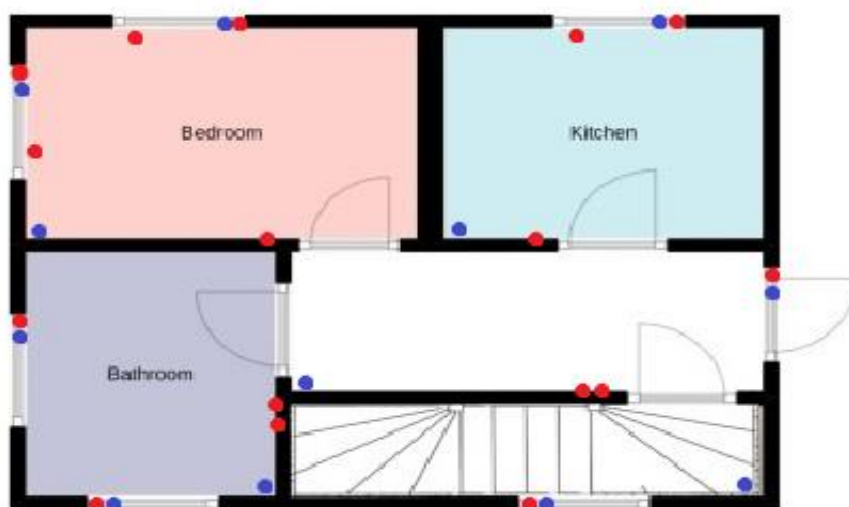
Obrázek 4-5: Multifunkční meteorologický senzor. [59]

4.2.4 Zábava

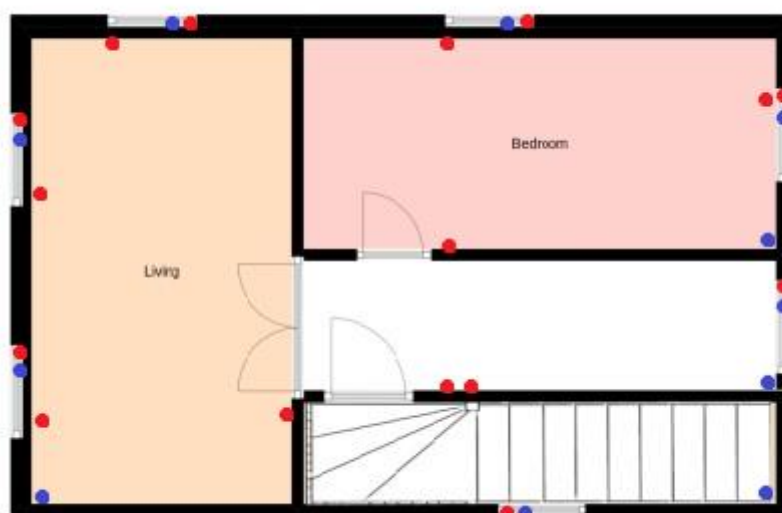
Vzhledem k nízkým přenosovým rychlostem standardu Zigbee, není vhodný pro propojení domácí audio a video techniky. Toto je běžně řešeno pomocí klasického WiFi připojení (např. připojení chytré televize k internetu) a běžné kabeláže (připojení televize a audio systému). Tato oblast chytré domácnosti tedy není do tohoto návrhu zahrnuta.

4.3 Umístění chytrých zařízení

Na obrázcích číslo 4-6 a 4-7, je znázorněno orientační umístění chytrých zařízení v domě, jsou zde zobrazena pouze koncová zařízení bez opakovačů. Pro rozlišení jsou zařízení rozdělena do dvou skupin: bezpečnostní jsou znázorněna modrou barvou a ostatní jsou znázorněna červenou barvou. Také jsou zde znázorněna pouze bezdrátově připojená zařízení, pro potřeby další části tohoto návrhu, kde bude realizována bezdrátová



Obrázek 4-6: Umístění chytrých zařízení v přízemí, modře: bezpečnostní zařízení, červeně: ostatní. [zdroj: autor]

