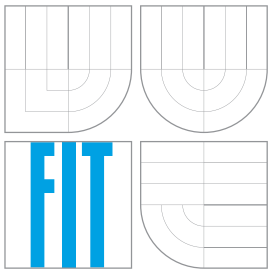
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÉ GRAFIKY A MULTIMÉDIÍ
FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER GRAPHICS AND MULTIMEDIA

INTERNET OF THINGS ZAŘÍZENÍ S PODPOROU BLUETOOTH A COAP

INTERNET OF THINGS DEVICE BASED ON BLUETOOTH AND COAP

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

ONDŘEJ FUCHS

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. PETR MUSIL

BRNO 2016

Zadání bakalářské práce/18444/2015/xfuchs03

Vysoké učení technické v Brně - Fakulta informačních technologií

Ústav počítačové grafiky a multimédií Akademický rok 2015/2016

Zadání bakalářské práce

Řešitel: **Fuchs Ondřej**
Obor: Informační technologie
Téma: **Internet of Things zařízení s podporou Bluetooth a COAP**
Internet of Things Device Based on Bluetooth and COAP
Kategorie: Vestavěné systémy

Pokyny:

1. Prostudujte dostupnou literaturu týkající se fenomenu Internetu věcí (Internet of Things - IoT).
2. Seznamte se s používanými komunikačními rozhraními a protokoly využitými v IoT. Zaměřte se na rozhraní Bluetooth a protokol COAP.
3. Navrhněte zařízení spadající do kategorie IoT.
4. Zařízení realizujte a otestujte.
5. Zhodnoťte výsledky práce a diskutujte případné pokračování nebo rozšíření práce.

Literatura:

- Dle pokynů vedoucího

Pro udělení zápočtu za první semestr je požadováno:

- Body 1 a 2 zadání

Podrobné závazné pokyny pro vypracování bakalářské práce naleznete na adrese http://www.fit.vutbr.cz/info/szz/

Technická zpráva bakalářské práce musí obsahovat formulaci cíle, charakteristiku současného stavu, teoretická a odborná východiska řešených problémů a specifikaci etap (20 až 30% celkového rozsahu technické zprávy).

Student odevzdá v jednom výtisku technickou zprávu a v elektronické podobě zdrojový text technické zprávy, úplnou programovou dokumentaci a zdrojové texty programů. Informace v elektronické podobě budou uloženy na standardním nepřepisovatelném paměťovém médiu (CD-R, DVD-R, apod.), které bude vloženo do písemné zprávy tak, aby nemohlo dojít k jeho ztrátě při běžné manipulaci.

Vedoucí: **Musil Petr, Ing.**, UPGM FIT VUT
Datum zadání: 1. listopadu 2015
Datum odevzdání: 18. května 2016

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta informačních technologií
Ústav počítačové grafiky a multimédií
612 66 Brno, Božetěchova 2

L.S.

doc. Dr. Ing. Jan Černocký
vedoucí ústavu

Abstrakt

Tato bakalářská práce se zabývá v dnešní době velmi zmiňovaným pojmem *Internet věcí*. Hlavním cílem je definovat *Internet věcí*, popsat jeho historii vzniku, základní charakteristiku, vývoj, problematiku zabezpečení a rizika s tím spojená, trendy a možné využití. Dále pak popsat možné technologie a protokoly pro přenos dat, skupiny výrobců zařízení a následně nastínit budoucnost *Internetu věcí*. Práce také zahrnuje návrh, implementaci a testování zařízení spadajícího do kategorie *Internetu věcí*.

Abstract

This bachelor thesis deals with nowadays very mentioned concept of the Internet of things. The main objective is to define the Internet of things, describe the history of the formation, basic characteristics, development, security issues and the associated risks, trends and possible use. Then describe possible technology and data transfer protocols, manufacturers of device and then outline the future of the Internet of things. Thesis also includes the design, implementation and testing of device falling into the category of Internet of Things.

Klíčová slova

Internet věcí, ESP8266, NodeMCU, Lua, Bluetooth, WiFi, CoAP.

Keywords

Internet of things, ESP8266, NodeMCU, Lua, Bluetooth, WiFi, CoAP.

Citace

FUCHS, Ondřej. *Internet of Things zařízení s podporou Bluetooth a CoAP*. Brno, 2016. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Musil Petr.

Internet of Things zařízení s podporou Bluetooth a CoAP

Prohlášení

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

.....
Ondřej Fuchs
10. května 2016

Poděkování

Chtěl bych poděkovat panu Ing. Petru Musilovi za odborné vedení a cenné rady, které mi pomohly při vytváření této práce.

Obsah

Kapitola 1

Úvod

Tato práce se zabývá v dnešní době velmi zmiňovaným pojmem *Internet věcí*, v anglické literatuře nebo na internetu označovaném jako *Internet of Things*.

Díky novým technologickým možnostem a stále se rozrůstajícímu pokrytí bezdrátového internetu vznikají ve velkém počtu levná elektronická zařízení, která skrze internet komunikují a dokáží přeměnit obyčejná „hloupá“ zařízení na chytré což znamená zejména rozšíření funkcionality, interakce, možnosti vzdáleného monitorování a ovládání.

Pojem je často uváděn v obecné souvislosti s internetem, často v souvislosti s komunikací mezi jednotlivými zařízeními, sběrem a zpracováním dat, vestavěnými systémy či vývojem nových nízkoenergetických senzorů. Souvisí také se stále se zvyšujícím počtem zařízení připojených k internetu díky snižujícím se výrobním nákladům a s tím spojeným významným poklesem prodejních cen využívaných zařízení. Důležitým faktorem prudkého rozvoje *Internetu věcí* je i technologický pokrok a vývoj a výroba nových zařízení v oblasti informačních technologií.

Internet věcí je pojem velmi rozsáhlý. Řada odborníků se ve svých definicích *Internetu věcí* často různí. *Internet věcí* otevírá nové možnosti pro velký počet úplně nových aplikací, které slibují např. zlepšení kvality lidského života. Zejména posledních několik let přispělo k procesu formování tohoto technologického fenoménu a tato práce se snaží *Internet věcí* popsat a zdokumentovat.

Druhá kapitola obsahuje základní informace o *Internetu věcí*, zejména definici samotného pojmu. Dále je uvedena historie vzniku *Internetu věcí*. Jsou popsány současné trendy a využití, zabezpečení a možná rizika s *Internetem věcí* spjata. Následně je popsán související pojem cloud computing, možné technologie a používané protokoly pro přenos dat. Kapitola je zakončena popisem skupin výrobců zařízení a následně je nastíněna budoucnost *Internetu věcí*.

Třetí kapitola obsahuje návrh zařízení spadajícího do kategorie *Internet věcí*, použitý hardware, software a možné využití. Následně je popsána samotná implementace zařízení, testování a celkové shrnutí zařízení.

Kapitola 2

Internet věcí

Hlavním cílem kapitoly je definovat *Internet věcí*, popsat historii vzniku, základní charakteristiku, popsat současné trendy a možné využití, problematiku zabezpečení a rizika s tím spojená, blíže ozřejmit využívané technologie a protokoly pro přenos dat a nastínit budoucnost této problematiky.

2.1 Základní informace

Internet věcí - obecně jde o označení nového trendu v oblasti informačních technologií využívajících různých zařízení propojených mezi sebou s přístupem do sítě. Tato zařízení umožní sběr dat pomocí senzorů, jejich analýzu a zpracování. Data jsou následně využita nejčastěji pro zlepšení kvality lidského života.

Pro *Internet věcí* existuje mnoho různých definic podle různých pohledů na tuto problematiku.

„Internet věcí můžeme chápat jako třívrstvý model, z čehož první vrstva je web (middleware). Druhá vrstva jsou jednotlivé zařízení (sensors) a třetí vrstva je sémantický model (knowledge). Pro úplnou využitelnost internetu věcí musíme tyto tři modely propojit.“[4]

Jiná definice: *„Internet věcí propojí objekty reálného světa s virtuálním světem, což umožní kdykoli a kdekoli komukoli se na cokoli připojit. Souvisí to se světem, kde fyzické objekty stejně jako virtuální data vzájemně spolu v čase interagují.“*[12]

Další možná definice: *„Je důležité pochopit zvláštní význam slova věci ve spojení Internet věcí. Věc může být reálná i virtuální. Tahle věc je vždy spojena s digitálním světem prostřednictvím bezdrátové komunikace. Jedna může najít ostatní kdekoli ve vesmíru.“*[13]

Mezinárodní telekomunikační unie roku 2012 vydala dokument s názvem Overview of the Internet of things[2], v rámci kterého definuje několik pojmů včetně *Internetu věcí* takto: *„Jedná se o globální infrastrukturu pro IT společnosti, která umožní využití pokročilých služeb propojením (fyzických i virtuálních) věcí na základě stávajících a vyvíjejících informačních a komunikačních technologií.“*

- *Poznámka 1 – prostřednictvím identifikace, sběru dat, zpracování a komunikačních schopností internet věcí vytváří celé spektrum využití věcí a zároveň zajišťuje, aby byly splněny požadavky na bezpečnost a soukromí.*
- *Poznámka 2 – z obecnějšího pohledu může být Internet věcí vnímán jako vize se sociálními a technologickými dopady.*

Dále pak popisuje rozdíl mezi zařízením a věcí. Zařízení musí splňovat schopnost komunikace s ostatními zařízeními a mělo by poskytovat aspoň jednu z možností snímání, sběr dat, ovládání či zpracování dat. Věc je v kontextu *Internetu věcí* předmět fyzického nebo informačního světa, u které je možné zajistit připojení a komunikaci s internetem.

Můžeme rozdělit zařízení spadající do *Internetu věcí*:

- Vysílač dat – zařízení je přímo připojeno na fyzickou „věc“ a umožňuje bezdrátové připojení této „věci“ do sítě.
- Přijímač dat – zařízení schopné čtení/zápisu dat. Umožňuje také interakci s fyzickou „věcí“. Tato interakce může probíhat nepřímo s vysílačem dat nebo přímo s datovým nosičem.
- Senzor – zařízení detekuje informace z okolního prostředí a převádí je do digitální podoby.
- Obecné zařízení – dokáže komunikovat s internetem přes kabelové nebo bezdrátové spojení. Obecné zařízení může být také sada fyzických věcí.

Mezinárodní telekomunikační unie také popsala model *Internetu věcí*, který se skládá ze čtyř vrstev a to aplikační, servisní, síťové a vrstvy zařízení.

- Aplikační vrstva – obsahuje aplikace *Internetu věcí*.
- Servisní vrstva – jedná se o podporu aplikační vrstvy a sjednocuje dvě podskupiny. Jedna skupina s názvem Generic support capabilities zaštiťuje funkce, které mohou být použity různými aplikacemi jako jsou ukládání či zpracování dat. Druhá skupina Specific support capabilities pojednává o specifických funkcích, které rozšiřují první skupinu.
- Síťová vrstva – i tato vrstva sjednocuje dvě podskupiny a to Networking capabilities a Transport capabilities. První skupina zajišťuje kontrolní funkce při připojování k internetu (autentizace a autorizace). Druhá skupina zajišťuje přenos dat.
- Vrstva zařízení – i tuto vrstvu dělíme na dvě podskupiny Device capabilities a Gateway capabilities. Device capabilities popisuje dva druhy zařízení podle komunikace se sítí přímo nebo nepřímo prostřednictvím Gateway capabilities. Druhá skupina Gateway capabilities popisuje zařízení schopné komunikovat přes rozdílné drátové i bezdrátové technologie (viz 2.6 Technologie přenosu dat).

Nové interakce přinášejí nové možnosti využití v mnoha oborech a jejich následné vylepšení. Můžeme mluvit o chytrých domácnostech s interakcí s chytrými automobily. Vznik nositelných zařízení pro monitorování jednotlivých uživatelů. Interakce s mobilními telefony a mnoho dalších aplikací (viz 2.3 Trendy a možné využití). Díky těmto zařízením dokážeme zlepšit kvalitu mnoha poskytovaných služeb, které budou moci být lépe zacíleny na konkrétního uživatele.

2.2 Vznik Internetu věcí

Z obecnějšího pohledu předchází vzniku několik přelomových událostí, které napomohly k vytvoření bezdrátové komunikace, internetu a v neposlední řadě k *Internetu věcí*.

V roce 1844 byl realizován první telegrafní přenos Morseovy abecedy z Washingtonu do Baltimoru. Za vším stál vynálezce Morseovy abecedy Samuel Morse. V roce 1969 vzniká předchůdce dnešního internetu Arpanet. Tim Berners-Lee 1984 navrhnul World Wide Web. Stejný člověk v roce 1991 vytvořil první webovou stránku. Jako první pojem *Internet věcí* (The internet of Things) použil Kevin Ashton ve svém článku publikovaném v roce 1999.

„I could be wrong, but I'm fairly sure the phrase "Internet of Things"started life as the title of a presentation I made at Procter & Gamble (P&G) in 1999. Linking the new idea of RFID in P&G's supply chain to the then-red-hot topic of the Internet was more than just a good way to get executive attention. It summed up an important insight which is stil often misunderstood.“[1]

V období 2003 – 2004 je pojem *Internet věcí* zmiňován v hlavních „mainstream“ publikacích jako jsou The Guardian, Scientific American a The Boston Globe.

V roce 2005 se pojem dostává do širšího povědomí, kdy Mezinárodní telekomunikační unie ITU OSN zveřejnila svou první zprávu na toto téma.

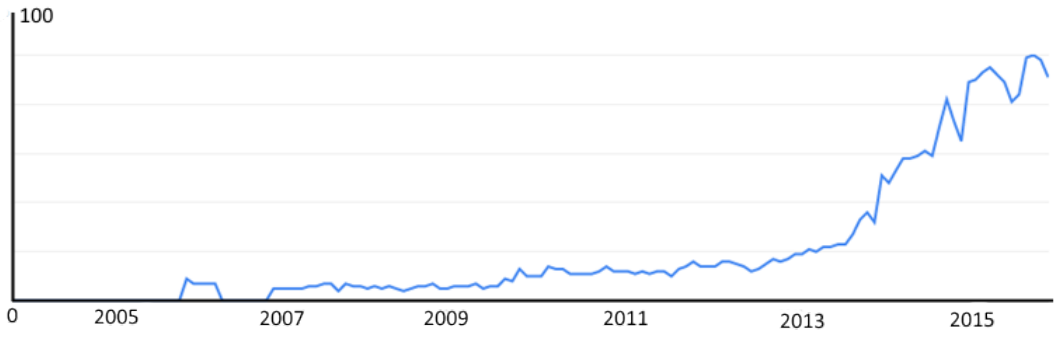
„A new dimension has been added to the world of information and communication technologies (ICTs): from anytime, any place connectivity for anyone, we will now have connectivity for anything. Connections will multiply and create an entirely new dynamic network of networks – an Internet of Things.“[22]

V letech 2006 – 2008 evropská unie uznává význam *Internetu věcí* a je uskutečněna první evropská konference na toto téma.

V roce 2010 prohlásil čínský premiér Wen Jiabao, že *Internet věcí* se stane hlavním a klíčovým průmyslem pro Čínu.

V roce 2011 je veřejně spuštěn protokol IPv6[1], který umožňuje adresovat 2^{128} zařízení v internetu. Stávající protokol IPv4[2] byl adresově vyčerpán 3. února 2011. Pro další možné zařízení bylo potřeba zvýšit adresový prostor.[21]

Vývoj zájmu o *Internet věcí* jde také demonstrovat pomocí databáze četnosti vyhledávání pojmu „Internet of Things“ na stránce www.google.com (viz obrázek 2.1).



Obrázek 2.1: Zájem o *Internet věcí* podle Google[3].

[1] Protokol pro komunikaci v současném Internetu, který nahrazuje starší verzi IPv4.

[2] IPv4 je datově orientovaný protokol, který je používán v internetových sítích (např. Ethernet).

[3] Čísla představují zájem o vyhledávání vzhledem k nejvyššímu bodu v grafu. Představují počet vyhledávacích dotazů, které se týkaly konkrétního výrazu, v poměru k celkovému počtu vyhledávání na Google. Převzato z: https://www.google.com/trends/explore#q=internet%20of%20things

2.3 Trendy a možné využití

V současnosti existuje rozsáhlé spektrum možností[3] pro využití zařízení z kategorie *Internet věcí*. Používání chytrého mobilního telefonu se senzory umožní monitorování pohybu, pozice a například i každodenní zátěž organismu. Umožní také jednoduchým způsobem ovládat ostatní připojená zařízení. Mobilní telefon již dnes zastává roli hlavního ovládacího prvku.

Integrovaný čip v lahvičce od léků připojený na internet dokáže zjistit, zda si uživatel vzpomněl a vzal si své pravidelné léky. V opačném případě umožňuje určitou formou připomenout užití léku.

Zařízení na tělo

Jedná se o tzv. wearable devices neboli nositelné zařízení. Do této kategorie spadají zejména chytré hodinky, náramky a např. chytré brýle (vyvíjené Google Glass[4]).

Zařízení integrovaná do dětského oblečku dokáží v reálném čase monitorovat, zda dítě dýchá, jaká je aktuální teplota pokožky, určí pozici tělíčka. Tyto a další informace neustále odesílají do centrálního zařízení (např. do mobilního telefonu).

Obrázek 2.2: Monitorování dětí (převzato z [3])

Módní značka Ralph Lauren představila pro sportovce Polo Tech Shirt. Jde o chytré tričko, které spolupracuje s mobilním telefonem a cloud aplikací. Tričko sbírá nejrůznější data jako např. tepovou frekvenci, hloubku nádechu, rovnováhu těla. Odešle data ke zpracování a poskytne uživateli přehledné statistiky o pohybu.

Chytrá domácnost

Chytré zásuvky, které jsou ovladatelné dálkově z mobilních zařízení zajistí možnost z jakéhokoliv místa na planetě zapnout nebo vypnout připojené spotřebiče. Umožňuje i monitorování spotřeby zařízení. Lze vytvořit podrobný časový plán provozu zařízení. Vše za účelem snížení výdajů za elektrickou energii.

Světla v domě můžeme z pohodlí pohovky nebo jakéhokoliv jiného místa ovládat, měnit barvu či dokonce můžeme synchronizovat světla s hudbou pro tzv. fototerapii. Světla se automaticky vypnou, když v osvětlené místnosti není nikdo přítomen. Vše vede k úspoře elektrické energie a zvýšení komfortu užívání běžných spotřebičů.

Chytrý spotřebič jako např. tiskárna, která sama detekuje docházející toner a v předstihu objedná z vybraného internetového obchodu nový. Uživatel je upozorněn a stará se jen o převzetí zásilky a instalaci nového toneru do tiskárny.

[4] Jde o nositelný počítač s náhlavním displejem vyvíjen společností Google.

Dalším chytrým zařízením je kartáček na zuby od společnosti Kolibree, který se spojí s mobilním telefonem a prostřednictvím her a mini úkolů se snaží, hlavně pro děti, udělat z čištění zubů radost a zábavu. Kartáček navíc umožňuje odesílat nashromážděná data zubaři, který podle informací přizpůsobí např. datum preventivní prohlídky.

Petnet's smart feeder (viz obrázek 2.3) jsou chytré misky, které dokáží dávkovat krmivo pro psy nebo kočky podle jejich fyzických proporcí. Dokáží objednat jídlo pro mazlíčka, pokud dochází. Vše je ovládáno prostřednictvím aplikace mobilního telefonu, která také vede statistiky o spotřebě potravy zvířete.

Obrázek 2.3: Miska pro domácí mazlíčky Petnet's[5].

Pračky Whirpool zase objednají nový prací prostředek. Samotná myšlenka jednoduchého objednání potřebných položek je dále rozvinuta např. tzv. Dash Buttonem (viz obrázek 2.4) od společnosti Amazon. Toto jednoduché zařízení se nalepí na spotřebič (např. obyčejná pračka) a jednoduchým stiskem tlačítka lze objednat potřebný prací prostředek z portálu www.amazon.com.

