

Internet věcí: přínosy a praktické aplikace

Daniel Réda

Bakalářská práce
2016



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2015/2016

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Daniel Réda**
Osobní číslo: **A13655**
Studijní program: **B3902 Inženýrská informatika**
Studijní obor: **Informační technologie v administrativě**
Forma studia: **prezenční**

Téma práce: **Internet věcí: přínosy a praktické aplikace**
Téma anglicky: **Internet of Things: Benefits and Practical Applications**

Zásady pro vypracování:

1. Zpracujte literární rešerši na téma vzájemné komunikace inteligentních systémů.
2. Provedte průzkum dostupných aplikací se zaměřením na praktickou využitelnost v domácnostech.
3. Vyberte a popište vhodné typy mikropočítačových vývojových desek pro demonstraci základních principů internetu věcí ve výuce.
4. Vyhodnoťte možná rizika internetu věcí a navrhnete způsoby řešení těchto rizik.
5. Vytvořte výukovou prezentaci zabývající se danou problematikou.

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **DHANJANI, Nitesh. Abusing the Internet of Things. United States of America: O'Reilly Media, 2010. ISBN 063-6-920-03354-7.**
2. **HOLLER, Jan. From machine-to-machine to the Internet of things: introduction to a new age of intelligence. Amsterdam: Elsevier Academic Press, 2014, xix, 331 pages. ISBN 9780080994017.**
3. **KUROSE, James F a Keith W ROSS. Počítačové sítě. 1. vyd. Brno: Computer Press, 2014, 622 s. ISBN 978-80-251-3825-0.**
4. **VASSEUR, Jean-Philippe a Adam DUNKELS. Interconnecting smart objects with IP: the next Internet. Burlington, MA: Morgan Kaufmann Publishers/Elsevier, 2010, xxiv, 407 p. ISBN 0123751659.**
5. **DR. OVIDIU VERMESAN a DR. PETER FRIESS. Internet of things: converging technologies for smart environments and integrated ecosystems. 2013. ISBN 9788792982964.**

Vedoucí bakalářské práce:

Ing. Petr Dostálek, Ph.D.

Ústav automatizace a řídicí techniky

Datum zadání bakalářské práce:

5. února 2016

Termín odevzdání bakalářské práce:

1. června 2016

Ve Zlíně dne 5. února 2016



doc. Mgr. Milan Adámek, Ph.D.
děkan



Ing. Miroslav Matýsek, Ph.D.
ředitel ústavu

Jméno, příjmení: Daniel Réda

Název bakalářské/diplomové práce: Internet věcí: přínosy a praktické aplikace

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 30.5.2016


.....
podpis diplomanta

ABSTRAKT

Tato bakalářská práce pojednává o Internetu věcí a zaměřuje se na praktické využití chytrých zařízení v domácnostech a ve výuce.

V teoretické části je nejdříve objasněn pojem Internet věcí, jeho vznik, uplatnění a situace na trhu. Po objasnění základního konceptu následuje přehled nových i konvenčních komunikačních technologií, na kterých chytrá zařízení v Internetu věcí pracují. V další kapitole jsou diskutována rizika plynoucí z používání těchto zařízení a přehled uplatnění chytrých zařízení v domácnostech.

Praktická část nabízí přehled vývojových desek vhodných pro výuku a demonstraci funkcí Internetu věcí. Součástí praktické části je i výuková prezentace, která shrnuje informace z teoretické části a jejím účelem je přiblížit problematiku této práce studentům.

Klíčová slova: Internet věcí, chytré zařízení, síťová komunikace, rizika internetu věcí, chytrá domácnost, výuka Internetu věcí, vývojové desky.

ABSTRACT

The theme of this bachelor thesis is Internet of things. It's focused on practical use of smart devices in homes and in teaching.

In the theoretical part there is firstly an explanation of the concept of Internet of Things, it's origin, areas of use and situation on market. After the explanation of the basic concept follows a summary of new and traditional communication technologies, on which the smart devices in Internet of Things are working. In the next chapter there are discussed the risks which emerges from use of these devices and a summary of use of smart devices in homes.