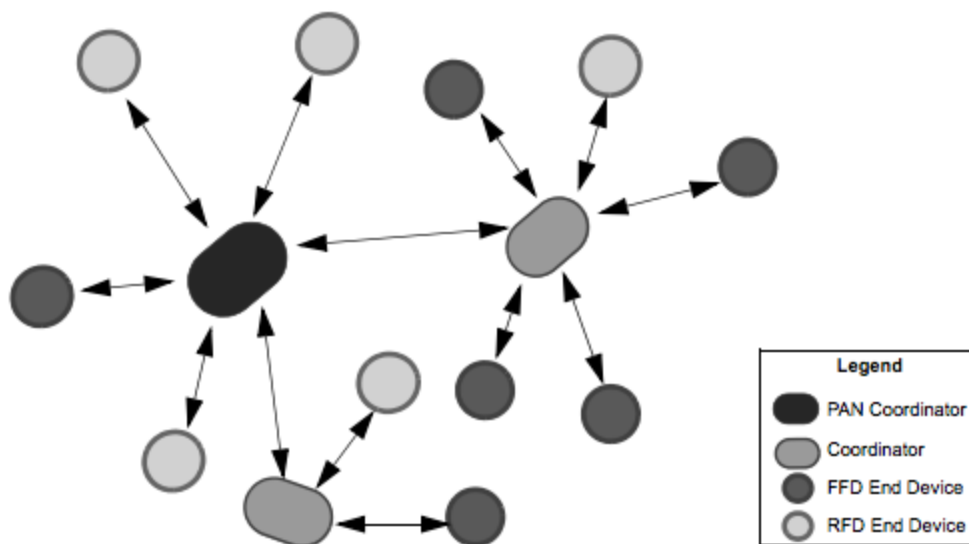


Obrázek 4-7: Umístění chytrých zařízení v 1.patře, modře: bezpečnostní zařízení, červeně: ostatní. [zdroj: autor]

infrastruktura. Právě díky využití bezdrátového připojení je možné jednotlivá umístění v průběhu času měnit.

4.4 Potřebná infrastruktura

Jak již bylo zmíněno výše v této kapitole, pro realizaci připojení zvolených chytrých zařízení je využita bezdrátová technologie Zigbee. Pro vytvoření chytré domácnosti je možné využít mnoho různých bezdrátových technologií, od běžné WiFi sítě až po specializované nízkoenergetické sítě jako je právě Zigbee. Další sítě, jež je možné použít, jsou celorepublikové sítě technologie LoRa nebo Sigfox, ale pro využití v domácnosti se tyto sítě spíše nehodí, protože je nutné platit stálé poplatky za každé připojené zařízení. V menším prostoru, jako je například rodinný dům, je levnější za jednorázovou investici vybudovat svou vlastní infrastrukturu, za kterou následně uživatel již neplatí. Z lokálních nízkoenergetických sítí je momentálně v nabídce dvojice standardů Z-Wave a Zigbee. Oba standardy se specializují především právě na domácí implementace Internetu věcí. V současné době je pro obě tyto sítě v nabídce obdobný počet zařízení a mnohá zařízení podporují dokonce oba tyto standardy. Standard Zigbee byl tedy vybrán především pro snadné zvýšení efektivního dosahu sítě.

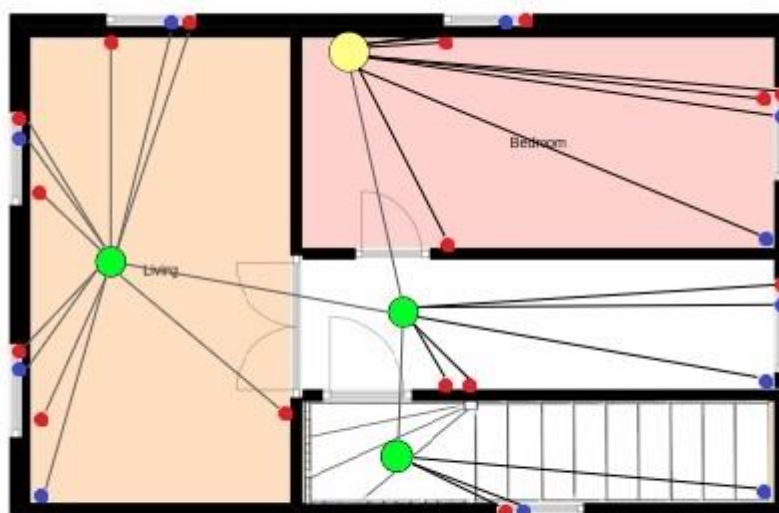


Obrázek 4-8: Příklad využití topologie. [60]