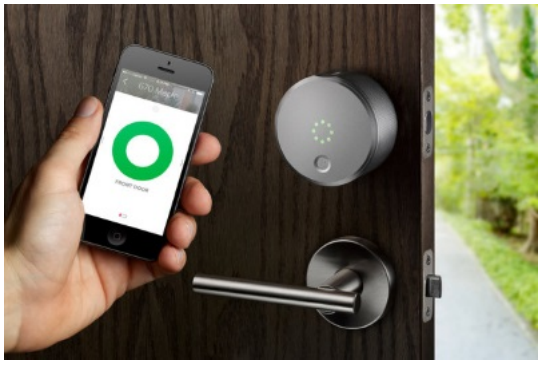
Obrázek 2.4: Amazon Dash Button[6].

Nest Thermostat od společnosti Google dokáže komunikovat s vytápěcím zařízením jako jsou kotle či bojlery na ohřev teplé vody a tím nastavovat teplotu po celém domě. Tento termostat se od běžného termostatu liší tím, že se dokáže učit, jaká teplota je pro uživatele nejvhodnější v průběhu dne, týdne, ročního období. Vše lze pohodlně nastavovat a ovládat prostřednictvím mobilního telefonu.

August Smart Lock (viz obrázek 2.5) je chytrý zámek, který rozpozná, že se blížíte domů (se svým mobilním telefonem), automaticky odemkne dveře a za vámi znovu zamkne. Pro-

[5]Převzato z: http://www.petnet.io/.
[6]Převzato z: http://www.engadget.com/2015/03/31/amazon-dash-button/.

střednictvím mobilní aplikace lze udělit práva i přátelům či známým. Zámek však obsahuje i klávesnici pro zadání číselného kódu (pokud právě nemáme mobilní telefon).



Obrázek 2.5: August Smart Lock[7].

Chytrá města

Chytrý koš, který odesílá data do centrály úklidové firmy ve městě podle toho, jak je zaplněný a kdy bude potřebovat vyprázdnit. Napomůže k zajištění čistějších ulic a zlevnění údržby čistoty měst.

Obrázek 2.6: Chytrý koš (převzato z [3])

Monitorování stání automobilů ve městě napomůže k lepšímu parkování. Jsou sdílena data s obsazenými a volnými parkovacími místy. Lidé rychleji zjistí aktuální vytížení dostupných parkovacích míst. Pomocí dopravních dat se může lépe a rychleji ovládat aktuální doprava. Což vede také ke snížení emisí a celkovému snížení znečištění ovzduší měst.

Chytrá pouliční světla přizpůsobují svícení podle aktuálního počasí, viditelnosti a denní doby. Města dokážou snížit spotřebu elektrické energie a snížit světelné znečištění.

Chytré továrny

Senzory instalované uvnitř zařízení sledují, zda nejsou některé části strojů a zařízení více namáhány a zda nepřekročily limity deformace. Pomocí nasbíraných dat dokáží odborníci předvídat výdrž zařízení. Zajistí se efektivnější plánování servisní služby či zlepšení bezpečnosti více namáhaných součástí.

[7]Převzato z: http://recode.net/2014/10/14/review-a-high-tech-door-lock-thats-also-simple/.

Firma Black and Decker na veletrhu CES[8] na začátku roku 2016 představila vrtačku s chytrou baterií, kterou lze spárovat s mobilním telefonem. V telefonu se zobrazují podrobné informace o stavu baterie. Na dálku lze baterii uzamknout, a tak zabránit cizímu použití nebo lze vrtačku lokalizovat. Baterie obsahují USB konektor pro využití jako power banka k nabíjení ostatních zařízení.

Chytré hasicí přístroje upozorní centrální dispečink hasičské služby o poklesu tlaku v hasicích přístrojích. Může to znamenat, že jsou právě v provozu z důvodu požáru. Umožňují odeslat i data o své poloze. Tyto souhrnné informace přispívají k rychlejší a přesnější reakci na možný požár.

Obrázek 2.7: Chytrý hasicí přístroj (převzato z [3])

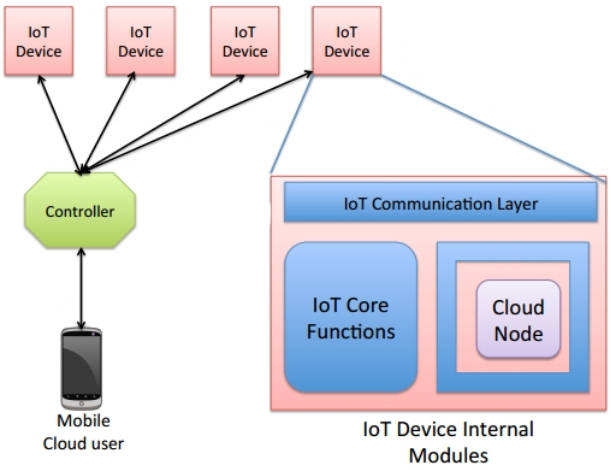
Internetu věcí není však jen zařízení řízená centrální aplikací či jiným přístrojem. Věci by měly komunikovat i mezi sebou. Znamenalo by to masivnější propojení a vzájemnou interakci. Pro představu by např. chytré žárovky poskytovaly své teplotní čidla klimatizaci. Ta by dokázala na základně informací ze žárovek přizpůsobit ochlazování místností v domě. Pokud by tato zařízení v domácnosti komunikovala, vytvořila by chytrou domácnost mnohem efektivnější, než na sobě nezávislá elektronická zařízení. Ve větším měřítku je možné si představit takto vybavené chytré firmy, společnosti, města i státy.

Velký výpočetní výkon

Projekt Aura[28] inženýrů z Alabamské univerzity představuje možnost využít výpočetní výkon zařízení připojených do *Internetu věcí*, jelikož většinou všechna tato zařízení obsahují nebo budou obsahovat jednoduchý čip (např. ARM), který většinu času nebude aktivní. Mnoho těchto jednoduchých čipů v kombinaci s domácími počítači, které disponují větším výkonem, by poskytovaly možnost využít mnohonásobně vyšší výpočetní výkon (viz obrázek 2.8). Celé schéma se skládá z M-agenta, Controlleru a Internet of Things devices.

- M-agent – jedná se např. o mobilní telefon, notebook, tablet. Na těchto zařízeních běží cloud aplikace. Pokud se uživatel s tímto zařízením objeví v přímém dosahu domácnosti, M-agent podá podrobné informace o práci, době potřebné k dokončení úkonu, celkovou doba běhu, zpracovaný objem dat atd.
- Controller(s) – poskytuje komunikační a výpočetní abstrakci mezi M-agentem a Internot of Things devices. Zachytí požadavek výpočtu, analyzuje jej a rozhodne o nejlepším rozdělení do jednotlivých zařízení (např. i podle výpočetní ceny).

[8] Consumer Electronics Show je veletrh spotřební elektroniky konaný každoročně v Las Vegas.



Obrázek 2.8: Projekt Aura (převzato z [28])

- Internet of Things devices – zařízení spadající do *Internetu věcí* s integrovanou částí Aura. Tato zařízení poskytují vlastní specifikace (rychlost výpočtu, stav paměti, energetickou náročnost, bezpečnostní protokoly atd.) a rozšiřují možnosti použití.

2.4 Zabezpečení

„Internet věcí se stává stimulem obrovské „demokratizace“, kdy data jsou v reálném čase sdílena v takovém rozsahu jako dosud nikdy. Paradoxně tato zásadní přednost, tj. potenciál okamžitě sdílet data s kýmkoli a s čímkoli, vytváří obrovskou bezpečnostní hrozbu.“[20]

Zabezpečení zahrnuje utajení osobních informací a schopnost kontroly, co se s informacemi děje. Lidské právo na soukromí je důležitým aspektem v otázce zabezpečení dat poskytovaných prostřednictvím *Internetu věcí*.

Zabezpečení je jeden z největších problémů *Internetu věcí*. Problémy jsou spojeny především se špatným zabezpečením webu a webového rozhraní. Další překážkou je špatná autentizace. Používáním cloud úložišť a používáním různých mobilních zařízení se špatným zabezpečením také nepřispívá ke kvalitní ochraně dat.

Je třeba přistupovat k otázkám zabezpečení zařízení po celou dobu „životního cyklu“ zařízení.[30]

Při prvním zapnutí zařízení je třeba aplikovat tzv. Secure booting. Musí se provést kontrola pravosti a neporušitelnosti software v zařízení pomocí kryptograficky generovaném digitálním podpisu. Slouží jako klasický podpis např. na šeku pro ověření pravosti. Ověřuje a verifikuje se pravost původního schváleného software. Pokud vše proběhlo v pořádku, zařízení se svěří důvěra. Nyní je třeba zařízení chránit před tzv. run-time hrozbami.

Další úrovní zabezpečení je tzv. Access control. V této fázi dochází ke kontrolám přístupů k zařízení či kontrolám zdrojů dat. Tyto kontroly by měly být vestavěny do operačního systému a měly by omezit práva přístupu samotným zařízením a aplikacím. Jsou udělena práva k přístupu jen k těm zdrojům dat, ke kterým nezbytně potřebují pro vykonávání své úlohy přistupovat. Je-li některá komponenta sítě narušena, řízení přístupu odpovídá za řešení tohoto problému a za minimální přístup narušitele do ostatních částí. Důležité je řídit se principem nastavení minimálních práv zařízením, jaká jsou nezbytná ve snaze snížit rizika narušení bezpečnosti.

Třetí fáze zabezpečení je tzv. Device authentication. Když už je zařízení připojeno do sítě, mělo by se ověřit před příjmem a vysíláním dat. Vestavěné systémy (embedded devices[9]) často nemají klávesnici, aby uživatel provedl klasickou autorizaci pomocí jména a hesla. Princip zařízení je podobný, jen jsou potřeba k ověření data, která jsou uložena v tzv. secure storage area (zabezpečovací sklad). Porovnáním dat ze zařízení a skladu se umožní autorizace.

Čtvrtá fáze je známa jako tzv. Firewall, kde dochází ke kontrole samotných paketů. Z obecnějšího hlediska jde o kontrolu přenosu dat. Nejvíce je třeba kontrolovat pakety, které by mohly jakýmkoli způsobem omezit provoz zařízení. Existuje mnoho různých protokolů, kterými komunikují zařízení (viz 2.7 Protokoly). Jelikož existuje více standardů komunikace, je vyžadována důkladnější kontrola. Není však potřeba kontrolovat přenos na vyšších přenosových síťových vrstvách. O to se starají síťové aplikace.

Poslední úroveň zabezpečení je tzv. Updates and patches. Jelikož je již zařízení v provozu, nevyhne se aktualizacím software či použití patches[10]. Je třeba důsledně kontrolovat všechny změny software, aby nezpůsobily snížení zabezpečení zařízení.

Všechny tyto fáze musí soukromé podniky, které se rozhodnou využít *Internet věcí*, popsat ve svém modelu řízení rizik[11], podle kterého se řídí obecné aktivity firmy.

Byla vyvinuta celá řada technologií k dosažení cílů ochrany osobních údajů obecně nazývaných Privacy Enhancing Technologies (PET).[14]

- Virtual Private Networks (VPN) – jde o spojení několika zařízení do soukromé sítě. Do sítě je možné připojit jen ověřené zařízení. Nevýhodou je, že není umožněna dynamická výměna informací z internetu, jelikož se jedná o uzavřenou síť.
- Transport Layer Security (TLS) – jedná se o model, který umožňuje aplikacím komunikovat po síti způsobem, který zabraňuje odposlechům a ztrátě osobních dat pomocí užití kryptografie.
- DNS Security Extensions (DNSSEC) – jsou specifikace, které zabezpečují poskytování informací prostřednictvím DNS systémem v IP sítích. Využívá metody asymetrického šifrování. Zabezpečení DNS zvětšuje objem dat, který se musí přenášet po síti.
- Onion Routing – metoda šifrování dat do více vrstev („cibulové směrování“) využívá alternativní routery po síti podporující toto směrování. Jednotlivá přenosová zařízení mají pouze omezené informace o datech (od koho data přichází a kam je má zařízení poslat). Nelze však zjistit zdroj dat. Každá vrstva dat je zašifrovaná odlišným klíčem. Na jednotlivých zařízeních se vždy jedna vrstva dekóduje a na konci přenosu zbudou jen holá data. Metoda šifrování dat však výrazně zvyšuje požadavky na přenos dat.

Rizika

Zvýšená bezpečnostní rizika s rostoucím využíváním *Internetu věcí* si uvědomuje i americký Federální úřad pro vyšetřování (FBI), který dne 13. října 2015 vydal článek upozorňující na možná nebezpečí.[24]

Text článku zejména upozorňuje na možnost vstupu přes *Internetu věcí* do domácí či firemní internetové sítě, na možnost odcizit chráněná data jako jsou identifikační údaje, bankovní účty, čísla kreditních karet. Také upozorňuje na možné zneužití internetové schránky

[9] Jednoúčelový systém, ve kterém je řídicí počítač zcela zabudován do zařízení, které ovládá.

[10] Jedná se o nástroj, který provede změny ve stávajícím software za účelem opravy či aktualizace.

[11] Oblast řízení projektů i procesů, která se zabývá zjišťováním a hodnocením jejich nebezpečí a nežádoucích důsledků.

či možné sledování a odposlouchání celé síťové infrastruktury za účelem získání citlivých dat.

Hlavní ochranou je míněna lepší ochrana lokální počítačové sítě. Odborníci doporučují zvážit nastavení sítí pomocí zkušených odborníků a neponechávat na síťových prvcích tovární nastavení či velmi slabá zabezpečení pomocí snadno uhodnutelných hesel. Také je kladen důraz na pochopení celé problematiky.

2.5 Cloud computing

Existuje mnoho definic tohoto pojmu. Z českých definic je nejznámější od autora Jana Kodery: *„Cloud computing označuje souhrnně technologie a postupy používané v datových centrech a firmách pro zajištění snadné škálovatelnosti aplikací dodávaných přes internet.“*[17]

Přední světová firma v oboru informačních technologií International Business Machines Corporation (IBM) popisuje cloud computing (často jen „the cloud“) jako poskytování on-demand[12] výpočetních zdrojů (všechno od aplikací po datová centra) prostřednictvím internetu na principu modelu pay-for-use[13].

V širším pohledu jde o poskytování služeb (např. počítačový software, e-mailové schránky, datová úložiště, atd.) uložených na internetových serverech. Uživateli je přímo propůjčen výpočetní výkon serverů. Přístup je realizován skrze webový prohlížeč, což vytváří možnost používání služeb takřka odkudkoli. Využití služeb může být bezplatné a uživatel tedy nemusí zaplatit za vlastní software. Cloud computing znamená, že více uživatelů využívá stejné zdroje (tj. multitenance), což klade důraz na jejich kvalitu (hardware i software).

Důležitou vlastností cloudu je zvýšené zabezpečení dat. Jelikož jsou však data uložena u poskytovatele cloudu, uživatel se na něj stává zcela závislým. Pokud se např. určitá firma rozhodne využít software poskytovaný cloudem, ztrácí možnost ovlivnit, kterou verzi bude používat. Firma také musí počítat s tím, že s postupem času se z bezplatných služeb mohou stát služby placené nebo vznikne nutnost placení tzv. mikrotransakcí[14]. V dnešní době se můžeme setkat i s plnohodnotnými operačními systémy, které běží v cloudu.

Podle rozsahu poskytovaných služeb v rámci cloud computingu jej můžeme rozdělit do několika skupin:[25]

- Infrastruktura jako služba (IaaS) – cloud poskytuje kompletní infrastrukturu (nejčastěji virtualizaci). Zabezpečení a servis služeb spadá zcela do povinností poskytovatele. Odpadá nutnost investice do vlastního hardware.
- Platforma jako služba (PaaS) – cloud poskytuje prostředky pro celý životní cyklus tvorby a poskytování webových aplikací. Výhodou je rychlý vývoj a nasazení aplikací na trh.
- Software jako služba (SaaS) – uživatel si kupuje či pronajímá přístup k aplikaci, ne aplikaci samotnou. Služby mohou být dynamicky škálovatelné podle potřeb uživatele.

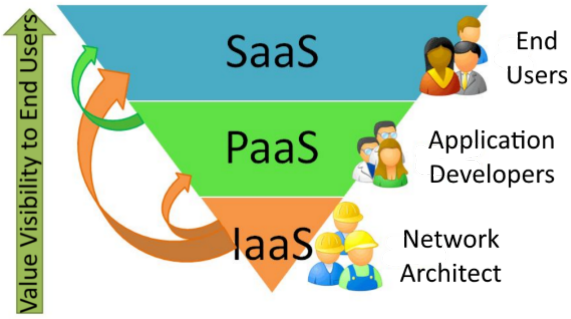
Podle firmy IBM se můžeme setkat s rozdělením cloud computingu také podle toho, jak je samotný cloud poskytován.[26]

[12] Služby nebo vlastnosti, které se zaměřují na potřeby uživatele pro okamžité uspokojení a bezprostřednost použití.

[13] Model využití služeb po zaplacení většinou nízkých transakcí a tyto transakce mohou být automatizovány.

[14] Pro zlepšení poskytovaných služeb je třeba část obsahu zakoupit.

[15] Převzato z: http://masters.donntu.org/2012/iem/shargorodsky/diss/indexe.htm.



Obrázek 2.9: Rozdělení cloud computingu podle poskytovaných služeb[15].

- Veřejný cloud – je poskytován společnostmi, které nabízejí rychlý přístup přes veřejnou síť k výpočetním prostředkům. Uživatel nemusí pořizovat vlastní hardware ani software, vše vlastní a spravuje poskytovatel.
- Privátní cloud – infrastruktura provozována výhradně pro jednu organizaci. Hlavní výhodou je přizpůsobení podle potřeb zákazníka.
- Hybridní cloud – jedná se o kombinaci veřejných a privátních cloudů, jelikož privátní cloud většinou nemůže existovat bez ostatních IT zdrojů a veřejného cloudu dané společnosti.

Obrázek 2.10: Veřejný (převzato z [26])

Obrázek 2.11: Privátní (převzato z [26])

Obrázek 2.12: Hybridní (převzato z [26])

John McCarthy se roku 1960 stal autorem první myšlenky sdílení výpočetního výkonu na internetu a je tedy považován za autora tohoto modelu. K velkému rozšíření až do dnešní podoby přispěla firma Amazon[16], která v roce 2002 vytvořila službu Amazon Web Services[17] (AWS). Hlavním důvodem byla snaha o efektivnější využití kapacity výpočetní techniky. Z velké části provozní doby tato technika nebyla naplno využita proto, že byla navržena pro případy vyššího okamžitého výpočetního výkonu v různých obdobích (např. typicky před koncem roku).

Jako příklady nejznámějších cloud computingu můžeme uvést:

- Google Apps (SaaS), který zastřešuje např. e-mail, docs, gtalk, kalendář...

[16] Internetový obchod patřící americké společnosti Amazon.com, Inc. ve státě Washington. Patří mezi nejstarší a největší obchody svého druhu.

[17] Cloud, který se skládá z mnoha služeb (např. databáze, výpočetní služby, monitorování či platby), které si mohou uživatelé pronajmout nezávisle na sobě.

- Microsoft 365 (SaaS), který zastřešuje např. dokumenty, weby, videokonference...
- Amazon EC2 (PaaS), který je v rámci Amazon Web Services (AWS) a nabízí pronájem virtuálních počítačů.
- IBM Cloud (Saas, PaaS, IaaS), který zastřešuje zejména komerční služby.

2.6 Technologie přenosu dat

Existuje velký výběr z technologií pro připojení a komunikaci jednotlivých zařízení z kategorie *Internet věcí*. Klíčové vlastnosti jednotlivých technologií jsou dosah, náročnost zpracování dat, bezpečnost, energetická náročnost a rychlost přenosu dat.

V této části je často užíván pojem šířka pásma. Jde o jeden z dílčích aspektů ovlivňující přenos digitální informace spolu s dalšími jako jsou např. použité kódování, šum. Jedná se o rozsah přenášeného signálu. V pásmu od 2,40 GHz do 2,48 GHz je šířka pásma 0,08 GHz neboli 80 MHz.

Pásmo je následně rozděleno do rovnoměrně velkých kanálů. Technologie bluetooth např. používá 79 kanálů nebo WiFi standard 802.11b rozdělí uvedených 80 MHz do 22 MHz širokých 5 MHz od sebe posunutých překrývajících se kanálů (viz příloha D.1). Překrývající kanály se mohou navzájem rušit.