The practical part offers an analysis of development boards suited for teaching and for demonstrating the functions of Internet of Things. It also contain an educational presentation, which summarizes informations from the theoretical part and its goal is to bring the issues of this thesis to students.

Keywords: Internet of things, smart device, network communication, risks of Internet of Things, smart home, teaching of Internet of Things, development boards.

Rád bych poděkoval panu Ing. Petru Dostálkovi Ph.D. za cenné rady, věcné připomínky a vstřícnost při konzultacích a vypracování bakalářské práce.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD	9
TEORETICKÁ ČÁST	10
1 INTERNET VĚCÍ	11
1.1 CO JE INTERNET VĚCÍ	11
1.2 VZNIK	11
1.3 UPLATNĚNÍ, SITUACE NA TRHU A BUDOUCNOST	12
1.3.1 SITUACE NA TRHU	13
1.3.2 BUDOUCNOST IOT	13
2 KOMUNIKACE	14
2.1 TRANSPORTNÍ A SÍŤOVÁ VRSTVA VRSTVA	15
2.1.1 TCP/IP	15
2.1.2 PROČ TCP/IP?.....	16
2.1.3 INTERNET PROTOCOL VERSION 6	17
2.1.4 SMĚROVÁNÍ.....	17
2.1.5 UDP	20
2.2 LINKOVÁ A FYZICKÁ VRSTVA	20
2.2.1 IEEE	20
2.2.2 MOBILNÍ DATOVÉ SÍTĚ	22
2.2.3 WI-FI	22
2.3 APLIKAČNÍ VRSTVA	23
2.3.1 CoAP.....	23
3 RIZIKA IOT	24
3.1 ODPOSLOUCHÁVÁNÍ KOMUNIKACE	24
3.1.1 ZPŮSOBY ODPOSLOUCHÁVÁNÍ KOMUNIKACE	24
3.1.2 MOŽNÉ NÁSLEDKY	24
3.1.3 ŘEŠENÍ	25
3.2 ZÍSKÁNÍ PŘÍSTUPU K ZAŘÍZENÍ	25
3.2.1 ZPŮSOBY ZÍSKÁNÍ PŘÍSTUPU	25
3.2.2 MOŽNÉ NÁSLEDKY	26
3.2.3 ŘEŠENÍ	27
3.3 ZTRÁTA SOUKROMÍ	28
3.3.1 MOŽNÉ NÁSLEDKY	28
3.3.2 ŘEŠENÍ	29
4 APLIKACE IOT V DOMÁCNOSTECH	30
4.1 CHYTRÁ DOMÁCNOST	30
4.2 CHYTRÁ ZAŘÍZENÍ PRO DOMÁCNOSTI	31

4.2.1	PROSTŘEDÍ	32
4.2.2	ELEKTROINSTALACE	34
4.2.3	ZABEZPEČENÍ	35
4.2.4	MULTIMÉDIA	37
4.2.5	KUCHYNĚ	38
4.2.6	KOUPELNA	39
4.2.7	ZAHRADA	40
4.2.8	OSTATNÍ	41
PRAKTICKÁ ČÁST		42
5	VÝVOJOVÉ DESKY PRO VÝUKU MIKROPOČÍTAČŮ	43
5.1	DESKY ARDUINO	43
5.1.1	ENTRY LEVEL	44
5.1.2	ENHANCED FEATURES	45
5.1.3	IoT 47	
5.1.4	WEARABLE	47
5.1.5	SHIELDY	49
5.2	DESKY INTEL	49
6	VÝVOJOVÉ DESKY PRO VÝUKU PROGRAMOVÁNÍ	51
6.1	RASPBERRY PI	51
6.2	GIZMOSPHERE	53
7	VÝUKOVÁ PREZENTACE	55
ZÁVĚR		56
SEZNAM POUŽITÉ LITERATURY		57
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK		67
SEZNAM OBRÁZKŮ		70
SEZNAM TABULEK		71
SEZNAM SCHÉMÁT		72
SEZNAM PŘÍLOH		73

ÚVOD

Dnes ještě poměrně neznámý pojem Internetu věcí stále více proniká do lidských životů a čím dál více jej ovlivňuje. Současné předpovědi předních společností v oboru informačních technologií říkají, že v horizontu čtyř let bude mít téměř každý člověk v rozvinutém světě alespoň jedno chytré zařízení a to ať už na sobě nebo v domácnosti.