S nízkou energetickou náročností síť Zigbee se pojí také nevýhoda v podobě špatné prostupnosti pevnými překážkami. Toto je vyřešeno použitím zařízení schopných fungovat jako opakovače. Pro realizaci je zvolena topologie označována jako strom (viz. obrázek 4-8), kdy jeden řídicí router komunikuje s několika dalšími a ty následně zprostředkovávají připojení koncovým zařízením, která mohou být připojena i

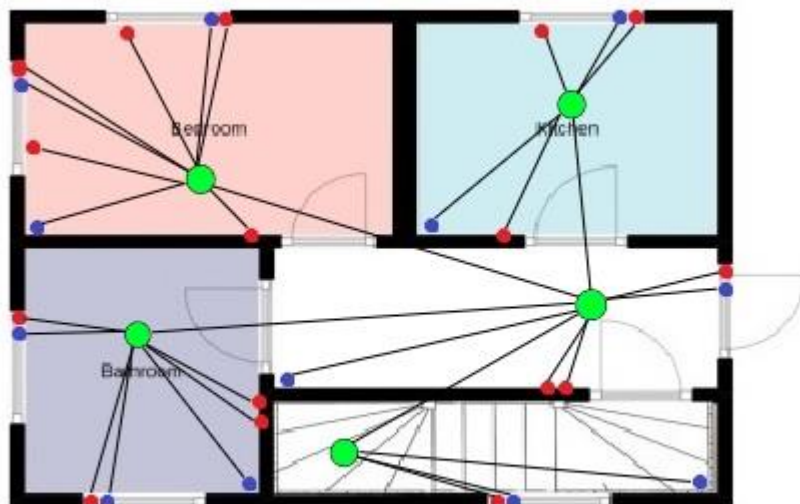
k samotnému řídicímu routeru. Tato topologie byla zvolena pro zajištění optimálního pokrytí po celém domě. Při využití klasické topologie ve tvaru hvězdy, kdy všechna koncová zařízení komunikují přímo s jedním řídicím routerem, by mohlo docházet k problému v komunikaci mezi zařízeními v jednotlivých patrech. Z důvodu silných zdí by se tento problém mohl ovšem projevit i na jednom patře mezi různými pokoji. Další možností je topologie takzvaného smíšeného typu, kdy všechna zařízení mohou komunikovat mezi sebou. Tato topologie zde není potřeba, protože všechna zařízení budou ovládána z centrálního řídicího prvku, a tedy by to pouze zvyšovalo cenové náklady na zařízení, každé z těchto zařízení by totiž muselo nabízet plnou funkcionalitu (viz s. 23).

Bezdrátová síť je strukturovaná tak, že řídicí prvek se nachází v pokoji v prvním patře, protože je zde umístěna zásuvka internetového připojení. Internetové připojení je nutné pro vzdálené ovládání domu. Připojení k internetu je v tomto případě realizováno pomocí UTP kabelu, ale může být použito i bezdrátové připojení WiFi. Řídicí jednotka komunikuje s nejbližšími koncovými prvky a opakovači, ty jsou realizovány pomocí detektorů kouře a umístěny v každé místnosti. Opakovače následně komunikují se zařízeními ve stejné místnosti a předávají signál řídicímu prvku, případně pokud není řídicí prvek v dosahu, je signál předán pomocí dalších opakovačů. Tímto využitím možností sítě je jednoduše zajištěno maximální pokrytí v celém domě. Pro pouhé připojení tohoto počtu chytrých zařízení v rámci standardně velkého domu, by stačil i menší počet opakovačů. Na obrázcích číslo 4-9 a 4-10 je znázorněno rozmístění opakovačů po domě. Koncová zařízení jsou označena červenou a modrou barvou, řídicí jednotka je označena žlutě a opakovače



Obrázek 4-9: Síťová infrastruktura v 1.patře. [zdroj: autor]

(detektory kouře) zeleně. Vyznačená komunikace mezi zařízeními je pouze ilustrační, v síti Zigbee každé zařízení komunikuje se všemi routery v dosahu.