Bluetooth

Technologie bluetooth[7] je určena pro bezdrátovou komunikaci na krátkou vzdálenost mezi několika elektronickými zařízeními. Je definovaná standardem IEEE[18] 802.15.1. V roce 1998 vznikla skupina firem (Ericsson, IBM, Intel, Nokia, Toshiba a později se přidaly další) pro vytvoření standardu bezdrátové komunikace pro WPAN[19] za účelem redukovat množství kabelů při připojování zařízení k PC. Bluetooth je rozdělen do několika verzí. Nejnovější verze je 4.2 (viz níže), která byla vytvořena v roce 2014, a která v sobě zahrnuje protokol 6LoWPAN[20].

Bluetooth využívá k přenosu radiové vlny v bezlicenčním pásmu 2,402 GHz – 2,480 GHz rozdělené s odstupem 1 MHz do 79 kanálů. Maximální dosah komunikace je 100 m s přímou viditelností, ale většinou bývá nižší. Velkou výhodou je možnost používat nízký vysílací výkon. Podporuje také hlasové přenosy. Vyznačuje se komunikací typu master-slave. Zařízení master může být synchronizováno až se sedmi zařízeními slave. Slave zařízení z podstaty komunikace nemohou přímo komunikovat mezi sebou. Zařízení Bluetooth jsou rozdělena do tří tříd (class) podle výkonu vysílání (viz tabulka 2.1). Rostoucí výkon ovšem zvyšuje energetické nároky. Dvě zařízení s rozdílnou třídou (např. 1 a 2) se musejí dostat do vzájemného dosahu, což znamená, že zařízení s třídou 1 musí být ve vzdálenosti maximálně 20 m od zařízení s třídou 2.

Technologie bluetooth se během několika let vyvíjela.[37] Počátky vzniku první verze se datují do roku 1999. Během tohoto roku postupně vznikaly verze *1.0a* a *1.0b*. Potýkaly se však s mnoha technickými problémy zejména s kompatibilitou jednotlivých zařízení a s přiřazováním rolí master a slave. Používaly také povinné hardwarové adresy pro zařízení s bluetooth (BD_ADDR).

[18] Ústav elektrotechnických a elektronických inženýrů. Koordinuje mj. tvorbu mezinárodně uznávaných výpočetních a komunikačních norem.

[19] Bezdrátové soukromé sítě.

[20] Standard pro bezdrátovou technologii využívající síťový protokol IPv6 vyznačující se nízkou spotřebou.

Třída	Dosah	Maximální výstupní výkon	Minimální výstupní výkon
1	100 m	100 mW	1 mW
2	20 m	2,5 mW	0,25 mW
3	1 m	1 mW	není stanoveno

Tabulka 2.1: Třídy bluetooth

Až verze *1.1* v roce 2001 způsobila masové rozšíření této technologie do komerčních produktů. O rok později byla schválena jako standard IEEE 802.15.1. Již v této verzi došlo k přidělení podpory pro nešifrované kanály a indikaci síly signálu. Další verze *1.2* byla definována v roce 2003. Jednalo se o velké změny ve specifikaci standardu. Došlo k zrychlení přenosu a také ke zrychlení vyhledávání zařízení. Integrovala se funkce přeskakování frekvence tzv. Adaptive Frequency Hopping (AFH). Jelikož bluetooth pracuje v bez licenčním pásmu ISM, které je využíváno i jinými technologiemi (např. WiFi 802.11b), docházelo často ke kolizím při současné komunikaci. AFH umožňuje komunikaci přizpůsobit se prostředí tím, že určí pevné zdroje rušení a dojde k jejich vyloučení ze seznamu dostupných kanálů. Verze *1.2* se roku 2005 také stala standardem IEEE 802.15.1.

Roku 2007 byla představena verze *2.1+EDR*. Opět došlo k navýšení přenosové rychlosti. Je kompatibilní s nižší verzí a její hlavní rys je párování zařízení pomocí tzv. Secure simple pairing (SSP), což způsobilo lepší zabezpečení pomocí generování tzv. Link key. Zařízení může podle něj rozhodnout, zda je připojení bezpečné nebo zahájit nový proces párování, což generuje nové Link keys.

Specifikace verze *3.0+HS* byla vytvořena 21. dubna 2009. Přenosová rychlost vzrostla až na teoretickou hodnotu 24 Mb/s. Integrovaná je funkce Alternate MAC/PHY (AMP). Bluetooth zahrnuje vyhledávání zařízení, počáteční připojení a konfiguraci. Pro přenos dat však používá další vrstvu (MAC PHY 802.11), což znamená, že během nečinnosti je využíván nižší výkon modulu. Při přenosu velkého množství dat roste přenosový výkon. Tato technologie však u verze *3.0* není podporována.

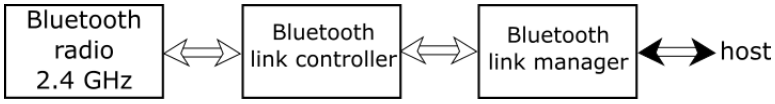
V červenci roku 2010 vznikla verze *4.0*. Tato verze nemá nahrazovat stávající verzi *3.0*. Důkazem je nižší přenosová rychlost. Novější standard klade důraz na nižší energetickou náročnost použitím velmi krátkých datových paketů. Zefektivnilo se také uspání a probuzení hostitelského zařízení. Poprvé došlo k situaci, kdy se bluetooth technologie rozdělila na dva typy podle rozdílného použití. Zatím co verze *3.0* díky své rychlosti přenosu cílí do zařízení s potřebou přenosu velkého objemu dat (video, zvuk, fotografie), tak verze *4.0* cílí spíše do jednodušších zařízení a vestavěných systémů. Tento typ bluetooth lze také implementovat v tzv. dual-mode, což znamená, že na již stávající čipy *2.1* a *3.0* lze implementovat nízkoenergetickou funkci *4.0*.

Všechna zařízení, pokud jsou zaplá a viditelná, poskytují o sobě informace např. název zařízení, třídu zařízení, seznam služeb a dále pak technické informace (výrobce). Při prvním navázání spojení (proces párování) jsou tyto informace předány a uloženy. Pokud již v minulosti byla tato zařízení připojená, nedochází k výměně základních informací a ihned dochází ke spojení. Každé zařízení má vlastní 48 b adresu, avšak častěji se můžeme setkat s popisem pomocí jednoduchého názvu definovaného výrobcem, který lze změnit.

Hardwarová část bluetooth se skládá ze tří základních komponent.

- Bluetooth radio – vysílač a přijímač v pásmu 2,4 GHz. Dělení do tříd (viz tabulka 2.1).
- Bluetooth Link Manager – připravuje data pro komunikaci.

- Bluetooth Link Controller – zařízení typu master a řídí modul bluetooth radio. Stará se o navázání spojení, identifikaci, přístup a komunikaci. Může dojít ke spojení několika zařízení a vznikne síť s označením PICONET.



Obrázek 2.13: Hardwarová struktura bluetooth zařízení.

BLE

Bluetooth Low Energy[7] neboli BLE (často označováno také jako Bluetooth Smart) je jedna z novinek Bluetooth ve verzi *4.0*. Aliance Bluetooth SIG, která se nejvíce podílí na vývoji Bluetooth se ve verzi *4.0* nejvíce zaměřila na prozatímní nedostatky této technologie. Jelikož se Bluetooth snaží proniknout do nízkoenergeticky náročných zařízení, byla hlavní snaha snížit spotřebu. Pokud by se snižoval vysílací výkon, vedlo by to i k nižšímu dosahu technologie. Tato cesta tedy nebyla zvolena. BLE se snaží oproti původním Bluetooth snížit dobu, za kterou se naváže spojení se zařízením, proběhne komunikace a následné uspání zařízení (celkově jde o tzv. enumeration time). Tato doba je až 20x nižší než u předchozích verzí.

O technologii BLE by se dalo říci, že zaplnila místo na trhu. BLE se stal standardem roku 2010, zaznamenal však neobvykle rychlý schvalovací proces a také rychle rostl počet navrhovaných zařízení s touto technologií. Vše souvisí s tehdejším nárůstem poptávky o smart telefony a tablety. Samotná technologie bluetooth byla lákavou marketingovou značkou a BLE znamenalo jen další vývojový stupeň, který ve svých telefonech integrovaly největší firmy vyrábějící telefony jako je Apple a Samsung.

Bluetooth 4.2

Tato verze Bluetooth se stala základem a nástrojem pro další rozvoj *Internetu věcí*. V předchozích verzích byly technologie typu Bluetooth Smart (často označované jako BLE) a Bluetooth Smart Ready, což definuje dvě odlišná zařízení komunikující mezi sebou. První tzv. Smart (nízkoenergetické zařízení jako např. chytré žárovky, senzory atd.) posílá svá naměřená data do druhého zařízení tzv. Bluetooth Smart Ready (mobily, PC atd.), které tato data interpretuje. Jde tedy o určitou mezivrstvu.

Nová verze však přináší novinku v podobě Internet Protocol Support Profile (IPSP). Tato technologie využívá protokol IPv6/6LoWPAN pro přístup k internetu. Tato novinka umožňuje zařízením Smart přístup k internetu bez nutnosti dalšího zařízení. Zlepšení úspory energie se tedy nejvíce projeví v úsporných režimech, které se však stávají prioritní pro zařízení v rámci *Internetu věcí*. Je důležité zmínit, že rozdíl mezi verzí *4.0* a *4.2* je pouze v software. Je tedy zachována zpětná kompatibilita s nižší verzí a je tak možné starší čipy, které pracující s nižší verzí, aktualizovat.

Nejnovější verze *4.2* má zatím na trhu nízké HW zastoupení. Stále však platí nejvyšší přenosová rychlost 24 Mb/s ještě od verze *3.0+HS*. Aliance Bluetooth SIG také uvádí, že došlo k výraznému zlepšení zabezpečení komunikace.

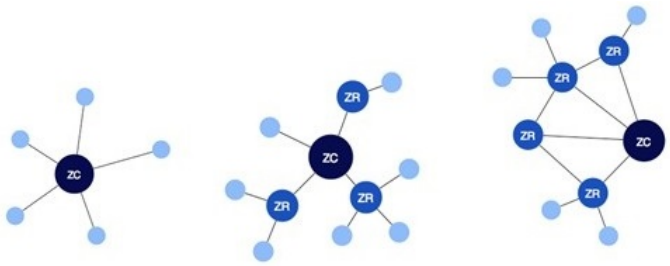
ZigBEE

Rádiová technologie ZigBEE[10] je podobná technologii bluetooth. Je definovaná standardem IEEE 802.15.4 od kroku 2004. Jejím hlavním zaměřením jsou nízkoenergetické zařízení (zdravotní péče, domácí spotřebiče, počítačové periferie nebo řada zařízení spadajících do

Internetu věcí). Autorem technologie je skupina ZigBee Alliance, která sdružuje společnosti jako jsou Texas Instruments, Samsung, AT&T, Philips, Huawei, Intel a Cisco. ZigBEE obecně pracuje v pásmu 2,4 GHz. V Evropě se můžeme setkat s pásmem 868 MHz, v Číně 784 MHz a v Americe zase s 915 MHz. Dosah komunikace činí maximálně 100 m. Největší rozdíl je však v přenosové rychlosti, která dosahuje hodnot 20, 40 nebo 250 kb/s. Není tedy vhodná pro přenos velkého objemu dat (fotky, videa). Nejnovější verze ZigBEE se nazývá Pro. Byla představena roku 2007 a je dodržena kompatibilita se starší verzí.

Komunikace je rozdělena do tří vrstev:

1. Fyzická – tato vrstva definuje způsob vysílání, užívané frekvenční pásma a komunikační protokol.
2. Síťová – definuje topologii sítě (viz obrázek 2.14). Dále je pak definováno zabezpečení pomocí algoritmu AES.
3. Aplikační – popisuje proces párování zařízení. Dále pak ZigBEE objekty a jejich role v síti.



Obrázek 2.14: Topologie sítě ZigBEE. Zleva Star, Tree a Mesh[21].

Existují tři rozdílná hardwarová zařízení.[38]

- ZigBee Coordinator (ZC) – jedná se o nejschopnější zařízení. Tvoří kořen stromu sítě a pomocí něj lze propojit více sítí (slouží jako most). V síti se může nacházet pouze jedno takové zařízení. Umožňuje shromažďovat informace o síti, stará se o zabezpečení a slouží jako úložiště pro zabezpečovací klíče.
- ZigBee Router (ZR) – sloužící jako směrovač v topologii, který přeposílá data v rámci sítě.
- ZigBee End Device – tato zařízení obsahují jen tolik funkcionality, aby dokázaly komunikovat s ZC a ZR. Jedná se o koncové zařízení s nízkou spotřebou a výkonem. Díky tomu, že koncová zařízení jsou značnou dobu v úsporném režimu, prodlužuje se výdrž baterie. Jejich výrobní náklady jsou nižší než u ZC a ZR.

Základním mechanismem pro zajištění bezpečnosti a ochrany dat je symetrická kryptografie[22] pomocí 128 bitových klíčů. Je tedy nutné, aby obě komunikující strany měly tyto klíče. Klíče se nikdy nepřenášení po nezabezpečených tocích dat. Nejčastěji se distribuují z tzv. Trust center. Pro eliminaci jakéhokoli předávání klíčů mohou být klíče přednastaveny výrobcem pro každé jednotlivé zařízení zvlášť. Existuje několik typů klíčů. „Master key“

[21] Převzato z: http://www.ni.com/white-paper/7118/en/.
[22] Zpráva šifrovaná vybraným klíčem je tímto klíčem také dešifrovatelná na prostý text.

slouží pro odvození ostatních klíčů a je základním kamenem dlouhodobé bezpečnosti sítě. Musí být získaný prostřednictvím zabezpečeného média (např. předinstalovaný výrobcem), protože na něm závisí bezpečnost celé sítě. „Link key“ vytváří unikátní komunikaci mezi dvěma zařízeními pomocí šifrování. „Network key“ je nejčastěji uložen v trust center a je používán k broadcast[23] komunikaci.

Z-Wave

Bezdrátová technologie Z-Wave[11] byla vyvinuta společností Zensys spadající do Z-Wave Alliance (podobné jako ZigBee Alliance). Aliance sdružuje firmy jako Cisco, HP, AT&T a Honeywell. Cílem a hlavním využitím je chytrá domácnost se zařízeními jako jsou např. chytré žárovky, vzduchotechnika, termostaty a zámky dveří (obecně nízkoenergetická zařízení). Klade důraz na nízké pořizovací náklady zařízení. Pracuje na frekvenci 868,42 MHz v Evropě a v Americe na 908,42 MHz. Jedná se spíše o méně využívané frekvence, a tak dochází jen k malé míře rušení vlivem ostatních technologií. Dosah signálu na otevřeném prostranství je udávaný až 100 m (v budovách zhruba poloviční). Zařízení tvoří privátní síť (PAN) topologie mesh.

Základním prvkem sítě je Z-Wave Controller[39]. Jedná se o centrální zařízení, které řídí ostatní prvky sítě. Abychom přidali další zařízení, je třeba provést proces párování. Nejčastěji se jedná o stisknutí předem definované kombinace tlačítek na controlleru a na přidávaném zařízení (podobný proces pro odstranění). Celý proces je třeba provést jen jednou, avšak pro všechna zařízení. Informace jsou uloženy v controlleru a příště se provede proces párování automaticky. Controller si také pamatuje sílu signálu. Tato informace pomáhá při rozpoznávání jednotlivých zařízení. Je doporučeno, aby v době párování byly přístroje umístěny na svém finálním místě. Přesun samotného controlleru je možný díky vestavěné baterii, která je využita při vypnutí přístroje, aby nedošlo ke ztrátě dat.

Všechny privátní sítě jsou jednoznačně identifikované pomocí Network ID (někdy také Home ID) a každý uzel v síti pomocí Node ID. Network ID má délku 32 b a při procesu párování je pomocí controlleru přiřazen všem ostatním uzlům. Pokud mají uzly rozdílnou Network ID, nedokážou mezi sebou komunikovat. Topologie mesh zajišťuje komunikaci pomocí tzv. mezi-uzlů. Zpráva z uzlu X směřuje do uzlu Y. Pokud však nejsou ve vzájemném dosahu, je využit mezi-uzel Z, který má v dosahu obě zařízení. Obecně se dá říci, že více zařízení zvyšuje dosah sítě.

WiFi

Technologie Wireless Fidelity[15] neboli WiFi je označení několika standardů 802.11x (x zastupuje jednotlivé verze) instituce IEEE popisující bezdrátovou komunikaci používající elektromagnetické rádiové vlny v sítích WLAN[24]. Důvodem vzniku byla snaha připojit přenosná zařízení do firemních sítí LAN bez nutnosti užití kabelového ethernetu. Je používáno bezlicenční frekvenční pásmo 2,4 GHz. Rozvoj této technologie přinesl velké zahlcení této frekvence.

Vznik technologie WiFi se datuje do roku 1997, kdy vznikl první standard s označením 802.11. Tato první verze dosahovala rychlosti 2 Mb/s. Frekvenční pásmo bylo definováno v rozsahu od 2,400 GHz do 2,485 GHz a bylo celé využíváno jedním zařízením při aplikovaní hoppingu (změna frekvence po určitém datovém rámci).

O dva roky později (16. září 1999) vznikly dva standardy 802.11a a 802.11b. Standard „a“ pracuje s pásmem od 5,745 GHz do 5,805 GHz, díky čemuž dosahuje nižších vzdáleností

[23] Zpráva, která je v síti cílená na všechna připojená síťová rozhraní.
[24] Bezdrátová místní síť.

a je nekompatibilní s „b“. Rychlost „a“ standardu vzrostla na 54 Mb/s a u pomalejšího standardu „b“ na 11 Mb/s. V důsledku toho se začaly pomalu rozvíjet bezdrátové WiFi sítě. Vyšší rychlost přinesl v roce 2003 i standard 802.11g. Tento standard je zpětně kompatibilní s verzí 802.11b a v dnešní době je nejvíce používán. Srovnání viz příloha D.1.

Další posun v rychlosti standardu přinesl rok 2011, kdy se zvýšila až na 150 Mb/s (802.11n). V dnešní době je také znám standard 802.16 (také znám jako WiMax). Tato nová technologie je brána jako doplněk WiFi. Největší rozdíl je v dosahu. Na místo sta metrů by měl dosahovat až na řádově kilometrové vzdálenosti. WiMax také nabízí podporu zajištění kvality služeb (QoS) zejména proto, že používá licenční pásma pro menší rušení od ostatních technologií. Je tedy spíše určen pro poskytovatele internetu, kteří vlastní tato oprávnění. Stejně jako 802.11n není ani WiMax natolik rozsáhlý jako jejich předchůdci.

Základním stavebním kamenem sítě je přístupový bod (Access point nebo hotspot). Jeho primárním úkolem je vysílat bezdrátový signál, který počítač dokáže rozpoznat a naladit se na stejnou frekvenci. Pro rozsáhlejší pokrytí sítě je potřeba rozmístit více přístupových bodů. Pro připojení k síti musí být zařízení vybavena síťovým adaptérem. V domácnostech se nejčastěji vyskytují routery vybavené WiFi anténou, které jsou do páteřní sítě připojeny kabelem a po domě šíří WiFi signál bezdrátově.

PoWiFi

V roce 2015 inženýři z univerzity ve Washingtonu představili jednu z nejnovějších technologií využívající WiFi signál. Jedná se o tzv. The Power Over WiFi neboli PoWiFi[29]. Jak je již z názvu patrné, podařilo se pomocí WiFi signálu přenášet i energii potřebnou k napájení nízkoenergeticky náročných zařízení. Při testování nebyl zjištěn úbytek rychlosti přenosu sítě. Celá technologie je prozatím ve vývoji, ale již dnes inženýři tímto signálem napájeli jednoduché teplotní čidlo, fotoaparát s nízkým rozlišením fotografující ve stupni šedi či jednoduchý nositelný náramek sledující funkce lidského těla. Hlavním předpokladem většího rozšíření je zvýšení přenášené napájecí energie a také snížení energie potřebné k napájení jednotlivých zařízení. Mohlo by se však jednat o další vývojový stupeň WiFi. Vyřešilo by to i problém s napájením jednoduchých senzorů spadajících do *Internetu věcí*.