Cílem této bakalářské práce je v první řadě seznámit čtenáře s tímto trendem, ukázat jim oblasti, ve kterých najdou chytrá zařízení uplatnění, jaká je situace na trhu a co podle předpovědí čeká Internet věcí v budoucnosti.

Díky tomu, že jsou chytrá zařízení složena z malých zařízení s omezeným a různorodým výkonem, muselo dojít i k úpravě síťových technologií, aby splňovaly požadavky těchto sítí. Z těchto skutečností vyplývá potřeba celkové analýzy používaných komunikačních technologií, která je součástí teoretické části práce.

Už dnes je nabídka chytrých zařízení velmi pestrá a to zejména těch pro domácnost. Tzv. chytré domácnosti jsou hitem současnosti a v budoucnosti můžeme téměř jistě čekat jejich další rozvoj. Průzkum v této oblasti může inspirovat potencionální vývojáře, ale i seznámit čtenáře s posledními technologickými novinkami a ilustrovat funkce chytrých zařízení na praktických příkladech.

Hlavním cílem však je vzbuzení zájmu o tuto velmi perspektivní oblast informačních technologií ve studentech, kteří v této oblasti mohou najít uplatnění. Tohoto cíle je možné dosáhnout zařazením výuky Internetu věcí do osnov předmětů programování, mikropočítačů nebo síťových komunikací. Za tímto účelem je třeba vybrat vhodnou vývojovou desku, se kterou by studenti mohli pracovat. Právě tato problematika je součástí praktické části.

Praktická výuka se neobejde bez teoretických základů a proto budou všechny informace obsažené v této práci shrnuty ve výukové prezentaci, která poslouží k výuce teoretických základů Internetu věcí.

Díky tomu, že se jedná o poměrně novou a dynamicky se rozvíjející oblast informačních technologií, počet literárních zdrojů je velmi omezený a knihy jsou brzy zastaralé. Proto tato práce čerpá z velkého počtu internetových zdrojů, které o Internetu věcí dokáží podávat informace stejně rychle, jak se tato oblast rozvíjí.

I. TEORETICKÁ ČÁST

1 INTERNET VĚCÍ

1.1 Co je internet věcí

Internet věcí (IoT) je počítačový koncept sítě chytrých zařízení, které jsou vybaveny technologiemi ke sběru a výměně dat prostřednictvím internetu bez zásahu člověka.^[6]

Za původce definice je považován expert na digitální inovaci Kevin Ashton, který v článku pro magazín RFID Journal v roce 1999 napsal:^[6]

„Pokud bychom měli počítače, které by věděly o všem, co se dá o věcech vědět – za použití dat, které shromáždí bez lidské pomoci – byli bychom schopní sledovat a spočítat vše, a tím významně snížit ztráty, ceny i objem odpadů.“

Kevin Ashton, RFID Journal 1999^[7]

Za chytrá zařízení se označují takové objekty, které jsou vybaveny nějakým druhem senzoru nebo pohonu, mikroprocesorem, komunikačním zařízením a zdrojem energie. Funkce jednotlivých součástí jsou popsány na následujícím schématu:^{[4] [5]}