Obrázek 4-10: Síťová infrastruktura v přízemí. [zdroj: autor]

4.5 Cena

V tomto návrhu se jedná o dovybavení běžného domu, za účelem přiblížení se takzvanému ideálnímu chytrému domu. Tomu odpovídá i cena, která je výrazně nižší než v případě, kdy je dům od začátku stavěn jako chytrý. Náklady na celkové realizování tohoto návrhu se pohybují kolem 80 000 Kč (viz tabulka 4-1) za všechna koncová zařízení. Další investice je potřeba do síťové infrastruktury, v tomto návrhu jde o částku necelých 15 000 Kč (viz. tabulka 4-2). Celkově jde tedy o necelých 100 000 Kč. Protože řídicí jednotka je třeba i při použití běžných kabelových rozvodů a rozdíl v ceně kouřových detektorů s možností šíření signálů Zigbee a bez této možnosti, je v řádu stokorun za kus, jedná se v porovnání s kabelovými rozvody o velmi nízkou částku. Běžně instalované kabelové rozvody pro chytrou domácnost se totiž pohybují v řádech desítek tisíc korun a samotný rozdíl v ceně koncových zařízení je zanedbatelný. Nutno ovšem říci, že kabelové rozvody již nejsou tolik využívány jako dříve, a lze předpokládat jejich kompletní nahrazení bezdrátovými sítěmi. Využití bezdrátových sítí pro vybavení chytré domácnosti je ideální volbou pro lidi, kteří chtějí získat chytrý dům bez stavebních úprav a při menší finanční náročnosti. Ale i přes nižší cenu oproti běžným řešením chytrých domů, se stále jedná o poměrně vysokou částku,

která může být pro mnoho domácností nedostupná. V budoucnosti můžeme, společně s dalším rozvojem chytrých domácností, očekávat výrazný pokles cen.

Tabulka 4-1: Ceny koncových zařízení. [zdroj: autor]

Název	Cena	Množství	Celkem
Kamery	2 300 Kč	5	12 350 Kč
Zámek	4 420 Kč	1	4 420 Kč
Pohybové senzory	1 300 Kč	9	11 700 Kč
Senzory na okno	1 040 Kč	15	15 600 Kč
Stmívače	950 Kč	12	11 400 Kč
Vypínače	560 Kč	9	5 040 Kč
Termostatická hlavice	2 100 Kč	6	12 600 Kč
Termostat	1 820 Kč	3	5 460 Kč
Celkem			78 570 Kč

Tabulka 4-2: Celková cena. [zdroj: autor]

Název	Cena	Množství	Celkem
Detektor kouře	680 Kč	7	4 760 Kč
Řídící jednotka	9 800 Kč	1	9 800 Kč
Celkem			14 560 Kč
Celkem se zařízeními			93 130 Kč

5 Závěr

V úvodní části práce bylo za cíl popsat historický vývoj Internetu věcí a popsat pojmy a definice související s tímto tématem. Tento cíl byl naplněn vytvořením uceleného přehledu o tom, co je vlastně Internet věcí a následujícím shrnutím historického vývoje tohoto tématu.

Dalším cílem bylo shrnout informace o používaných bezdrátových sítích a analyzovat současnou rozšířenost těchto sítí po světě. Byl tedy vytvořen souhrn nejvýznamnějších bezdrátových technologií sloužících pro přenos dat, v tomto souhrnu jsou zastoupeny běžně užívané sítě a také sítě speciálně vyvíjené a budované pro Internet věcí. Sítě byly vzájemně porovnány a nachází se zde také předpoklad, jaká z technologií může zaujmout v budoucnosti dominantní postavení. Následuje popis, jaké sítě jsou používány ve vybraných státech na světě. Státy byly vybrány podle obecné technologické vyspělosti a jsou jimi: Spojené státy Americké, Jižní Korea a souhrnně státy v západní Evropě, především tedy Francie, Nizozemsko a Německo. V souvislosti s těmito státy bylo také provedeno porovnání současného stavu infrastruktury v těchto státech a její předpokládaný vývoj. V návaznosti byla provedena stejná analýza zaměřená na stav a vývoj v České republice s konstatováním, že v tomto odvětví může být Česká republika plně srovnávána s nejvyspělejšími státy na světě.