	Bluetooth	**ZigBEE**	**Z-Wave**	**WiFi**
Standard	802.15.1	802.15.4	N/A	802.11x
Zaměření	Nahrazení krátké kabeláže	Monitorování	Monitorování	WLAN
Energetická spotřeba	Střední	Nízká	Nízká	Vysoká
Rychlost	v4.2 24 Mb/s	až 250 kb/s	až 100 kb/s	až 54 Mb/s
Frekvence	2,4 GHz	obecně 2,4 GHz	868,42 MHz (EU)	2,4 GHz
Dosah	až 100 m	až 100 m	až 100 m	až 100 m

Tabulka 2.2: Srovnání uvedených technologií.

2.7 Protokoly

Internet věcí zahrnuje širokou škálu možných protokolů pro přenos dat. Tyto protokoly většinou nebyly primárně vyvíjeny pro *Internet věcí*, ale jsou odvozeny od protokolů telekomunikačních. Jejich hlavním znakem je přenos malého objemu dat (řádově desítek až stovek bitů) pro nižší energetické a paměťové nároky.

MQTT

Jedná se o komunikační protokol Message Queuing Telemetry Transport[6] vyvinutý společností IBM v roce 1999. Je určen zejména pro méně výkonná zařízení. Jeho hlavní výhody jsou jednoduchost a snadná implementace. Používá se např. v lékařské technice (komunikace s kardiostimulátory). Mnoho z nás se s ním může nepřímo setkat v mobilní aplikaci Facebook Messenger. V dnešní době patří mezi dva nejpoužívanější protokoly (s CoAP) v *Internetu věcí*.

Protokol používá TCP/IP[25] pro připojení k internetu. Přenos dat na bázi publish a subscribe, kde publisher odesílá data do tzv. brokeru (mezičlánek). Tento broker následně poskytuje data odběrateli (subscriber). Obě zařízení tedy mezi sebou komunikují nepřímo. Můžeme se setkat s označením one-to-many komunikace. Důležitým předpokladem použití protokolu je přenos dat v blocích, nelze jej tedy použít pro datový proud (streamování).

Broker je softwarová aplikace, která se stará o autorizaci a autentizaci odběratelů. Také se stará o zabezpečení poskytovaných dat pomocí kryptografických funkcí. Zajišťuje komunikaci mezi jednotlivými brokery, tím pádem mohou vznikat i složitější struktury zapojení jednotlivých komponent. Lze využít aplikaci pro ukládání zpráv, které nebyly doručeny. Maximální velikost jedné zprávy je 256 MB.

V MQTT brokeru se používají tzv. topics (témata) pro rozhodnutí, který klient (odběratel) získá jaká data. Tato témata mají hierarchickou strukturu (viz obrázek 2.15). Jednotlivé úrovně jsou popsány ASCII řetězci case-sensitive[26] v doporučeném kódování UTF-8, pro předejití komplikací s českou diakritikou. Úrovně témat jsou odděleny znakem „/“. Každé téma musí obsahovat alespoň jeden znak, přičemž i samotné lomítko či mezera je platné téma.

Obrázek 2.15: Hierarchická struktura topics MQTT[27].

Klient se může přihlásit k odebírání tématu podle přesného popisu nebo získá více témat najednou pomocí zástupných znaků „#“ a „+“. Znak plus slouží jako zástupce jedné úrovně (viz obrázek 2.16). Znak mřížka se používá pro popis všech následujících úrovní (viz obrázek 2.17). Nelze jej tedy použít uprostřed definice.

[25] Soustava síťových protokolů, alternativa k sedmivrstvému modelu (ISO/OSI). Model TCP/IP řadí své protokoly do 4 vrstev: aplikační (application layer), transportní (transport layer), mezisíťové (internet layer) a vrstvy přístupu k síti (network interface layer).

[26] Řetězce citlivé na velikost písmen. Tedy rozdíl mezi „CASE“ a „case“.

[27] Převzato z: http://www.hivemq.com/blog/mqtt-essentials-part-5-mqtt-topics-best-practices.

Obrázek 2.16: Použití zástupného znaku „+“[27].

Obrázek 2.17: Použití zástupného znaku „#“[27].

Existují vyhrazená témata začínající na symbol „$“ jako např. „$sys“ určená pro informace o stavu a běhu brokeru. Poskytované informace tohoto tématu se liší podle brokeru.

Komunikace mezi odběratelem a brokerem začíná požadavkem na připojení pomocí *Connect*. V této fázi dochází k autorizaci pomocí *Username* a *Password*. MQTT je textový protokol a je doporučeno používat zašifrování zpráv pomocí SSL/TLS. Po ověření může odběratel přijímat aktuální zprávy z jednotlivých témat.

Standard také definuje několik možných úrovní spolehlivého doručení zpráv tzv. Quality of Service (QoS) Level 0 – 2.

- Nultá – nejnižší úroveň známá jako „Fire and forget“. Během této úrovně se pošle zpráva jen jednou a následně se zapomene bez jakékoli záruky příchodu. Nejčastěji se používá u vysoce se opakujících zpráv nebo u zpráv, kde nedoručení není bráno jako kritická chyba.
- První – tato úroveň se snaží zaručit přijetí zprávy aspoň jedním odběratelem. Přijetí je potvrzováno pomocí tzv. acknowledgment message (ACK)[28].
- Druhá – nejvyšší úroveň zabezpečení přijetí zprávy. Publisher posílá zprávu o nastavení QoS level 2. Příjemce dekóduje zprávu a indikuje, že je připraven přijímat. Publisher posílá data a jakmile příjemce data dekóduje, posílá potvrzovací zprávu (ACK). Nejvyšší úroveň je vhodná např. pro zapnutí a vypnutí alarmu v domě.

XMPP

Extensible Messaging and Presence Protocol[8] (XMPP) je protokol vyvíjený open-source[29] komunitou Jabber určený pro zajištění instant messagingu[30]. Je založený na architektuře klient-server s využitím TCP spojení. Server čeká na připojení klienta na portu 5222.

Roku 1999 Jeremie Miller zakládá projekt Jabber určený pro instant messaging. Stejný rok se také Miller zavázal k Jabber IETF standardizaci. Po roce vývojáři představili open-source Jabber server (tzv. jabberd), několik open-source klientů, jazykových knihoven a bezdrátový protokol pro real-time XML streaming. V roce 2001 vzniká skupina The Jabber Software Foundation (JSF), protože bylo zapotřebí koordinovat rychle rostoucí počet Jabber open-source projektů. JSF také dohlíží na používání protokolů v rámci Jabber komunity, stará se o dokumentování a vývoj rozšíření již stávajících protokolů. O rok později se formuje XMPP Working Group, která přispívá k rozšíření stávajících Jabber protokolů a v důsledku toho se vytváří nový protokol pod názvem XMPP.

[28] Zpráva, která má potvrzovací charakter a informuje o přijetí dané informace.

[29] Počítačový software s otevřeným zdrojovým kódem. Při dodržení jistých podmínek umožňuje uživatelům zdrojový kód využívat legálně.

[30] Uživatelům mezi sebou poskytuje možnost zasílání zpráv, souborů, chatování v reálném čase.

V říjnu roku 2004 IETF[31] vydává RFC 3920 a RFC 3921, kde definuje XMPP jako standard pro instant messaging. V České republice se první Jabber server objevil 1. dubna 2001.

Klient je jednoznačně identifikovaný pomocí Jabber ID (JID). Tento JID se nejčastěji vyskytuje ve tvaru „user@domain/source“. Uvedení source vytváří možnost připojení z více míst na jeden účet. Nejčastěji to však není vyžadováno. Komunikace[27] mezi dvěma zařízeními (koncovými body) vytváří na obou stranách XML dokument. Nejprve se klient ohlásí na server.

Po odeslání žádosti klienta na server „jabber.cz“ klient čeká na odpověď. Po příchodu odpovědi ze serveru dojde k autentizaci uživatele. Tato autentizace může proběhnout několika způsoby a to zabezpečenou a nezabezpečenou cestou. Pokud se na serveru nachází údaje klienta (user name, password), klient je úspěšně přihlášen a může začít komunikovat.

Pro použití XMPP v rámci *Internetu věcí* má tento protokol několik předpokladů a výhod. Je vyvíjen a testován více jak 10 let. Za tuto dobu byla vytvořena značná infrastruktura. Existuje mnoho serverů po celém světě. Zejména instant messaging má velkou uživatelskou základnu. Od roku 2014 nesmí žádné veřejné servery běžet nezašifrovaně, což přispává k zlepšení zabezpečení. Díky dlouhodobému vývoji je software dostupný v mnoha programovacích jazycích.

AMQP

The Advanced Message Queuing Protocol[9] neboli AMQP je open-source standard navržen tak, aby pracoval jako middleware[32] ve zprostředkování zpráv mezi různými procesy, aplikacemi a i mezi systémy, které nemají mezi sebou vazby, ale potřebují mezi sebou komunikovat a předávat zprávy (viz obrázek 2.18). AMQP je binární síťový protokol a pracuje na aplikační vrstvě ISO/OSI[33] modelu jako např. XMPP.

Cílem AMQP bylo vytvořit způsob komunikace mezi širokou škálou různých aplikací a systémů s různou vnitřní strukturou a implementací. Do té doby neexistoval způsob, který by tuto komunikaci zajišťoval. Jedním ze způsobů bylo zavedení nové vrstvy pro převod zpráv mezi systémy zvané messaging bridge. Tato metoda vyžaduje použití „adaptérů“ pro příjem zpráv v různých systémech. AMQP oproti tomu nabízí jasně definovaná pravidla a pokyny, které vytvoří základ pro příjem a odesílání všech typů zpráv. Také zajišťuje spolehlivost a zabezpečení přenosu zpráv pomocí Transport Layer Security[34] (TLS) a Simple Authentication and Security Layer[35] (SASL).

AMQP vznikl roku 2003 Johnem O'Harou z firmy JP Morgan Chase[36] v Londýně. V roce 2005 se přidaly další firmy jakou jsou Cisco, Iona Technologies, iMatix a Red Hat. Pracovní skupina se postupně rozrostla do dvaceti tří firem. V roce 2011 se původní AMQP working group stala organizací OASIS.

Model AMQP definuje např. příjem zpráv, směrování a vložení do front. Obě strany komunikace se musí dohodnout, jakou aplikaci budou používat, jelikož existuje mnoho implementací využívající AMQP protokolu. Obě strany mohou být příjemci i odesilateli zpráv.

[31] Organizace, která vyvíjí a podporuje internetové standardy a úzce spolupracuje s konsorciem W3C a organizacemi ISO/IEC.

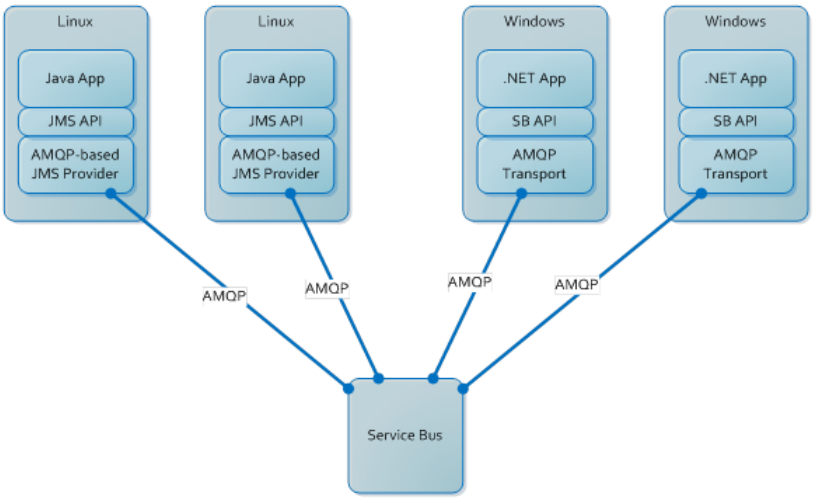
[32] Integrační nástroj (software), který zajišťuje přenos dat mezi různými komponenty technické části informačního systému.

[33] Rozděluje vzájemnou komunikaci mezi počítači do sedmi souvisejících vrstev.

[34] Kryptografický protokol poskytující možnost zabezpečené komunikace na internetu i prostřednictvím autentizace.

[35] Metoda ověřování autentizace v protokolech klient-server.

[36] Jedna z nejstarších firem na světě poskytující finanční služby.



Obrázek 2.18: Komunikace mezi různými platformami s využitím AMQP[37].

AMGP definuje formát posílaných zpráv. Část zprávy, která je vytvořena odesilatelem a také její přenos je pevně daný. Odesílatel může zabezpečit zprávu podpisem či šifrováním. Zpráva může být opatřena poznámkami o přenosu. Hlavička obsahuje standardní informace související s přenosem zprávy jako jsou např. TTL (Time to live) a priorita. Samotná zpráva se následně skládá ještě z volitelného seznamu standardních vlastností jako jsou Message ID, User ID, Creation time, Reply to, Subject, Correlation ID.

Pro příklad AMQP využívá NASA pro Nebula Cloud Computing, JP Morgan ke zpracování zpráv a Google pro komplexní zpracování událostí.

CoAP

Constrained Application Protocol[5] neboli CoAP je síťově orientovaný (network-oriented) protokol definován IETF pracující na aplikační vrstvě ISO/OSI primárně určený pro velmi jednoduchá nízkoenergetická zařízení (např. senzory). Navržen pro tzv. machine-to-machine (M2M)[38] použití. Je realizována asynchronní výměna zpráv mezi zařízeními. Využívá pro komunikaci UDP[39] protokol. Není tedy zaručen spolehlivý přenos, protože samotný UDP nezaručuje doručení všech datagramů, zda dorazí ve správném pořadí nebo zda nebudou doručeny vícekrát.

Je používán model dotaz/odpověď (request/response). Oproti MQTT je primárně CoAP určen pro komunikaci na bázi modelu one-to-one (jedno zařízení poskytuje data druhému zařízení bez možnosti dalších zařízení). Je možnost jej však využít i pro komunikaci one-to-many a many-to-many.

Protokol je jednoduše přeložitelný do HTTP[40]. Lze jednoduše využit DTLS (Datagram Transport Layer Security) protokol pro zajištění zabezpečení. Na rozdíl od bezpečnostních protokolů běžících na síťové vrstvě ISO/OSI, DTLS pracuje na aplikační vrstvě. Je zame-

[37] Převzato z: https://azure.microsoft.com/en-gb/documentation/articles/service-bus-java-amqp-overview/

[38] Bezdrátová i drátová komunikace mezi zařízeními využívající stejný hardware bez zásahu člověka.

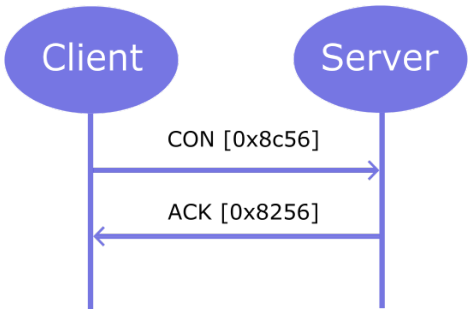
[39] Nespojovaný (nepotvrzovaný) protokol transportní vrstvy pro přenos zpráv mezi uživatelskými aplikacemi.

[40] Protokol pro komunikaci prohlížeče s WWW serverem.

zeno odposlechům, falšování nebo padělání jednotlivých posílaných zpráv. Hlavička zprávy, metody i stavové kódy jsou kódovány binárně. Snižuje to režii protokolu.[18]

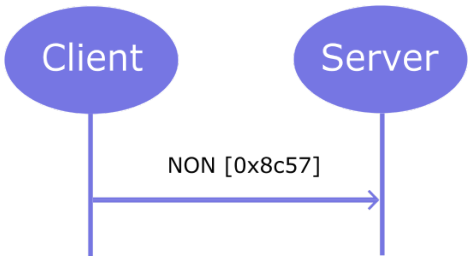
Protokol nabízí ve srovnání s MQTT QoS tzv. Reliability. V rámci ní rozlišujeme dva typy zpráv:

- Confirmable zpráva (CON) je potvrzována ACK zprávou od zamýšleného příjemce se stejným Message ID jako měla původní zpráva (viz obrázek 2.19). Využívá se tzv. default time out (potřebná doba k doručení). Pokud příjemce nestihne zpracovat zprávu, je místo ACK poslána zpráva RST (Reset).



Obrázek 2.19: Zpráva CoAP typu Confirmable[41].

- Non-confirmable zpráva (NON) je jako MQTT QoS nulté úrovně „Fire and forget“, kde není vyžadováno potvrzení pomocí ACK (viz obrázek 2.20). Odesílaná zpráva však také obsahuje Message ID, pro identifikaci a možnost např. dohledání cesty přenosu zprávy.



Obrázek 2.20: Zpráva CoAP typu Non-confirmable[41].

CoAP umožňuje více způsobů implementace modelu request/response:

- První z nich tzv. Piggy-backed, kdy klient pošle request ve formě CON či NON zprávy a ihned očekává potvrzení ve formě ACK. Při úspěšném přijetí ACK obsahuje příslušná data, v opačném případě obsahuje chybová hlášení (viz příloha B.1).

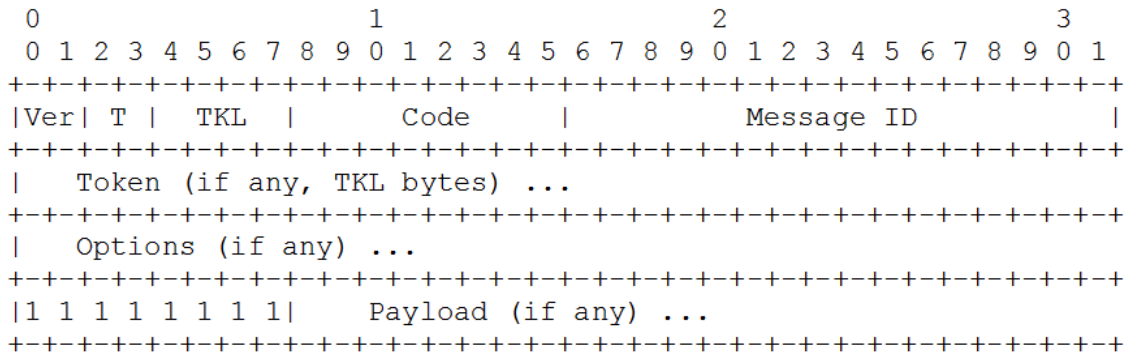
- Druhý způsob je tzv. Separate response. Pokud server obdrží zprávu CON, ale není schopen ihned odpovědět, čeká. Pokud klient zašle CON zprávu znovu, zašle zpět prázdný ACK. Až je server schopen odpovědět na dotaz, zašle klientovi CON zprávu. Klient reaguje odpovědí ACK (viz příloha B.2).

[41] Převzato z: http://www.cse.wustl.edu/~jain/cse574-14/ftp/coap/.

- Třetí způsob vyžaduje odeslání klientské NON zprávy, čímž klient oznamuje serveru, že není nutné potvrzovat příjem. Data jsou následně od serveru poslána také v NON typu zprávy (viz příloha B.3).

Formát binární CoAP zprávy je pevně určen. Zpráva musí obsahovat v přesném pořadí tyto položky:

- Version – verze protokolu v dnešní době nastavena na 1.
- Type – typ zprávy (CON, NON, ACK, RST).
- Token Length – specifikace délky tokenu od 0-8 bytů.
- Code – kód odpovědi jako úspěšné doručení, chyba klienta nebo chyba serveru. Analogie s HTTP.
- Message ID – identifikace jednotlivých zpráv. Nejčastější implementace pomocí postupného zvyšování, což však není vhodné z hlediska bezpečnosti.
- Token – používá se pro rozlišení paralelních požadavků mezi klientem a serverem.
- Options – může obsahovat jeden nebo více příznaků včetně nastavení, která jsou k dispozici v HTTP hlavičce.
- Payload – tělo zprávy.