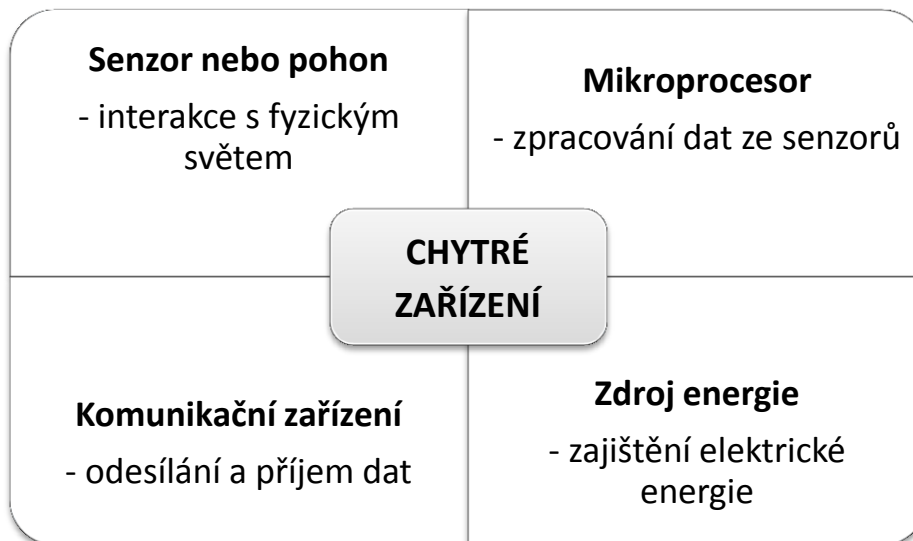


Schéma 1: Funkce součástí chytrého objektu

1.2 Vznik

IoT je výsledkem vývoje počítačových a telefonních technologií v posledních desetiletích. Mezi hlavní skutečnosti, které vedly ke vzniku IoT patří klesající ceny polovodičových součástek, zapříčiněné velkou poptávkou po tomto druhu čipů na trhu se smartphony

a tablety. Dalším je široké rozšíření Internetu a zvýšení jeho kapacity, rozvoj mikro-elektro-mechanických systémů (MEMS)¹, Cloudu a bezdrátových technologií.^[2]

První chytrý objekt, který odstartoval vývoj IoT vznikl na univerzitě Carnegie Mellon v Pittsburghu. Stáli za ním čtyři studenti: Mike Kazar, David Nichols, John Zsarnay a Ivor Durham; ti připojili automat na Coca-Colu k síti, aby mohli vzdáleně sledovat stav inventáře a teplotu nápojů.^[9]

1.3 Uplatnění, situace na trhu a budoucnost

Uplatnění najde IoT prakticky v každém odvětví lidského života. Nejrozšířenější oblasti současnosti včetně příkladů použití jsou uvedeny v následující tabulce:

Nositelná elektronika	Zábava, fitness, sledování prostředí a zdravotního stavu.
Zdravotní péče	Prevence, výzkum a monitoring.
Automobily	Autonomní vozidla, komunikace mezi vozy, telemetrie.
Chytré domácnosti	Zabezpečení, ovládání spotřebičů, optimalizace energií.
Chytrá města	Ovládání dopravy a osvětlení, správa parkování a odpadů.
Chytrý průmysl	Monitoring, správa a ovládání skladů, výroby, zásilek.

Tabulka 1: Nejrozšířenější odvětví IoT

IoT však nezasahuje pouze do lidských životů, ale i do života zvířat, jako například kachny v německém Radolfzelli, kterým tamní vědci z Institutu Maxe Plancka implantovali senzory na měření srdeční činnosti a tělesné teploty. Dokáží tak včas rozpoznat nástup ptačí chřipky, protože kachny mají vyšší teplotu už v době, kdy nemoc ještě nepropukla.^{[2] [10]}

¹ MEMS je technologie, která kombinuje počítače s malými zařízeními (např. senzory) do polovodičových

1.3.1 Situace na trhu

Žádná přesná čísla o velikosti IoT bohužel známá nejsou, ale podle dostupných dat se dá odhadnout, že v současnosti existuje na celém světě 10 – 23 miliard chytrých zařízení (tato čísla nezahrnují smartphony, tablety a počítače). Příjmy z těchto zařízení se pohybují mezi 300 miliardami až třemi trilióny dolarů za rok.^[11]