V praktické části práce bylo za cíl prezentovat návrh konkrétního využití specializovaných bezdrátových sítí pro Internet věcí. Cílem zvoleného návrhu bylo změnit normální rodinný dům na dům chytrý. V prvotní části byla provedena úvaha, jak má fungovat ideální chytrý dům. V další části byla určena potřebná zařízení, pro zajištění funkcionality co nejvíce podobné jako v předchozí úvaze, a jejich ideální umístění v domě. Nejdůležitější částí je ale návrh samotné síťové infrastruktury, pro vybudování chytré domácnosti byla zvolena technologie Zigbee, protože disponuje ideálními vlastnostmi pro připojení chytrých zařízení a oproti technologií celorepublikového dosahu, zde není potřeba platit paušální poplatky za každé připojené zařízení. Na konci návrhu bylo provedeno cenové srovnání s dříve hojně používanými kabelovými rozvody pro připojení chytrých zařízení. Z tohoto vychází že kabelové rozvody jsou finančně náročnější a v budoucnu budou plně nahrazeny bezdrátovými technologiemi.

6 Seznam použité literatury

1. KOPETZ, Hermann. *Real-time systems: design principles for distributed embedded applications*. 2nd ed. Boston: Springer, c2011. Real-time systems series. ISBN 978-1-4419-8236-0.
2. YANG, Shuang-Hua. *Wireless sensor networks: Principles, Design and Applications*. 1. London: Springer-Verlag London, 2013. ISBN 9781447155041.
3. GUBBI, Jayavardhana, Rajkumar BUYYA, Slaven MARUSIC a Marimuthu PALANISWAMI. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*. 2013, **2013**(29), 1645–1660.
4. VALEŠ, Miroslav. *Inteligentní dům*. Brno: ERA, 2006. 21. století. ISBN 8073660628.
5. MAŘÍK, Vladimír. *Průmysl 4.0: výzva pro Českou republiku*. Praha: Management Press, 2016. ISBN 978-80-7261-440-0.
6. Big Data. *Management Mania* [online]. 14.2.2017 [cit. 2017-03-01]. Dostupné z: <https://managementmania.com/cs/big-data>
7. Big data a jejich zpracování. *Root.cz* [online]. 18.2.2013 [cit. 2017-03-02]. Dostupné z: <https://www.root.cz/clanky/big-data-a-jejich-zpracovani/>
8. Internet of Things (IoT) History. *Postscapes* [online]. Denver, February 1, 2016 [cit. 2017-03-02]. Dostupné z: <http://www.postscapes.com/internet-of-things-history/>
9. ZAKON, Robert. Hobbes' Internet Timeline. ZAKON, Robert. *Rober Hobbes Zakon* [online]. January 29, 2017 [cit. 2017-03-03]. Dostupné z: <https://www.zakon.org/robert/internet/timeline/>
10. 11 Internet of Things (IoT) Protocols You Need to Know About. *DesignSpark* [online]. April 20, 2015 [cit. 2017-03-06]. Dostupné z: <https://www.rs-online.com/designspark/eleven-internet-of-things-iot-protocols-you-need-to-know-about>
11. Overview for 6LoWPAN. *Texas Instruments* [online]. c1995-2016 [cit. 2017-03-07]. Dostupné z: <http://www.ti.com/llds/ti/wireless-connectivity/6lowpan/overview.page>