Obrázek 2.21: Formát zprávy (převzato z [18], více tabulka C.1)

Jak již bylo zmíněno výše, k zabezpečení CoAP protokolu se používa Datagram Transport Layer Security. Tento protokol řeší problém jiného pořadí příchodu zpráv a také problém ztráty paketu pomocí několika principů:

- Opakovaným přenosem paketů.
- Přiřazení pořadového čísla k paketům.
- Vyžadování odpovědi.

CoAP je stále považován za vyvíjející se protokol na rozdíl od MQTT. Může to způsobit problémy s použití v různých prostředích. Je však velmi pravděpodobné, že CoAP v blízké budoucnosti dosáhne stejné úrovně jako MQTT.

2.8 Skupiny výrobců pro standardy Internetu věcí

Jelikož prozatím neexistuje žádný obecný standard *Internetu věcí*, začaly se formovat aliance firem, které na trhu vystupují jako větší celky a snaží se prosadit svá technologická řešení. Jedna z takových společenství je tzv. AllSeen Alliance. Jedná se o neziskovou organizaci založenou v roce 2013 s hlavním cílem zjednodušeného vývoje a následného schvalování nových výrobků, systémů a služeb spadajících do *Internetu věcí*. Hlavní členové jsou Cisco, LG, Microsoft, Qualcomm, Sharp, Sony, TP Link, Panasonic a Electrolux. Spolupracují na vývoji open-source software projektu ALLJoyn, který podporuje vývoj *Internetu věcí* a celý by jej měl zastřešovat. Jde o systém, který umožní komunikaci mezi jednotlivými zařízeními, stará se o zabezpečení a celkovou interoperabilitu. Poskytuje univerzální rámcový software a základní sadu systémových služeb, který umožní spolupráci mezi produkty a aplikacemi od různých výrobců bez ohledu na použitou platformu či operační systém. Projekt podporuje protokoly MQTT a XMPP.

Další skupina se nazývá Open Interconnect Consortium (OIC). Její hlavní náplní je vyvíjet standardy a certifikáty pro zařízení v rámci *Internetu věcí* podporující protokol CoAP. Byla vytvořena v červenci roku 2014 oznámením spolupráce firem Broadcom, Intel a Samsung (Broadcom později vystoupilo). Postupně se přidávaly další firmy jako Cisco, Acer, HP, DELL, Atmel, Lenovo či MediaTek. Podobně jako AllSeen Alliance, také Open Interconnect Consortium nabízí vlastní open-source framework[42] nazvaný IoTivity.

Obě zmíněné aliance vedou na trhu *Internetu věcí* spor a každá strana se snaží prosadit vlastní vizi a vyvíjený software. Jejich strategie se však liší. Dne 19. února 2016 OIC změnila svůj název na Open Connectivity Foundation (OCF). Toto nové společenství by v budoucnu mělo více spolupracovat s AllSeen Alliance. Nedošlo ke spojení organizací, ale zařízení pracující se standardy AllSeen Alliance (zejména vyvýjené firmou Qualcomm) by měly podporovat i standardy OCF. Jedná se o důležitý milník ve vývoji *Internetu věcí*. K OCF se také připojil Microsoft a slíbil spolupráci a interoperabilitu s Windows 10. Dávní rivalové ve vývoji mikroprocesorů Intel a Qualcomm také potvrdili spolupráci.

„We believe that fragmentation is the enemy of IoT. That's why we are working with these likeminded companies to invest in the future of IoT.“ Tato slova pronesl Michael Wallace, generální manažer části rozvíjejících se oblastí společnosti Qualcomm. S tímto výrokem souhlasil i Terry Myerson, výkonný viceprezident Windows and devices group ve společnosti Microsoft a dále pak dodal, že všechna zařízení s Windows 10 budou podporovat standardy OCF. Nyní má skupina OCF více jak 140 členských firem.

Další takovou neziskovou organizací je Industrial Internet Consortium (IIC). Zakládající členové 27. března 2014 byly firmy AT&T, Intel, Cisco, IBM a General Electric. Dne 2. února 2016 měla 237 členů. Její hlavní cíl je také snaha propojit jednotlivá zařízení a urychlení rozvoje a zavedení *Internetu věcí*. Zaměřují se však více na průmyslové využití a zejména strojové učení, zpracování velkého objemu dat a machine-to-machine komunikaci.

IIC organizace existovala paralelně s bývalou OIC. Došlo však ke vzájemné dohodě. Mělo by se jednat o otevřenou spolupráci a zejména sdílení use-cases[43] a požadavků na architekturu zařízení. Organizace IIC bude také testovat projekt IoTivity na svých přístrojích pro zajištění lepší kompatibility. Zejména tedy došlo ke spojení open-source software od OIC využitím use-cases a definovaných požadavků od IIC. Organizace IIC na počátku roku 2016

[42] Struktura, která slouží jako podpora při programování, vývoji a organizaci jiných softwarových projektů.
[43] Popis chování systému z hlediska uživatele.

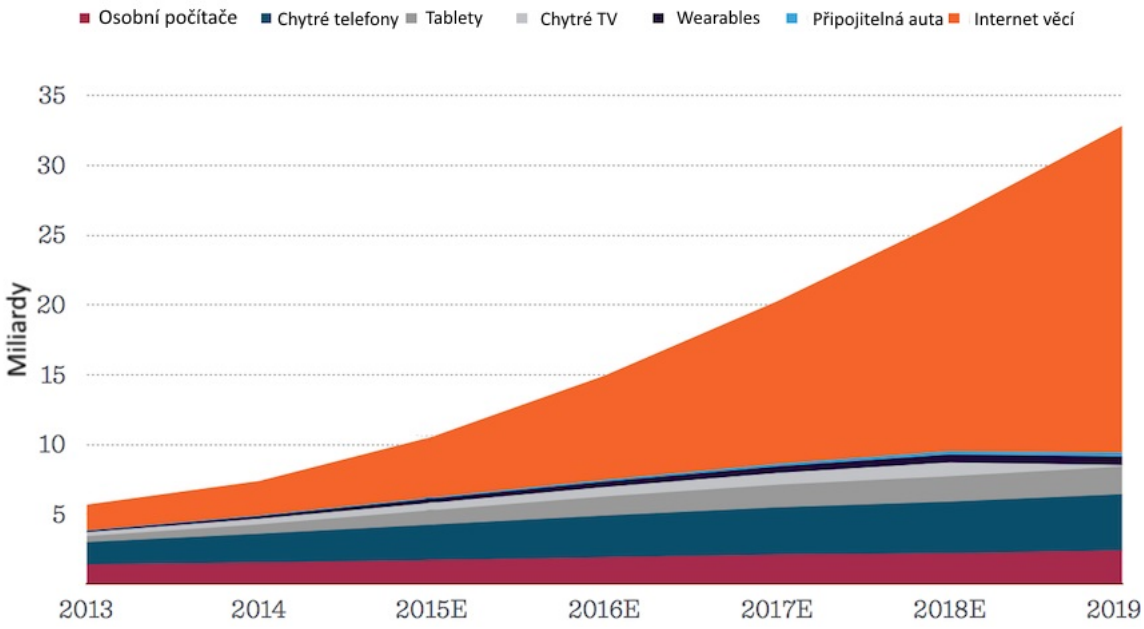
představila vlastní vizi *Internetu věcí* nazvanou Time Sensitive Networking. Jde o testovací platformu pro vývoj průmyslových aplikací a zařízení. Hlavní prvky jsou komunikace v reálném čase, bezpečnost a spojení s ostatními standardy jiných výrobců.

2.9 Budoucnost

„V příštím století bude planeta Země obalena elektronickou vrstvou. Bude používat internet jako prostředek pro přenášení pocitů.“ - Neil Gross 1999 Podle společnosti Texas Instruments bude v roce 2020 připojeno k internetu 50 miliard zařízení.[23] O něco mírnější předpověď zveřejnila společnost Gartner. Jejich analytici odhadují v roce 2019 okolo 35 miliard zařízení spadající do kategorie *Internet věcí* (viz obrázek 2.22). Je třeba zmínit, že předpovědi se často v počtu zařízení liší. Analytici společnosti IDC vydali předpověď na rok 2015, kde zdůrazňují zvýšení používání cloud úložišť, jelikož se uživatelé (např. firmy) oprostí od nutné výstavby vlastní datové infrastruktury.

Dále pak byla předpovězena zvýšená rizika používání *Internetu věcí*. Více jak 90% firem mělo zaznamenat bezpečnostní narušení prostřednictvím *Internetu věcí*. Je značná snaha upozornit na stálá rizika spojená s touto tématikou (viz 2.4 Zabezpečení).

Předpověď na rok 2016 pomocí společnosti Fortinet naznačuje opět zvýšení množství útoků na zařízení v rámci *Internetu věcí*. Zejména půjde o útoky typu „land and expand“. Podle názvu je zřejmé, že jde o napadení jednoho zařízení v síti, ze kterého se škodlivý malware[44] bude šířit do dalších zařízení. S rostoucím počtem *Internetu věcí* se zvyšuje i riziko napadení. Společnost také upozorňuje na možné proniknutí do zařízení skrze cloud aplikace.[16]



Obrázek 2.22: Předpokládaná velikost trhu se zařízeními spadající do kategorie *Internet věcí*[46].

[44] Všeobecné označení pro skupinu škodlivých počítačových programů určených ke vniknutí do nebo poškození počítačového systému.

[46] Převzato z: http://www.corelynx.com/blog/hottest-new-thing-it-iot.

Kapitola 3

Zařízení spadající do Internetu věcí

Tato kapitola si klade za cíl popsat vývoj zařízení spadajícího do kategorie *Internet věcí*, a to zejména návrh, implementaci a testování zařízení. Jedná se o bezdrátová zařízení pro detekci příchodu pošty do poštovní schránky a WiFi teplotní čidlo. Zařízení s využitím protokolu CoAP odesílají data do řídící jednotky. Řídící jednotka příchozí data zpracovává a poskytuje uživateli zpětnou vazbu v podobě webového grafického rozhraní či e-mailového upozornění. K řídící jednotce je možné připojit pomocí bluetooth chytrý mobilní telefon s operačním systémem Android[1] a skrze mobilní aplikaci lze zmiňované upozornění vypnout/zapnout.

3.1 Návrh zařízení

Zařízení, které by spadalo do kategorie *Internet věcí*, musí splňovat několik požadavků. Jedná se zejména o kompaktnost, nízkou pořizovací cenu a nízkou spotřebu energie. Jak již bylo zmíněno v předchozích kapitolách, musí také disponovat komunikačními schopnostmi pro připojení k internetu a to nejlépe bezdrátově. Je třeba také zajistit vysokou úroveň zabezpečení.

Na trhu se nachází spousta různých vývojových desek, modulů, senzorů a elektronických součástek, ze kterých lze sestavit výsledné zařízení. Výše popsané požadavky byly hlavním aspektem při výběru jednotlivých komponent. Nebyly však jediné. Bylo třeba také zohlednit podporu jednotlivých komponent a kvalitu dokumentace.

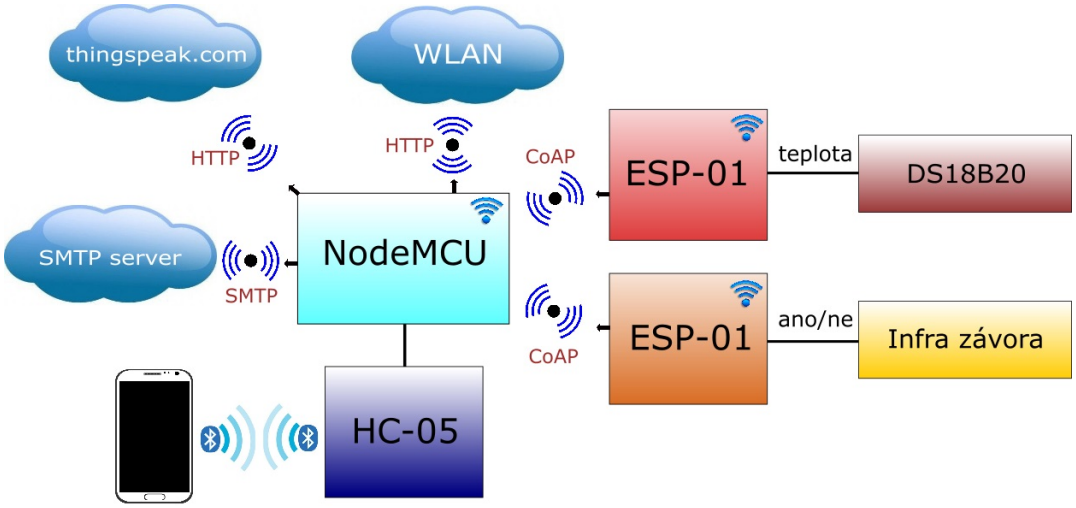
Při výběru řídící jednotky se zprvu nabízel mini počítač Raspberry pi 2[2], který disponuje velkou výpočetní silou (čtyř jádrový procesor s grafickým čipem, 1 GB SDRAM) a mezi uživateli je oblíbený. Nepodporuje však potřebné bezdrátové WiFi připojení (je třeba dokoupit WiFi dongle do USB). Cena za Model B okolo 1000 Kč byla zbytečně vysoká.

Mezi uživateli je také velmi oblíbená řada vývojových desek Arduino[3]. Existuje několik druhů, které se liší velikostí a výbavou. K deskám je také vytvořeno vývojové prostředí Arduino IDE, které zjednodušuje vývoj software.

Z hlediska ceny, výbavy, dostupnosti a velikosti se nejlépe jevila deska Arduino Nano. Na trhu se objevují i klony této desky za přijatelnou cenu okolo 250 Kč. Samotná deska však také nepodporuje WiFi připojení a je třeba jej řešit dodatečnými WiFi moduly. Mnoho uživatelů tuto zkutečnost řeší WiFi modulem z řady ESP8266 (nejčastěji ESP-01). Jelikož tento modul může pracovat samostatně (nepotřebuje další vývojovou desku), stojí zhruba

[1] Mobilní operační systém založený na jádře Linux.
[2] Jednodeskový počítač s deskou plošných spojů o velikosti zhruba platební karty.
[3] Jednodeskové počítače založené na mikrokontrolerech ATmega od firmy Atmel.

130 Kč, podporuje sériovou komunikaci a o rozměrech 25 x 14 mm nejvíce vyhovuje potřebám zařízení spadajícího do kategorie *Internet věcí*.



Obrázek 3.1: Schéma zapojení vybrané elektroniky a senzorů.

3.2 Popis jednotlivých částí zařízení

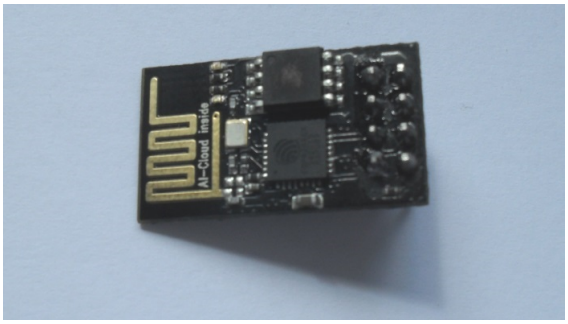
V této části se nachází popis všech jednotlivých komponent, které byly využity v praktické části bakalářské práce.

ESP8266

Nejpoužívanější WiFi modul z řady ESP8266[32] je verze ESP-01 (viz obrázek 3.2). Jedná se o výrobek pocházející z Číny a ještě do nedávna byla jeho hlavní nevýhoda nízká podpora ze strany výrobce. Zejména čínský datasheet[4] snižoval možnost využití v ostatních částech světa. Nejen přeložení datasheetu do angličtiny má však důsledky v masovém rozšíření těchto modulů. Přispělo k tomu i vytvoření oficiálního internetového fóra pro dotazy uživatelů a vytvoření softwarových knihoven.

Napájecí napětí u ESP-01 je 3,3 V. Modul může krátkodobě odebírat proud až 300 mA a je třeba s těmito špičkami počítat. Průměrná spotřeba je však udávaná okolo 80 mA. Je osazen 32 bitovým mikroprocesorem Tensilica L106. Modul disponuje 8 piny (VCC, GND, RST, RX, TX, GPIO0, GPIO2 a CH_PD) s roztečí 2,54 mm. Na modulu se nachází vestavěná plošná PCB anténa pro bezdrátové připojení WiFi, které podporuje standardy 802.11 b/g/n. Modul disponuje třemi režimu tzv. „Active mode“, „Sleep mode“ a „Deep sleep mode“. Od výrobce je v modulu firmware určený pro ovládání pomocí AT příkazů. Tento firmware byl však na začátku sestavování zařízení přehrán (viz 3.3 Implementace a testování zařízení).

[4] Dokument uvádějící technické charakteristiky výrobku, stroje či součástky.



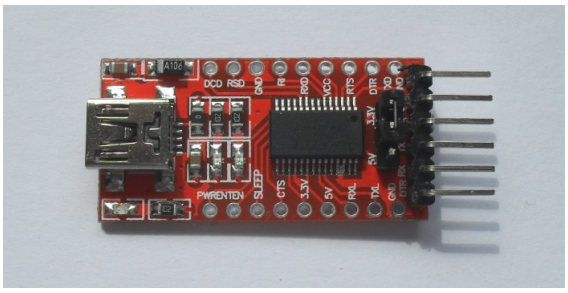
Obrázek 3.2: Modul ESP-01.

USB/UART FTDI převodník FT232RL

Zmíněné ESP-01 disponuje piny RX a TX pro sériovou komunikaci. Pro komunikaci s PC a následným nahráním software je třeba ESP-01 připojit k převodníku FT232RL[33] (viz obrázek 3.3) a ten přes USB mini připojit k PC. Tento převodník se hojně využívá k programování (i flashování[5]) různých modulů včetně řady Arduino. Převodník FT232RL disponuje možností manuálního nastavení rozhraní 5 V a 3,3 V pomocí jumperu.

Samotná komunikace prostřednictvím UART (Universal Asynchronous Receiver Trensmitter) neboli Univerzální asynchronní přijímač/vysílač využívá sériový vysílač (pin TX) a sériový přijímač (pin RX). Vysílač pracuje s datovým registrem TxDR a přijímač s registrem RxDR. Při odesílaní dat se data umístí do registru TxDR, kde se podle nastavení doplní datový rámec o start bit (pro synchronizaci a stejnou fázi hodinového signálu), paritní bit (pro kontrolu přenosu) a stop bit (pro detekci ukončení přenosu). Všechny bity se následně umístí do posuvného registru, ze kterého jsou data odeslána.

Příjem dat má opačný průběh. Pokud registr RxDR obdrží start bit, dojde k zahájení příjmu dat. Data se ukládají do posuvného registru. Po ukončení přenosu se data z posuvného registru přesunou do registru RxDR a následně jsou poskytnuta ke zpracování.



Obrázek 3.3: FT232RL převodník.

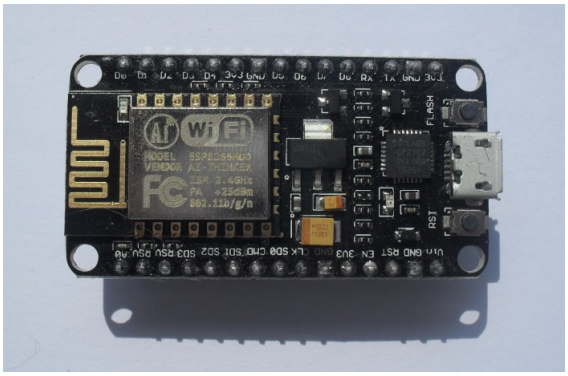
NodeMCU DEVKIT 1.0

Vývojová deska NodeMCU[34] (viz obrázek 3.4) eliminuje nutnost použití převodníku k WiFi modulu řady ESP, jelikož je již převodník osazen na desce. Jedná se o open-source hardware platformu primárně určenou pro vývoj zařízení spadajících do kategorie *Internet věcí*. Integruje GPIO, PWM, IIC, 1-Wire a ADC na jedné desce. První kusy byly vyrobeny v pro-

[5]Proces přehrání firmwaru v elektronickém zařízení.

sinci 2014. Deska je založena na modulu ESP-12 a je poháněná procesorem Tensilica Xtensa LX106. Modul ESP-12 disponuje vestavěnou plošnou PCB anténou. Uváděná velikost paměti je 20 kB a úložný prostor 4 MB. Pro napájení a připojení k PC slouží micro USB. Na desce se nachází i dvě tlačítka (Button a Flash), které lze při vývoji využít. Udávané rozměry výrobcem jsou 49 x 25 x 13 mm.