12. Bluetooth Low Energy. *Bluetooth* [online]. c2017 [cit. 2017-03-07].
Dostupné z: <https://www.bluetooth.com/what-is-bluetooth-technology/how-it-works/low-energy>
13. About Near Field Communication. *Near Field Communication* [online]. c2017 [cit. 2017-04-06]. Dostupné z: <http://nearfieldcommunication.org/about-nfc.html>
14. HUNN, Nick. LoRa vs LTE-M vs Sigfox. *Creative Connectivity* [online]. London, December 22, 2017 [cit. 2017-03-09]. Dostupné z: <http://www.nickhunn.com/lora-vs-lte-m-vs-sigfox/>
15. SIGFOX: Internet věcí bez internetu a jen pro některé věci. *Lupa.cz* [online]. 22.5.2015 [cit. 2017-03-10]. Dostupné z: <http://www.lupa.cz/clanky/sigfox-internet-veci-bez-internetu-a-jen-pro-nektere-veci/>
16. What Is SigFox? *Link Labs* [online]. February 12, 2015 [cit. 2017-03-10].
Dostupné z: <https://www.link-labs.com/blog/what-is-sigfox>
17. SIGFOX. *SimpleCell* [online]. 2016 [cit. 2017-03-10]. Dostupné z: <https://www.simplecell.eu/technologie-sigfox/>
18. Sigfox, the world's leading Internet of things (IoT) connectivity service. *Sigfox* [online]. 2017 [cit. 2017-03-10]. Dostupné z: <http://www.sigfox.com/en>
19. Coverage. *Sigfox* [online]. 2017 [cit. 2017-03-11]. Dostupné z: <http://www.sigfox.com/en/coverage>
20. LoRa Technology. *OSEL* [online]. 5.3.2016 [cit. 2017-03-11]. Dostupné z: <http://www.osel.cz/8732-lora-technology.html>
21. LoRaWAN™ What is it?: A technical overview of LoRa® and LoRaWAN™. *LoRa Alliance* [online]. San Ramon, 2015 [cit. 2017-03-11].
Dostupné z: <https://www.lora-alliance.org/portals/0/documents/whitepapers/LoRaWAN101.pdf>
22. LoRa Alliance™ Technology. *LoRa Alliance* [online]. c2017 [cit. 2017-03-11].
Dostupné z: <https://www.lora-alliance.org/What-Is-LoRa/Technology>
23. Služby IoT. *České radiokomunikace* [online]. c2017 [cit. 2017-03-15].
Dostupné z: <https://www.cra.cz/sluzby-iot>

24. What is LTE-M? *Link Labs* [online]. January 27, 2017 [cit. 2017-03-15].
Dostupné z: <https://www.link-labs.com/blog/what-is-lte-m>
25. Varianty LTE LPWA jako konkurent Sigfoxu v IoT v podobě nízkoenergetických bezdrátových sítí. *Marigold* [online]. 28.11.2016 [cit. 2017-04-06]. Dostupné z: <https://www.marigold.cz/item/varianty-lte-lpwa-jako-konkurent-sigfoxu-v-iot-v-podobe-nizkoodberovych-bezdratovych-siti>
26. Z-Wave, the Smartest Choice for your Smart Home. *Z-Wave* [online]. c2017 [cit. 2017-04-06]. Dostupné z: <http://www.z-wave.com/about>
27. MUSHTAQ, Noor Ul. Z Wave for Home Automation. *CCTV Institute* [online]. November 1, 2016 [cit. 2017-03-15]. Dostupné z: <http://cctvinstitute.co.uk/z-wave/>
28. GALEEV, Mikhail. Catching the Z-Wave. *Embedded* [online]. October 2, 2006 [cit. 2017-04-06]. Dostupné z: <http://www.embedded.com/design/connectivity/4025721/Catching-the-Z-Wave>
29. FOULADI, Behrang a Sahand GHANOUN. *Security Evaluation of the Z-Wave Wireless Protocol*. London, 2013.
30. EZ-Wave: A Z-Wave hacking tool capable of breaking bulbs, abusing Z-Wave devices. *Network World* [online]. January 19, 2016 [cit. 2017-03-16].
Dostupné z: <http://www.networkworld.com/article/3024217/security/ez-wave-z-wave-hacking-tool-capable-of-breaking-bulbs-and-abusing-z-wave-devices.html>
31. Z-WAVE SMARTHOME. *ROBB* [online]. c2016 [cit. 2017-03-16]. Dostupné z: <https://en.robbshop.nl/about-z-wave/what-is-z-wave>
32. FARAHANI, Shahin. *ZigBee wireless networks and transceivers*. Boston: Newnes/Elsevier, c2008. ISBN 978-075-0683-937.
33. PAVLIS, Jakub. ZigBee - když je pomalejší síť výhodnější. *NOTEBOOK.cz* [online]. 24.8.2011 [cit. 2017-04-07]. Dostupné z: <http://notebook.cz/clanky/technologie/2011/ZigBee>
34. ZIGBEE® WIRELESS STANDARD. *DIGI* [online]. c1996-2017 [cit. 2017-04-07]. Dostupné z: <https://www.digi.com/resources/standards-and-technologies/rfmodems/zigbee-wireless-standard>

35. SMITH, Zachary. Make the right choices when building ZigBee applications. *EE Times* [online]. 7.11.2005 [cit. 2017-04-07]. Dostupné z: http://www.eetimes.com/document.asp?doc_id=1273370
36. Zigbee Introduction. *ICP DAS USA* [online]. c2001-2017 [cit. 2017-04-09]. Dostupné z: <https://www.icpdas-usa.com/zigbeeintro.php>
37. ZILLNER, Tobias. *ZIGBEE EXPLOITED: The good, the bad and the ugly*. Vienna, 2015.
38. DONKIN, Chris. Low-power IoT networks more than doubled in 2016. *Mobile World Live* [online]. January 20, 2017 [cit. 2017-04-13]. Dostupné z: <https://www.mobileworldlive.com/featured-content/home-banner/nb-iot-drives-strong-growth-in-lpwa/>
39. KINNEY, Sean. 100 US cities covered by Senet LoRa network for IoT. *RCR Wireless News* [online]. June 15, 2016 [cit. 2017-04-13]. Dostupné z: <http://www.rcrwireless.com/20160615/internet-of-things/100-u-s-cities-covered-senet-lora-network-iot-tag17>
40. HIGGINBOTHAM, Stacey. Sigfox's network hits 100 U.S. cities: Does it matter? *STACEY ON IOT* [online]. December 28, 2016 [cit. 2017-04-13]. Dostupné z: <https://staceyoniot.com/sigfoxs-network-hits-100-u-s-cities-does-it-matter/>
41. ALLEVEN, Monica. Verizon, AT&T both claim LTE Cat M firsts for Internet of Things. *Fierce Wireless* [online]. October 31, 2016 [cit. 2017-04-13]. Dostupné z: <http://www.fiercewireless.com/tech/verizon-at-t-both-claim-lte-cat-m-firsts-for-internet-things>
42. Senet Coverage. *Senet* [online]. April 13, 2017 [cit. 2017-04-13]. Dostupné z: <http://www.senetco.com/coverage/>
43. DO, Michelle a Harrison SON. SK Telecom's Multi-Track IoT Network: LTE, LTE-M and LoRa. *Net Manias* [online]. December 27, 2016 [cit. 2017-04-14]. Dostupné z: <http://www.netmanias.com/en/post/blog/10974/iot-lte-sk-telecom/sk-telecom-s-multi-track-iot-network-lte-lte-m-and-lora>
44. SK Telecom Commercializes Nationwide LoRa Network for IoT. *SK Telecom* [online]. July 4, 2016 [cit. 2017-04-14]. Dostupné z: <http://www.sktelecom.co.kr/en/press/detail.do?idx=1172>