Desku lze po připojení k PC programovat z vývojového prostředí Arduino IDE stejně jako desky Arduino. Tato kompatibilita je výhodou zejména pro vývojáře, kteří jsou již zvyklí na práci s deskami Arduino. Výrobce NodeMCU však pro desky vytvořil vlastní firmware, který slouží k programování jednoduchých aplikací prostřednictvím jazyka Lua (viz 3.3 Implementace a testování zařízení).

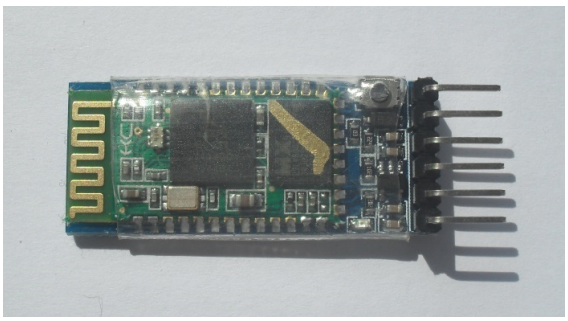


Obrázek 3.4: NodeMCU DEVKIT 1.0.

Bluetooth modul HC-05

Levných bluetooth modulů na českém trhu moc nenajdeme. Modul HC-05[35] (viz obrázek 3.5) je svou výbavou dostačující a pro potřeby praktické části práce vhodný. Podporuje sériové rozhraní a má integrovanou anténu. Napájecí napětí je 3,3 V. Disponuje signalizační diodou, které podle frekvence blikání určuje, v jakém stavu se modul nachází. Nevýhodou tohoto modulu je podpora starší verze bluetooth a to *2.0+EDR*. Modul může pracovat v režimu master i slave. Udávaný dosah je až 10 m a rozměry jsou 32 x 16 x 3 mm.

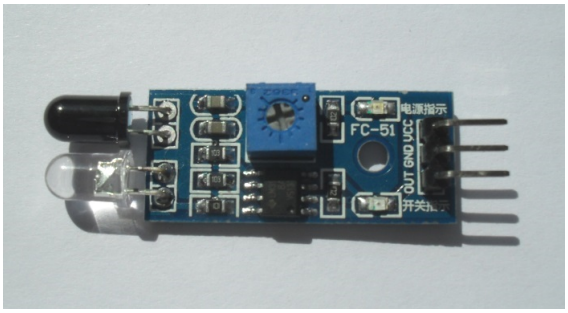
Modul má dva režimy činnosti a to tzv. „Data mode“ a „Command mode“. První zmíněný slouží pro přenos dat a při zakoupení se modul také v tomto režimu nachází. Command mode slouží pro nastavení modulu pomocí AT příkazů. Od výrobce je nastavena přenosová rychlost 9600 Bd, datový rámec o velikosti 9 bitů (8 bitů data a 1 stop bit). Jméno zařízení pro párování je „HC-05“ a heslo „1234“. Všechny tyto hodnoty lze v Command mode změnit.



Obrázek 3.5: Bluetooth modul HC-05.

Modul Infra závora

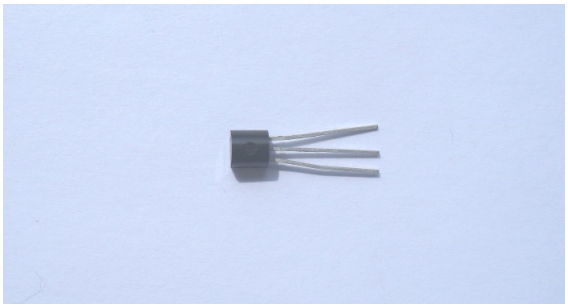
Tento modul Infra závora (viz obrázek 3.6) je osazen dvěma diodami. Jedna infra LED dioda vysílá paprsek a pokud se do určité vzdálenosti paprsek odrazí a přijme jej druhá LED, je detekován předmět. Modul je napájen 3,3 V. Dosah detekce předmětu je až 40 cm v úhlu přibližně 35°. Modul je osazen trimrem, pomocí kterého lze nastavit citlivost detekce. Pokud se nenachází před modulem žádný předmět, je výstup ve vysoké úrovni (H). Pokud je před modulem předmět do nastavené vzdálenosti, výstup je v nízké úrovni (L) a zároveň se rozsvítí indikační zelená LED dioda. Modul také disponuje LED diodou, která indikuje napájení. Rozměry modulu jsou 32 x 14 x 10 mm. Nevýhodou tohoto modulu je, že je vyráběn čínským výrobcem a neexistuje k němu žádná dokumentace. Všechny výše popsané informace jsou poskytovány prostředníkem, který realizuje prodej těchto modulů v ČR.



Obrázek 3.6: Modul Infra závora.

Teplotní čidlo DS18B20

Teplotní čidlo DS18B20[36] (viz obrázek 3.7) od firmy DALLAS je jedno z nejoblíbenějších a nejpoužívanějších teplotních čidel na českém trhu. Připojuje se přes 1-Wire[6] sběrnici. Každé čidlo má svou unikátní 64-bitovou sériovou adresu uloženou přímo v čidle. Rozsah měření teploty je od −55 °C do 125 °C, což v našem klimatickém pásmu dostačuje. Udávaná přesnost měření je ±0, 5 °C. Rozsah napájení je od 3 až do 5,5 V. Čidlo má tři vývody a to GND, DQ a VCC. Cena čidla se pohybuje okolo 35 Kč a udávané rozměry jsou 18 x 4 x 3 mm.



Obrázek 3.7: Teplotní čidlo DS18B20.

[6]Sběrnice vyznačující se nízkou datovou rychlostí, signalizací i napájením, která využívá ke komunikaci jen jeden vodič a připojení na zem.

3.3 Implementace a testování zařízení

V rámci implementace a testování bylo zapotřebí splnění dílčích kroků k vytvoření navržené soustavy zařízení.

Připojení zařízení k PC

Nejdříve bylo nutné připojit dílčí programovatelné moduly (NodeMCU a ESP-01) k PC. K propojování jednotlivých modulů bylo použito nepájivé pole. Pro připojení ESP-01 modulu k počítači byl použit USB/UART FTDI převodník. Zapojení modulů viz tabulka 3.1. Převodník FT232RL je od výrobce nastaven jumprem na 5 V. Před připojením k PC je třeba jumper přenastavit na 3,3 V nebo by mohlo dojít k nevratnému poškození modulu ESP-01.

ESP-01	**USB/UART**
VCC	VCC
GND	GND
RX	TX
TX	RX
CH_PD	VCC

Tabulka 3.1: Zapojení ESP-01 a USB/UART převodníku.

Při prvním připojení se rozezná připojené zařízení, stáhnou se a nainstalují potřebné ovladače převodníku a modul se připojí na portu COMx. Stejný postup se aplikuje při připojení desky NodeMCU DEVKIT 1.0 pomocí micro USB. Při správném zapojení se na modulech rozsvítí LED dioda indikující napájení.

Firmware a vývojové prostředí

Deska NodeMCU i modul ESP-01 od výrobce obsahují firmware. Tento firmware se však často liší verzí. Některé firmware mohou být přizpůsobené pro programování pomocí vývojového studia Arduino IDE. Jiné mohou obsahovat firmware pro sériovou komunikaci pomocí AT příkazů. Pro zajištění bezproblémové komunikace se doporučuje firmware přehrát. Výrobce desky NodeMCU vytvořil i několik verzí firmware pod stejnojmenným názvem.

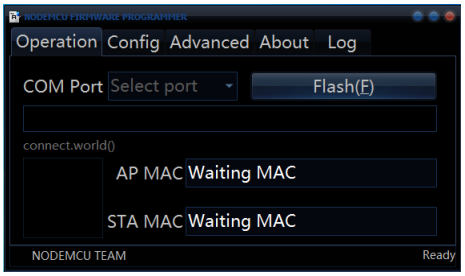
Tento firmware je přizpůsobený pro programování jednoduchého software pomocí jazyka Lua[31]. Jedná se o skriptovací jazyk nejvíce podobný jazykům Python, Perl, a Ruby. Jeho hlavním znakem je jednoduchost a rychlost díky automatické kompilaci do „byte code“[7]. Podporuje jen určité atomární datové struktury (boolovské hodnoty, čísla a řetězce). Složitější datové struktury mohou být reprezentovány pomocí tabulky. Výhodou jazyku Lua je možnost používat garbage collector[8].

Jazyk byl vytvořen roku 1993 na Papežské univerzitě v Rio de Janeiro. S jazykem Lua se můžeme často setkat v počítačových hrách, ve kterých si hráči mohou do určité míry přizpůsobit rozhraní právě pomocí jazyka Lua. Výrobce desky NodeMCU pro ukázku jazyka vytvořil několik vzorových skriptů, díky kterým si lze jazyk Lua rychle osvojit.

Pro přehrání firmware v desce NodeMCU a modulu ESP-01 byl použit program „ESP8266-Flasher“ (viz obrázek 3.8). Během práce byla použita verze firmware *0.9.6*.

[7] Instrukční sady navrženy pro realizaci snadno přenositelných aplikací a jejich efektivní běh na cílové platformě.

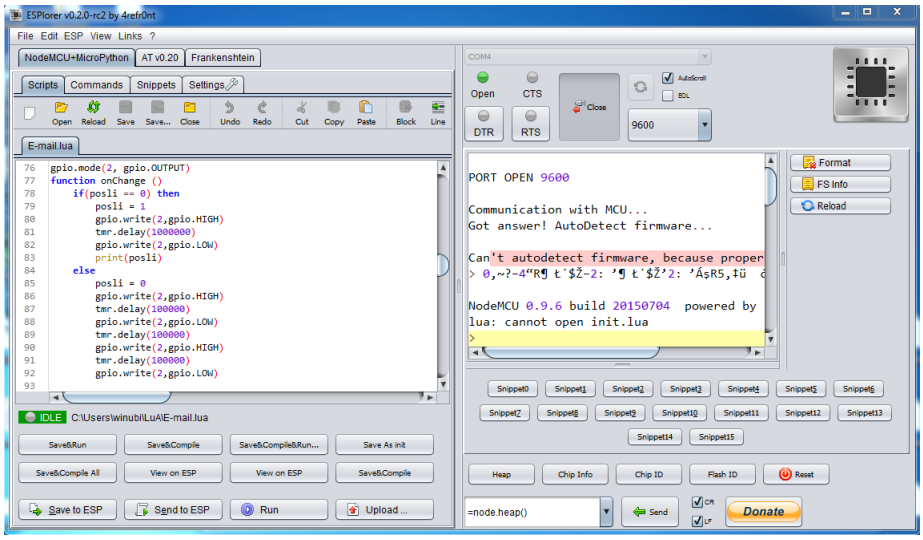
[8] Způsob automatické správy paměti.



Obrázek 3.8: Program ESP8266Flasher pro přehrání firmware.

Při snaze přehrát firmware v modulu ESP-01 je nutné připojit pin GPIO0 na GND. Po skončení přehrávání je nutné spoj odpojit. Jakmile byl úspěšně nahrán nový firmware, je možné začít programovat.

Jelikož jsou zařízení k PC připojena pomocí sériové komunikace, lze použít pro posílání příkazů jakýkoli terminál (např. PuTTY). Přímo pro práci s deskou NodeMCU a moduly řady ESP je však vytvořen program „ESPLorer“ (viz obrázek 3.9).



Obrázek 3.9: Program ESPlorer pro programování modulu ESP-01 a desky NodeMCU.

Program nabízí široké možnosti nastavení komunikace. Nejčastěji se však nastavuje přenosová rychlost a port COMx, pokud je najednou připojeno více zařízení. V levé polovině rozhraní uživatel vytvoří soubor s příponou *.lua* a následně může začít psát kód. Pro nahrání kódu do modulu či desky je třeba zvolit možnost „Save to ESP“. Pokud se však soubor nejmenuje „init.lua“, po vypnutí napájení a opětovném zapnutí modul přijde o nahraný software.

Pravá část programu je věnována zobrazení průběhu připojení modulu, nahrávání software do modulu a také zobrazuje běh nahraného programu. Program umožňuje při nečekaném chování zařízení použít Software Reset. Lze vytvořit vlastní uživatelské zkratky. Po stisku tlačítka program umožní poslat do modulu námi definovanou posloupnost příkazů jako např. připojení k WiFi, tisk přidělené IP adresy a mnoho dalšího, což zjednoduší vývoj.

CoAP klient v modulech ESP-01

Z návrhu zařízení je patrné, že moduly ESP-01 posílají naměřená data prostřednictvím protokolu CoAP. Jde o komunikaci klient-server, kdy moduly ESP-01 pracují v režimu klient a deska NodeMCU v režimu server. Moduly ESP-01 získávají data prostřednictvím senzorů a tato data poskytují serveru na zpracování. Jelikož jsou moduly ESP-01 napájeny z baterií, byla snaha snížit logiku a náročnost kódu na minimum ve prospěch nižší spotřeby energie. V praktické části práce byly využity dva ESP-01 moduly. Jeden pro detekci příchozí pošty v poštovní schránce a druhý pro měření venkovní teploty.

ESP-01 určené pro detekci příchozí pošty v poštovní schránce využívá modul Infra závory a vše je napájené třemi AAA bateriemi, které jsou regulovány na napětí 3,3 V. Hlavní logikou tohoto sestavení je cyklus, který podle zvoleného intervalu (při testování zvolen interval 15 min) kontroluje logickou úroveň pinu, na kterém je připojen modul Infra závora. Pokud je detekován předmět, modul se přihlásí do lokální sítě a prostřednictvím CoAP protokolu a zprávy POST pošle na server hodnotu „1“. V opačném případě je hodnota „0“. Pro CoAP komunikaci je zvolen standardní port 5683.

Druhý modul ESP-01 měří venkovní teplotu pomocí senzoru DS18B20 a je taktéž napájen třemi bateriemi AAA regulovány na napětí 3,3 V. Logika je podobná jako u předchozího sestavení. Ve zvoleném intervalu (při testování interval 10 min) se čte naměřená teplota ze senzoru a tato teplota je následně prostřednictvím CoAP protokolu posílána na server. Konkrétně se využívá k přenosu dat ze senzoru DS18B20 1-Wire sběrnice a senzor je připojen na GPIO0 pin. Při testování měření teploty bylo zjištěno, že senzor DS18B20 potřebuje určitý čas na zpracování požadavku. Pokud mezi dvěma požadavky byl interval méně než 0,1 s, senzor nestihl zpracovat požadavky a vracel chybové hlášení v podobě hodnoty „85“.

Řídící jednotka NodeMCU

Hlavním a řídícím prvkem celého sestavení je deska NodeMCU DEVKIT 1.0. Tato deska má několik funkcí, které vykonává. K desce je připojen modul HC-05 pro bezdrátovou komunikaci pomocí bluetooth. Dále je připojena LED dioda, která má stavovou funkci a celé sestavení je napájené prostřednictvím micro USB kabelu a adaptéru do zásuvky.

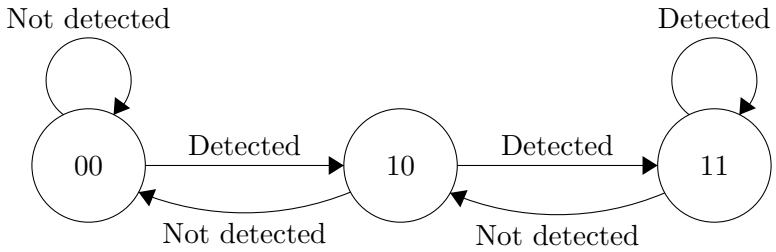
V první řadě deska slouží jako CoAP server na portu 5683 pro zpracování příchozích dat z bezdrátových modulů ESP-01 popsaných výše. Příchozí data jsou na server odesílána metodou POST. Při příchodu zprávy jsou spuštěny funkce pro zpracování dat.

Jelikož deska není vybavena dostatečnou velikostí paměti pro zálohu dat z teplotního čidla, bylo implementováno odesílání aktuální teploty na server *www.thingspeak.com*.

Tento server primárně určený pro zařízení *Internetu věcí* nabízí cloudové úložiště a grafické prostředí pro vizualizaci dat v podobě nejrůznějších nastavitelných grafů (u bezplatných uživatelů je nastavení omezené). Je nutná bezplatná registrace, při které je uživateli přidělen tzv. Api Key. Jedná se o řetězec znaků. Tímto řetězcem jsou příchozí data na server tříděna a poskytována jednotlivým uživatelům. Každý bezplatný uživatel může disponovat až osmi kanály pro příchozí data (může zpracovávat data z osmi různých zdrojů).

Data jsou odesílána na server prostřednictvím TCP spojení a HTTP protokolu, který obsahuje zmíněný Api Key (pro rozlišení uživatele), název kanálu (pro rozlišení zdroje dat) a samotná data (v tomto případě teplota). Výsledný graf lze jednoduše importovat do HTML stránky.

Pro zpracování příchozích dat z modulu ESP-01 umístěn v poštovní schránce je realizována jednoduchá logika popsána stavovým automatem (viz obrázek 3.10). Aby bylo zamezeno případným chybám v měření, je vyžadováno potvrzení naměřené hodnoty v po-



Obrázek 3.10: Stavový automat pro detekci příchozí pošty.

době následného měření. Obě tato měření jsou od sebe časově posunuta nastavitelným intervalem.

Pokud se logika dostane do stavu „11“, dochází k upozornění uživatele na poštu ve schránce pomocí zaslání e-mailu na zadanou e-mailovou adresu.

Pro zasílání elektronické pošty byl vytvořen e-mailový účet na stránkách *www.seznam.cz*. Pokud je detekována pošta v poštovní schránce, deska NodeMCU se připojí k SMTP serveru. Proběhne autentizace k vytvořenému účtu (uživatelské jméno a heslo jsou kódovány pomocí base64). Po úspěšném přihlášení je odeslán e-mail s textem „Došla Vám pošta.“. Pro vzdálenou kontrolu příchozí pošty v poštovní schránce je třeba jen zkontrolovat schránku elektronickou.

Uživatelské rozhraní

Další možností, jak získat přehledné informace o stavu poštovní schránky a aktuální teplotě je přes webové rozhraní. Deska NodeMCU také na své IP adrese poskytuje webovou stránku s potřebnými informacemi (viz obrázek 3.11). Byla snaha o přehlednost a jednodu-

Obrázek 3.11: Webová stránka zobrazující data.

chost rozhraní. Na stránce je zobrazena aktuální teplota. Dále je zde upravený graf z webu *www.thingspeak.com*. Pravá strana stránky je věnována informaci o stavu poštovní schránky. Pokud se nachází pošta ve schránce, dojde ke změně textu „Don't have a mail" na „Have a mail".

Z důvodu úspory paměti jsou všechny použité obrázky uloženy na webu *www.imgur.com* a kód se na ně odkazuje. Pro testování byla zvolena privátní IP adresa a web je tedy dostupný jen z lokální WiFi sítě.

Upozornění na příchozí poštu

Pokud je doručena do poštovní schránky pošta, je detekována, deska NodeMCU se připojí k SMTP serveru, proběhne autentizace a odeslání e-mailu na zvolenou adresu. Tohle upozornění by však mohlo být po jisté době nepříjemné. Zvláště pak, pokud by byla frekvence příchodů pošty příliš vysoká, a tak bylo potřeba toto upozornění regulovat.

Pro možnost nastavení upozornění byl k desce NodeMCU připojen modul HC-05, který rozšiřuje desku o možnost komunikace prostřednictvím bluetooth. Byla vytvořena jednoduchá mobilní aplikace pro telefony s operačním systémem Android (viz obrázek 3.12).

Obrázek 3.12: Rozhraní mobilní aplikace.

Aplikace byla vytvořena prostřednictvím webového rozhraní MIT App Inventor. Jedná se o cloudové vývojové prostředí, ve kterém lze programovat aplikace pro mobilní zařízení Android z internetového prohlížeče.

Aplikace nabízí stavovou lištu a tři různá tlačítka. Nejprve je třeba připojit mobilní zařízení k modulu HC-05. Pro tento účel slouží tlačítko „Select Bluetooth Device". Po stisknutí tlačítka se objeví nabídka se všemi bluetooth zařízeními v okolí. Po úspěšném spárování zařízení se objeví na stavové liště nápis „Connected". Nyní pomocí tlačítka „ON/OFF" lze zapnout/vypnout e-mailové upozornění na příchozí poštu. Pokud tedy uživatel očekává v příštích dnes příchod důležité pošty, připojí se přes bluetooth k desce NodeMCU a upozornění aktivuje. Poslední tlačítko je pro odpojení mobilního zařízení od HC-05 modulu. Po úspěšném odpojení se změní text stavové lišty na „Disconnected".

Testování

Samotné testování zařízení probíhalo v několika fázích. Nejprve bylo zapotřebí vyzkoušet činnost a hlavně funkčnost jednotlivých komponent. V této fázi se zjistilo, že jeden modul ESP-01 potřebuje pro správnou funkčnost vyšší napětí, než je 3,3 V. Pří této úrovni nepracoval a bylo jej třeba napájet 5 V. Při této úrovni se však přehříval a samovolně restartoval. Kvůli nestandardnímu chování byl vyřazen. Zřejmě došlo při manipulaci s modulem k poškození.

Druhá fáze testování probíhala pomocí nepájivých polí, na kterých byly propojeny všechny komponenty do výsledných zařízení. Na modulech ESP-01 byl nahrán software s názvem *init.lua*, což znamenalo, že při vypnutí a následném zapnutí zařízení byl software stále uložen a následně spouštěn. Deska NodeMCU byla přes micro USB kabel připojena k PC. Do desky byl nahrán software pro výpis příchozích dat a pomocí programu *ESPlorer* byla testována funkčnost sestavení.

Během této fáze testování se zjistil problém s nedostatečnou velikostí paměti v desce NodeMCU. Deska je určena na jednoduché softwarové úkony a v praktické části práce plní těchto úkonů více. Při pokusech o nahrání rozsáhlejšího programu nahrávání selhalo s hlášením „Not enough memory“. Z důvodu tohoto hlášení byla nutná optimalizace kódu. Výsledkem této fáze testování bylo zjištění, že naprogramovaný software funguje a pracuje spolehlivě.

Po zjištění, že všechny komponenty fungují, jsou správně propojeny a nahraný software pracuje spolehlivě, došlo k realizaci finální podoby zařízení. V této fázi se komponenty připájely na plošný spoj, propojily pomocí drátků a vše se umístilo do plastových krabiček. U konečného sestavení bylo nutné otestovat správné propojení jednotlivých komponent.

Dále následovalo na desku NodeMCU nahrání software s názvem *init.lua*, aby deska pracovala po odpojení od PC a následném připojení napájení pomocí USB adaptéru. V tento okamžik nastala třetí fáze testování. Modul ESP-01 detekující příchozí poštu se umístil do poštovní schránky. Modul Infra závora bylo třeba zkalibrovat pomocí trimru. Nejprve bylo simulováno vhození pošty do schránky a kontrolováno příchozí upozornění na e-mail. Jakmile byla ověřena zpětná vazba, modul se nechal umístěn ve schránce po dobu čtyř dnů. Po tuto dobu detekoval příchozí poštu.

Druhý modul ESP-01 byl umístěn ve venkovním prostoru do stínu. Po dobu čtyř dnů modul zůstal na svém místě a odesílal data na desku NodeMCU. Během těchto dnů docházelo k pravidelnému připojování na lokální web poskytovaný deskou pro kontrolu teploty.

Na závěr kapitoly byla vložena tabulka s cenou jednotlivých komponent využitých v praktické části práce.

Název	**ks**	**cena v Kč (bez DPH)**	**cena v Kč**
ESP-01	1 x	139	168
USB/UART FTDI převodník	1 x	185	224
NodeMCU DEVKIT 1.0	1 x	289	350
Bluetooth modul HC-05	1 x	221	267
Modul Infra závora	1 x	66	79
DS18B20	1 x	29	35

Tabulka 3.2: Cena jednotlivých komponent.

Kapitola 4

Závěr

Hlavním cílem bakalářské práce bylo popsat a definovat pojem *Internet věcí* a následně vytvořit zařízení spadající do této kategorie.

Pojem *Internet věcí* je velmi rozsáhlý, a tak bylo zapotřebí popsat dílčí části a související pojmy. Práce vznikala v období, kdy se *Internet věcí* formoval a kdy se vytvářely specifické podmínky na trhu pro zařízení spadající do *Internetu věcí*.

Nabité vědomosti bylo třeba ověřit v praxi a využít je při vytvoření zařízení spadající do kategorie *Internet věcí*. Tvorba zařízení postupovala podle dílčích kroků a výsledkem je několik propojených zařízení, která získávají data z okolí, zpracovávají je a poskytují uživateli zpětnou vazbu.

V praktické části práce byly z pohledu hardware využity vývojové desky, moduly a senzory, které jsou vhodné nebo dokonce přímo určené pro vytvoření zařízení spadajícího do kategorie *Internet věcí*. Z pohledu software byl pro výměnu dat využit protokol CoAP, který s protokolem MQTT má v kategorii *Internetu věcí* na trhu největší zastoupení.

Vytvořená zařízení jsou originální a praktická. Pro uvedení zařízení na trh by však bylo zapotřebí delšího testovacího období, kdy by se zařízení poskytla většímu spektru uživatelů a následně by se sledovala a analyzovala jejich zpětná reakce. Vše by vedlo k většímu přizpůsobení zařízení potřebám a požadavkům koncového zákazníka ve snaze uvedení zařízení na trh. V tomto směru spočívá možný další vývoj této práce.

Na závěr by bylo vhodné zdůraznit, že *Internet věcí* se stále vyvíjí a formuje. Samotný pojem obsahuje velký potenciál a je mu předpovídaná blízká budoucnost. Se zařízeními spadající do kategorie *Internet věcí* se však můžeme setkat již dnes. Všechny vytyčené cíle práce byly splněny.

Literatura

[1] ASHTON, Kevin. That 'Internet of Things' Thing: In the real world, things matter more than ideas. *RFID Journal* [online]. 2009, extbf3(1), 1 [cit. 2016-02-07]. Dostupné z: http://www.rfidjournal.com/articles/view?4986

[2] Recommendation ITU-T Y.2060: Overview of the Internet of things. *International Telecommunication Union* [online]. International Telecommunication Union, 2012 [cit. 2016-02-25]. Dostupné z: http://www.itu.int/rec/T-REC-Y.2060-201206-I

[3] Internet of things examples. *Postscapes* [online]. Denver: Colorado, 2013 [cit. 2016-02-07]. Dostupné z: http://postscapes.com/internet-of-things-examples

[4] VENKATESH, K., S. CHANDRAKANTH, J UMA MAHESH a Dr. K.V. NAGANJANEYULU. Internet of things. *International Journal of Innovations & Advancement in Computer Science* [online]. 2014, extbf3(8), 5 [cit. 2016-02-07]. ISSN 2347–8616.

[5] *Coap.technology* [online]. 2014 [cit. 2016-01-15]. Dostupné z: http://coap.technology/

[6] *Mqtt.org* [online]. MQTT community, 2014 [cit. 2016-01-15]. Dostupné z: http://mqtt.org/

[7] *The Bluetooth SIG* [online]. Kirkland: The Bluetooth Special Interest Group, 2016 [cit. 2016-01-15]. Dostupné z: https://www.bluetooth.com/

[8] XMPP: Oficiální stránky. *XMPP* [online]. Parker, CO 80134 USA: jabber.org, 2015 [cit. 2016-02-11]. Dostupné z: http://xmpp.org/

[9] AMQP. *Amqp.org* [online]. Burlington: OASIS, 2016 [cit. 2016-02-12]. Dostupné z: https://www.amqp.org/

[10] ZigbBEE. *Zigbee.org* [online]. Davis, CA: ZigBee Alliance, 2015 [cit. 2016-02-19]. Dostupné z: http://www.zigbee.org/

[11] Z-wave. *Z-wave.com* [online]. Sigma, 2016 [cit. 2016-02-22]. Dostupné z: http://www.z-wave.com/

[12] NEISSE, Ricardo, Gary STERI, Igor Nai FOVINO a Gianmarco BALDINI. SecKit: A Model-based Security Toolkit for the Internet of Things. *Computers* [online]. 2015, extbf54, 60-76 [cit. 2016-02-07]. DOI: 10.1016/j.cose.2015.06.002. ISSN 01674048.

[13] NATALIIA, Lukianova a Fell ELENA. Internet of Things as a Symbolic Resource of Power. *Procedia - Social and Behavioral Sciences* [online]. 2015, extbf166, 521-525 [cit. 2016-02-07]. DOI: 10.1016/j.sbspro.2014.12.565. ISSN 18770428.

[14] WEBER, Rolf H. Internet of Things – New security and privacy challenges. *Computer Law* [online]. 2010, extbf26(1), 23-30 [cit. 2016-02-17]. DOI: 10.1016/j.clsr.2009.11.008. ISSN 02673649.

[15] THE WNDW AUTHORS. *Wireless Networking in the Developing World*. 3. PDF: Butler, Jane, 2013. ISBN 978-1-4840-3935-9.

[16] 2016: KYBERÚTOKY SE ZAMĚŘÍ NA INTERNET VĚCÍ A BUDE TĚŽŠÍ JE ODHALIT. *Ekonomický deník* [online]. Praha: Ekonomický deník, 2015, 8. 12. 2015 [cit. 2015-12-27]. Dostupné z: http://ekonomicky-denik.cz/2016-kyberutoky-se-zameri-na-internet-veci-a-bude-tezsi-je-odhalit/

[17] Cloud computing: Jiný pohled na aplikace. *Zdrojak* [online]. Praha: Zdroják.cz, 2009, 3.7.2009 [cit. 2015-12-26]. Dostupné z: https://www.zdrojak.cz/clanky/cloud-computing-jiny-pohled-na-aplikace/

[18] The Constrained Application Protocol (CoAP). *RFC 7252* [online]. Bremen: Universitaet Bremen TZI, 2014, červen 2014 [cit. 2015-12-26]. Dostupné z: https://tools.ietf.org/html/rfc7252

[19] Programmer's Guide. *Iotivity* [online]. San Francisco: IoTivity, a Linux Foundation Collaborative Project, 2015, Nov 21, 2014 [cit. 2015-12-26]. Dostupné z: https://www.iotivity.org/documentation/linux/programmers-guide

[20] Kyberbezpečnost a Internet věcí. *Veracomp* [online]. Praha: Veracomp s.r.o., 2014 [cit. 2016-02-07]. Dostupné z: http://www.veracomp.cz/uploads/napsali%20o%20n%C3%A1s%202/Euro23_I_Extreme%20Networks.pdf

[21] History of Internet of things. *Postscapes: History of Internet of things* [online]. Denver: Colorado, 2013 [cit. 2016-02-07]. Dostupné z: http://postscapes.com/internet-of-things-history

[22] ITU Internet Reports: The Internet of Things. *ITU* [online]. Geneva: International Telecommunication Union, 2005 [cit. 2016-02-07]. Dostupné z: http://www.itu.int/net/wsis/tunis/newsroom/stts/The-Internet-of-Things-2005.pdf

[23] TI Internet of Things Overview: Internet of things. *Texas Instruments* [online]. Texas: Texas Instruments Incorporated, 2015 [cit. 2016-02-07]. Dostupné z: http://www.ti.com/ww/en/internet_of_things/iot-overview.html

[24] Cyber Tip: Be Vigilant with Your Internet of Things (IoT) Devices. *FBI* [online]. Washingtonu: fbi.gov, 2015 [cit. 2016-02-07]. Dostupné z: https://www.fbi.gov/news/news_blog/cyber-tip-be-vigilant-with-your-internet-of-things-iot-devices

[25] Cloud computing. *Wikipedia* [online]. 2015 [cit. 2016-02-07]. Dostupné z: https://cs.wikipedia.org/wiki/Cloud_computing

[26] IBM: Cloud-computing. *IBM* [online]. Armonk: IBM Corporation, 2015 [cit. 2016-02-10]. Dostupné z: http://www.ibm.com/cloud-computing/what-is-cloud-computing.html

[27] RFC 6120: Extensible Messaging and Presence Protocol (XMPP): Core. *RFC* [online]. P. Saint-Andre: Cisco, 2011 [cit. 2016-02-11]. Dostupné z: https://tools.ietf.org/html/rfc6120

[28] HASAN, Ragib, Md. Mahmud HOSSAIN a Rasib KHAN. Aura: An IoT based Cloud Infrastructure for Localized Mobile Computation Outsourcing. *SecretLab* [online]. University of Alabama at Birmingham, 2015, extbf1(1), 6 [cit. 2016-02-11]. Dostupné z: http://secret.cis.uab.edu/media/hasan2015aura.pdf

[29] TALLA, Vamsi, Bryce KELLOGG, Benjamin RANSFORD, Saman NADERIPARIZI, Shyamnath GOLLAKOTA a Joshua R. SMITH. *Powering the Next Billion Devices with Wi-Fi: PoWiFi* [online]. University of Washington, 2015, 1-13 [cit. 2016-04-02]. DOI: 10.1145/1235.

[30] Security in the Internet of things. *Windriver* [online]. Alameda, CA: Wind River Systems, 2015 [cit. 2016-02-16]. Dostupné z: http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf

[31] Lua: The Programming Language. *Lua.org* [online]. Departamento de Informática, PUC-Rio, 2016 [cit. 2016-04-15]. Dostupné z: https://www.lua.org/home.html

[32] ESP8266 Datasheet: Version 4.3. *Espressif.com* [online]. Espressif Systems IOT Team, 2015 [cit. 2016-04-15]. Dostupné z: https://cdn-shop.adafruit.com/product-files/2471/0A-ESP8266__Datasheet__EN_v4.3.pdf

[33] FT232R USB UART IC Datasheet: Version 2.13. *Http://www.ftdichip.com/* [online]. Future Technology Devices International, 2015 [cit. 2016-04-15]. Dostupné z: http://www.ftdichip.com/Support/Documents/DataSheets/ICs/DS_FT232R.pdf

[34] Oficiální stránky NodeMCU. *Nodemcu.com* [online]. Nodemcu Team, 2014 [cit. 2016-04-15]. Dostupné z: http://nodemcu.com/index_en.html

[35] HC-05: Bluetooth to Serial Port Module. *Teadstudio.com* [online]. ITead studio, 2010 [cit. 2016-04-15]. Dostupné z: http://www.robotshop.com/media/files/pdf/rb-ite-12-bluetooth_hc05.pdf

[36] DS18B20 datasheet: Programmable Resolution 1-Wire Digital Thermometer. *Http://www.gme.cz/* [online]. San Jose: Dallas semiconductor [cit. 2016-04-15]. Dostupné z: http://www.gme.cz/img/cache/doc/530/067/ds18b20-datasheet-1.pdf

[37] Bluetooth. *Wikipedia* [online]. wikipedia.org, 2016 [cit. 2016-02-18]. Dostupné z: https://cs.wikipedia.org/wiki/Bluetooth

[38] ZigBee. *En.wikipedia.org* [online]. wikipedia.org, 2016 [cit. 2016-02-19]. Dostupné z: https://en.wikipedia.org/wiki/ZigBee

[39] Z-Wave. *En.wikipedia.org* [online]. Wikipedia, 2016 [cit. 2016-02-22]. Dostupné z: https://en.wikipedia.org/wiki/Z-Wave

Přílohy

Seznam příloh

Příloha A

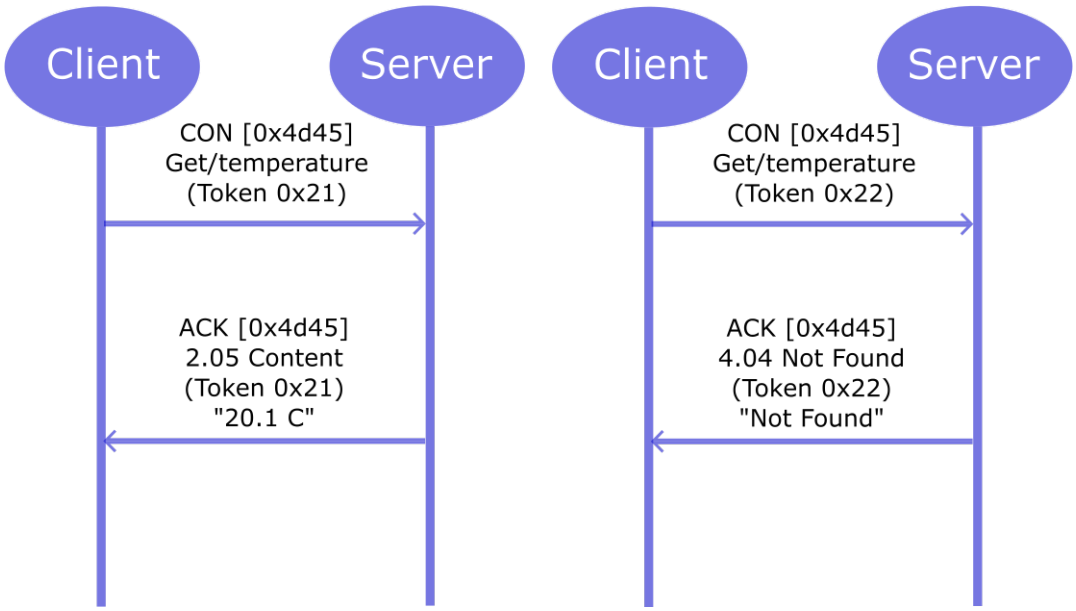
Obsah přiloženého CD

Na přiloženém CD se nacházejí tyto soubory:

- / (kořenový adresář)
  - *README* – Informace k přiloženému CD.
  - *Internet_veci.pdf* – Bakalářská práce *Internet of Things zařízení s podporou Bluetooth a CoAP* ve formátu PDF.
  - *PraceLatex.zip* – Všechny soubory potřebné k vysázení bakalářské práce *Internet_veci.pdf*.
  - /Mobilní aplikace
    - *BT_Email.apk* – Mobilní Android aplikace pro zapínání/vypínání upozornění na příchozí poštu v poštovní schránce.
  - /Detekce pošty
    - *init.lua* – Program v jazyce Lua pro zařízení využívající modul ESP-01 a modul Infra závoru pro detekci pošty v poštovní schránce.
  - /Měření teploty
    - *init.lua* – Program v jazyce Lua pro zařízení využívající modul ESP-01 a senzor DS18B20 pro měření venkovní teploty.
    - *ds18b20.lua* – Program pro získání správné teploty ze senzoru DS18B20 využitý v *init.lua*.
  - /Server
    - *init.lua* – Program v jazyce Lua pro zařízení využívající desku NodeMCU a modul HC-05 pracující jako server.

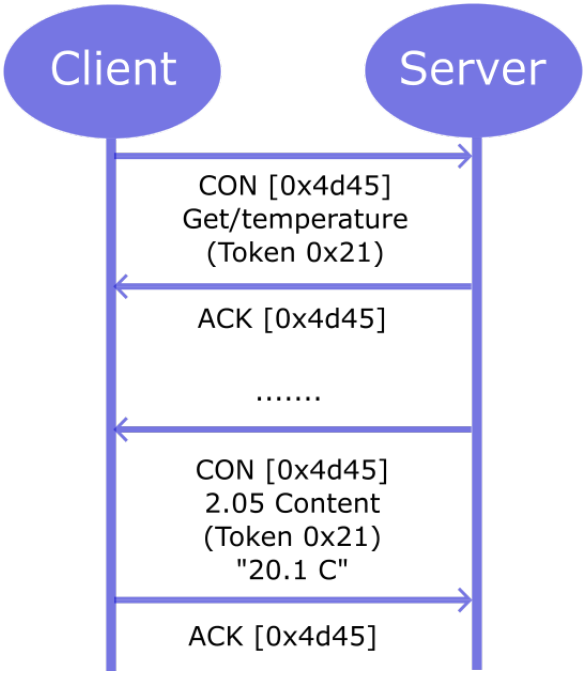
Příloha B

CoAP modely request/response

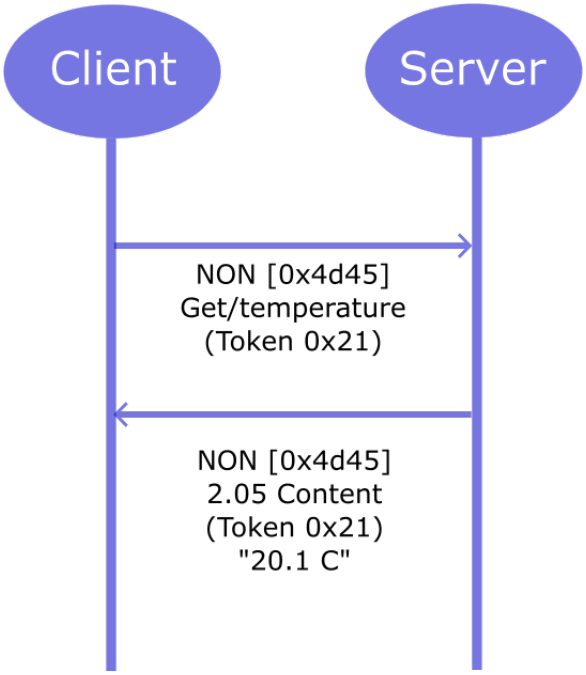


Obrázek B.1: Piggy-backed v modelu request/response[1].