45. South Korea launches first Internet of Things network. *BBC* [online]. July 5, 2016 [cit. 2017-04-14]. Dostupné z:
<http://www.bbc.com/news/technology-36710667>
46. BROWN, Isaac. The Netherlands and South Korea announce nationwide LoRa networks. *Tech Target IoT Agenda* [online]. September 21, 2016 [cit. 2017-04-14]. Dostupné z:
<http://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/The-Netherlands-and-South-Korea-announce-nationwide-LoRa-networks>
47. MORRIS, Anne. Ericsson: Western Europe to play leading role in adding IoT connections. *Fierce Wireless* [online]. June 1, 2016 [cit. 2017-04-15]. Dostupné z: <http://www.fiercewireless.com/europe/ericsson-western-europe-to-play-leading-role-adding-iot-connections>
48. GILL, Bob. Sigfox IoT Network Spreads Across the Globe. *Industrial IoT* [online]. January 26, 2017 [cit. 2017-04-15]. Dostupné z: <https://industrial-iot.com/2017/01/sigfox-iot-network-spreads-across-the-globe/>
49. BROWN, Bruce. Netherlands first to establish nationwide Internet of Things network. *Digital Trends* [online]. July 1, 2016 [cit. 2017-04-15]. Dostupné z: <http://www.digitaltrends.com/home/netherlands-kpn-lora-internet-of-things/>
50. WILSON, Richard. Europe goes for LoRa IoT network technology without UK. *Electronics Weekly* [online]. June 28, 2016 [cit. 2017-04-15]. Dostupné z: <https://www.electronicsworld.com/news/europe-goes-for-iot-network-technology-without-uk-2016-06/>
51. JIRÁSKO, Tomáš. Česká republika a sítě pro internet věcí. *Hospodářské noviny* [online]. 12.5.2016 [cit. 2017-04-17]. Dostupné z: http://ictrevue.ihned.cz/c3-65289170-0ICT00_d-65289170-ceska-republika-a-site-pro-internet-veci
52. BERÁNEK, Jan. Už i Vodafone si postaví síť pro internet věcí. Zkouší technologii NB-IoT. *Lupa.cz* [online]. 1.7.2016 [cit. 2017-04-17]. Dostupné z: <http://www.lupa.cz/clanky/uz-i-vodafone-si-postavi-sit-pro-internet-veci-zkousi-technologie-nb-iot>

53. HALATA, Ondřej. SimpleCell – nový operátor mobilní sítě v ČR. *Android Market* [online]. 16.2.2016 [cit. 2017-04-17]. Dostupné z: <http://androidmarket.cz/ruzne/simplecell-novy-operator-mobilni-site-v-cr/>
54. ROZŠÍŘUJEME POKRYTÍ IOT SÍTĚ O DALŠÍ MĚSTA. *České Radiokomunikace* [online]. Praha, 21.3.2017 [cit. 2017-04-17]. Dostupné z: <https://www.cra.cz/rozsirujeme-pokryti-iot-site-o-dalsi-mesta>
55. Actility a České Radiokomunikace uzavřely partnerství v projektu největší sítě LoRa v Česku. *Feed It* [online]. Paříž, 5.4.2016 [cit. 2017-04-17]. Dostupné z: <https://feedit.cz/2016/04/05/actility-a-ceske-radiokomunikace-uzavrely-partnerstvi-v-projektu-nejvetsi-site-lora-v-cesku/>
56. Vodafone si pro rozšíření služby Internet věcí vybral technologii NB-IoT. *Vodafone* [online]. 29.6.2016 [cit. 2017-04-17]. Dostupné z: <https://www.vodafone.cz/o-vodafone/o-spolecnosti/pro-media/tiskove-zpravy/detail/vodafone-si-pro-rozsireni-sluzby-internet-veci-vyb/>
57. Motion Sensor. *NYCE* [online]. c2017 [cit. 2017-04-19]. Dostupné z: <http://nycesensors.com/products/ncz3041/>
58. Trust Vestavěný multi stmívač světel k bezdrátovému stmívání světel ACM-100. *CZC.cz* [online]. 2017 [cit. 2017-04-19]. Dostupné z: <https://www.czc.cz/trust-vestaveny-multi-stmivac-svetel-k-bezdratovemu-stmivani-svetel-acm-100/191674/produkt>
59. AcuLink 5-in-1 PRO Sensor. *Smart Home DB* [online]. c2017 [cit. 2017-04-19]. Dostupné z: <https://www.smarthomedb.com/product/aculink-5-in-1-pro-sensor/p634>
60. FLOWERS, David a Yifeng YANG. Microchip MiWi™ Wireless Networking Protocol Stack. USA, 2010. ISBN 978-1-60932-346-2. Dostupné také z: <https://www.eeweb.com/company-blog/microchip/microchip-miwi-wireless-networking-protocol-stack>