[1]Převzato z: http://www.cse.wustl.edu/~jain/cse574-14/ftp/coap/.



Obrázek B.2: Separate response v modelu request/response[1].



Obrázek B.3: Zprávy typu Non-confirmable modelu request/response[1].

Příloha C

Prvky CoAP zprávy

Prvek zprávy	Hodnota	Zkratka	Poznámka
Adresa	224.0.1.187:5683		IP adresa zařízení a port
Verze	Verze 1 (0 1 b)		
Typ	00 Confirmable 01 Non-confirmable 10 Acknowledgement 11 Reset	CON NON ACK RST	
TKL	XXXX b		Délka v rozmezí 0 až 8
Code	(0.xx) Request (2.xx) Success (4.xx) Klient error (5.xx) Server error		Společné žádosti a odpovědi (requests and responses): GET (0.01), CREATED (2.01), CHANGED (2.04), CONTENT (2.05)
ID zprávy	0xXXXX	MID	Vytvořené odesilatelem
Token		TOK	Vytvořené klientem
Options			
Payload			

Tabulka C.1: Prvky CoAP zprávy

Prvek Zprávy	Hodnota	Poznámka
Adresa	224.0.1.187:5683	Multicast
Hlavička	NON, GET, MID = 0x7D40	GET (code=0.01)
Token	0x7555	Token Length = 2, Token = 0x7555
URI-path	oc	
URI-path	core	
URI-query	rt=core.sensor	
URI-query	if=core.mi.ll	

Tabulka C.2: Request zpráva

Prvky zprávy	**Hodnota**	**Poznámka**
Adresa	192.168.0.0:5683	Unicast
Hlavička	ACK,CONTENT, ID=0x7D40	Content (code=2.05), Message ID = 0x7D40
Token	0x7555	Token Length = 2, Token = 0x7555
Payload	Vzorek dat	

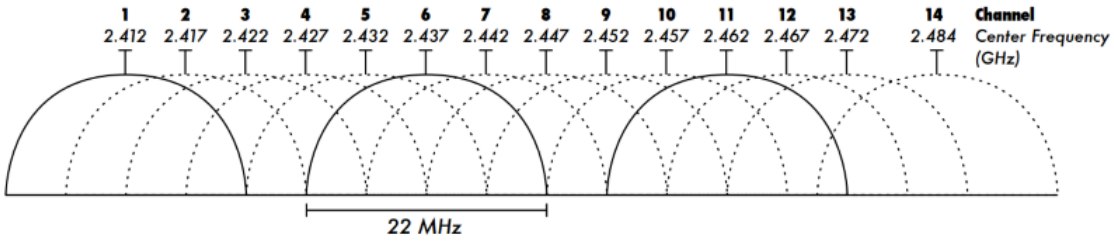
Tabulka C.3: Response zpráva

Příloha D

WiFi

Standard	**802.11a**	**802.11b**	**802.11g**
Datum představení	16. září 1999	16. září 1999	červen 2003
Pásmo	5,745–5,805 GHz	2,400–2,495 GHz	2,400-2,495 GHz
Rychlost	54 Mbs^{-1}	11 Mbs^{-1}	54 Mbs^{-1}
Modularita	OFDM	DSSS	OFDM
Aktuální propustnost	27 Mbs^{-1}	5 Mbs^{-1}	22 Mbs^{-1}

Tabulka D.1: WiFi standardy

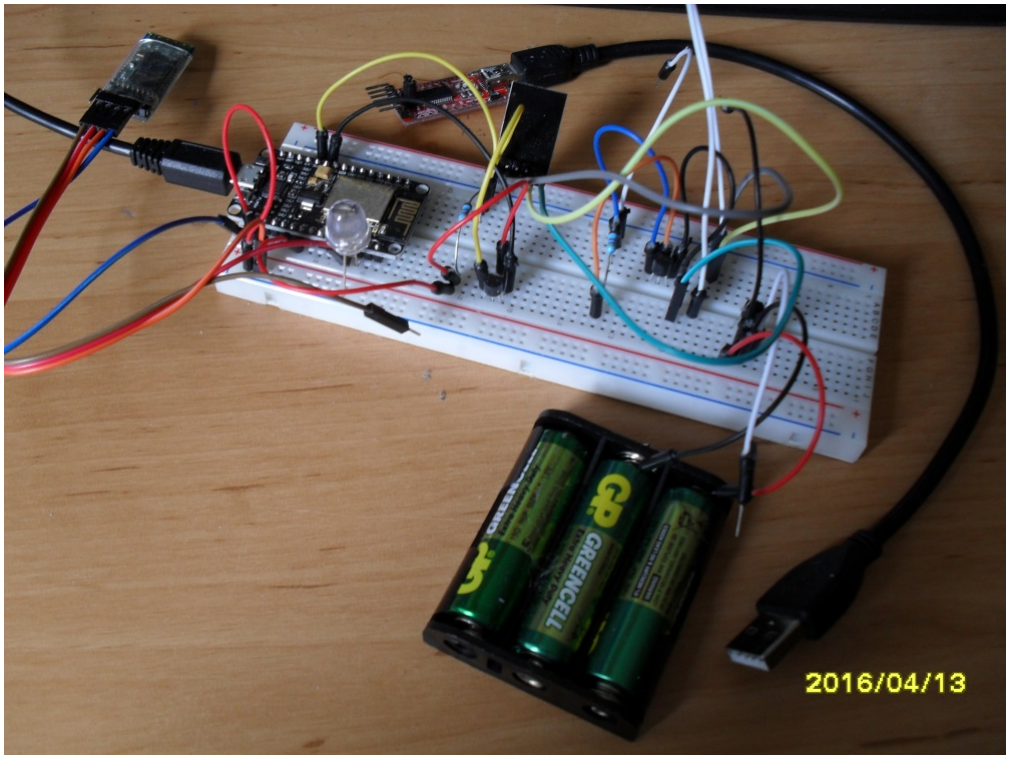


Obrázek D.1: Kanály rozdělující šířku pásma standardu 802.11b[1].

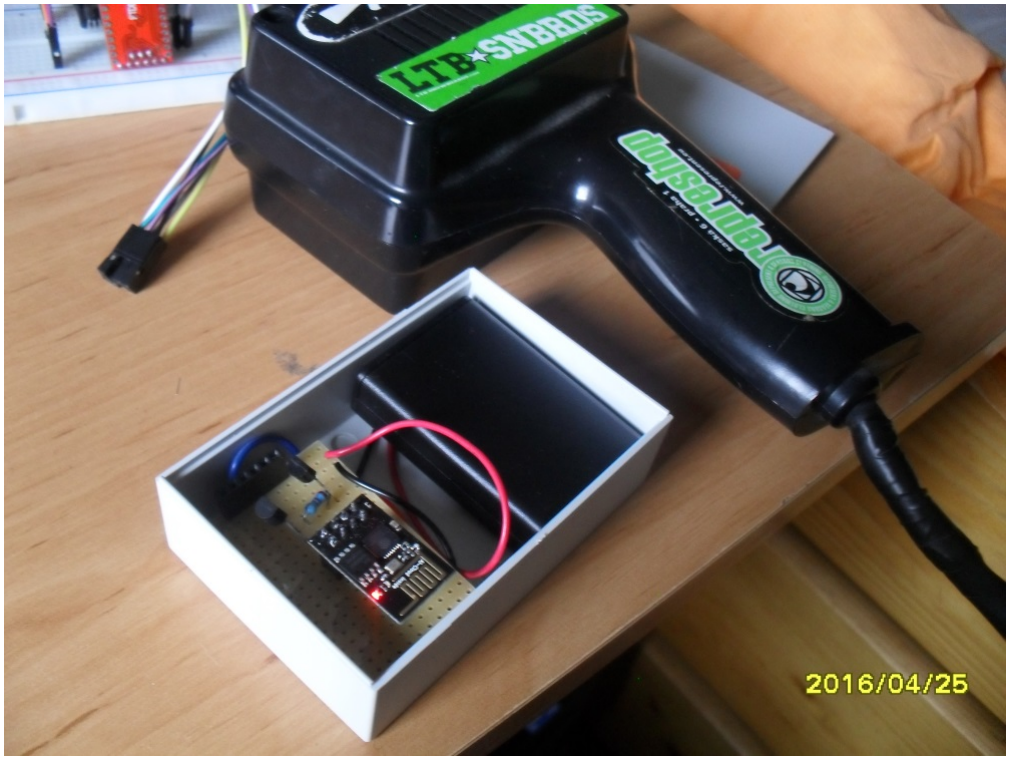
[1]Převzato z: https://kruckenberg1.wordpress.com/2010/06/15/identify-busy-wi-fi-channels-in-windows-7/.

Příloha E

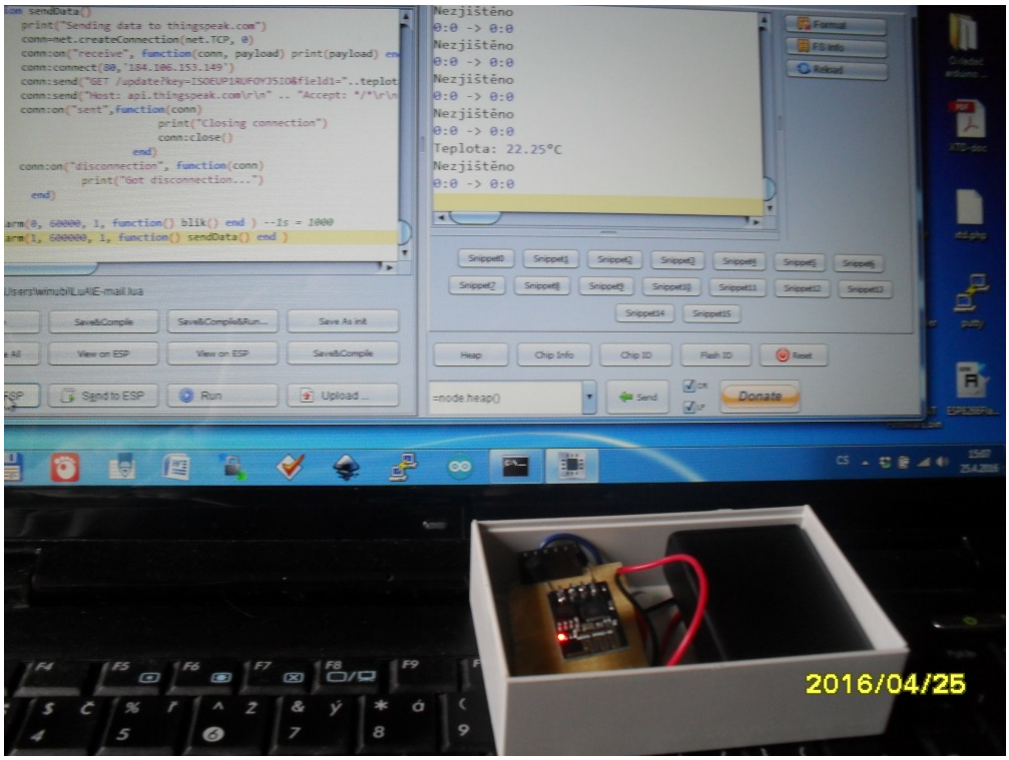
Realizace



Obrázek E.1: Propojování pomocí nepájivého pole.

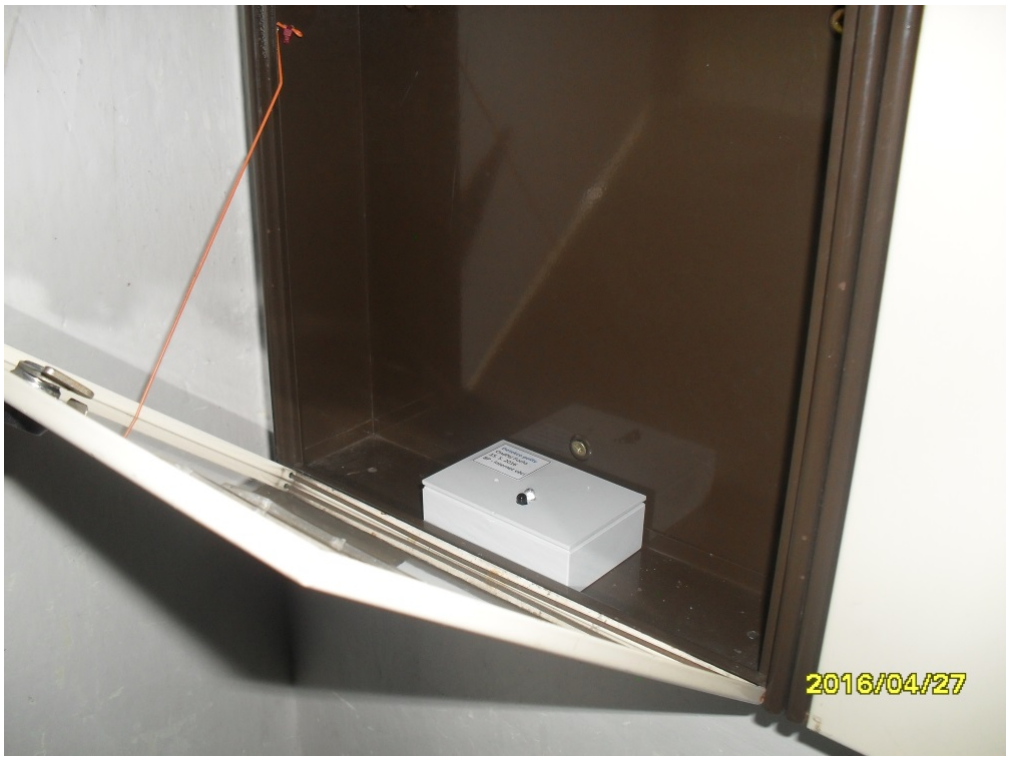


Obrázek E.2: Konečná podoba ESP-01 pro měření teploty.



Obrázek E.3: Testování měření teploty.

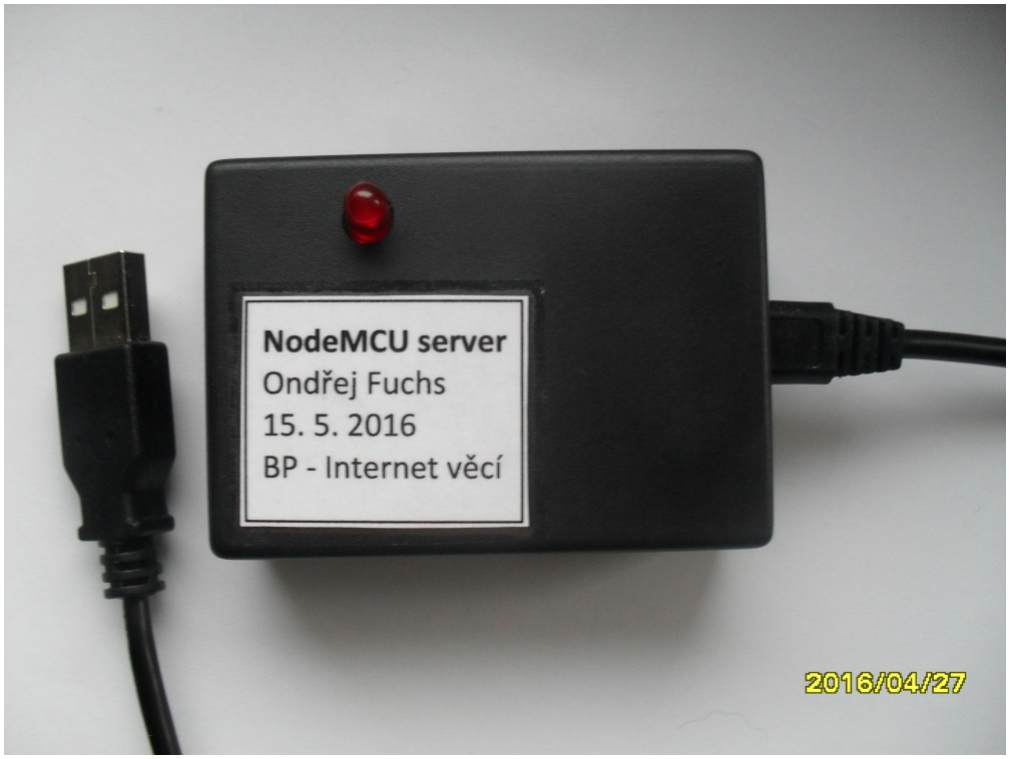
Obrázek E.4: Konečná podoba měřících senzorů.



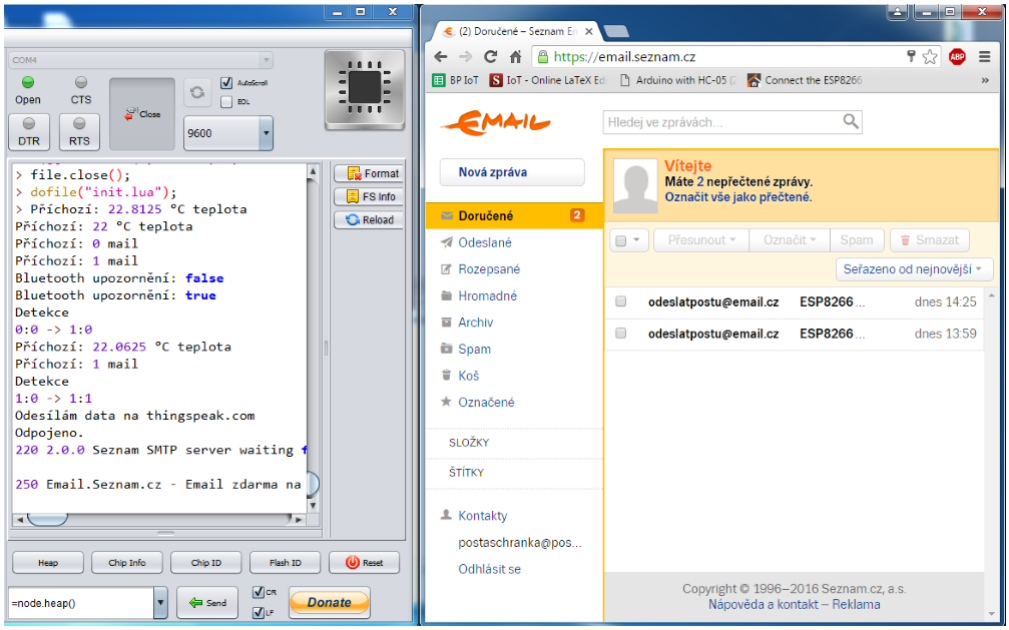
Obrázek E.5: Detail umístění ESP-01 pro detekci pošty.

Obrázek E.6: Umístění ESP-01 pro detekci pošty.

Obrázek E.7: Umístění ESP-01 pro měření teploty.



Obrázek E.8: Konečná podoba NodeMCU serveru.



Obrázek E.9: Příjem dat na NodeMCU a odesílání upozornění na e-mail.