Největší společnosti pohybující se na trhu IoT společně s jejich rozdělením podle hlavního odvětví, ve kterém se pohybují jsou popsány v následující tabulce:

Výrobci software	IBM, Google, Microsoft, SAP, Oracle, HP, Amazon, BlackBerry, Facebook, PTC
Výrobci hardware	Cisco, Dell
Výrobci polovodičových součástek	Intel, Texas Instrument
Komunikace	Ericsson, AT&T, Orange, Verizon, Qualcomm
Spotřebitelské produkty	Apple, Samsung
Průmysl	GE

Tabulka 2: Největší společnosti na trhu IoT

Česká republika

Podle společnosti IDC, která se zabývá analýzou IoT, byla v roce 2015 celková hodnota trhu 774 miliónů dolarů a pro letošní rok předpovídají nárůst na 946 miliónů dolarů.^[12]

Česká republika je také domovem mnoha startupů zabývajících se trhem IoT. Mezi nejvýznamnější patří Jablotron, zabývající se zabezpečovacími zařízeními, AngelCam zabývající se chytrými kamerami a platformou pro ně a nebo SimpleCell, který plánuje pokrytí ČR dedikovanou IoT sítí ve spolupráci se společností T-Mobile.^[13]

1.3.2 Budoucnost IoT

IoT je v následujících letech předpovídán velký rozvoj. Odhady se liší společností od společností, ale dá se předpovědět, že do roku 2020 bude existovat 20 – 100 miliard chytrých zařízení s ročním příjmem z prodeje 1 – 7 triliónů dolarů. Předpovídá se, že hodnota českého trhu v roce 2019 dosáhne 1,6 miliardy dolarů.^{[11][12]}

2 KOMUNIKACE

Komunikace chytrých zařízení se označuje pojmem M2M (*Machine to machine – stroj ke stroji*). Tento pojem se často zaměňuje s pojmem IoT, ale nejsou až tak úplně stejné. M2M označuje komunikaci bez připojení k internetu a bez použití obecných internetových technologií. To znamená, že IoT je rozšířením M2M.^[2]

Hlavní vlastností M2M systémů je, že mezi sebou dokáží komunikovat samy bez lidského zásahu. Data jsou pak předávána ke konečnému uživateli, u kterého jsou teprve vyhodnocena.^[2]

Obecné M2M řešení se skládá z M2M zařízení, komunikační sítě, zařízení k umožnění obsluhy, aplikace a integrace do celkového systému.

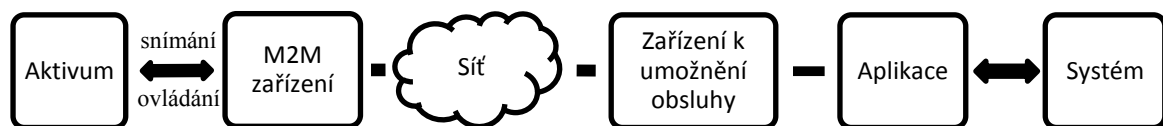


Schéma 2: Obecné M2M řešení

M2M zařízení je připojené k aktivu, které zprostředkovává snímání prostředí nebo interakci s ním. Síť zajišťuje vzdálenou komunikaci ať už bezdrátově nebo pomocí metalického vedení. Může být použito mnoho druhů sítě včetně Local Area Network (LAN) nebo větší Wide Area Network (WAN), které jsou někdy označovány jako Capillary Networks nebo M2M Area Networks. Trendem u většiny řešení M2M je použití zařízení k umožnění obsluhy, není však pravidlem. Toto zařízení zajišťuje obecnou funkcionalitu, která je běžná mezi mnoha různými aplikacemi a tím snižuje cenu implementace celého řešení a zjednodušuje vývoj aplikací. Následuje aplikace, která je většinou (také to není pravidlem) integrovaná do nějakého většího systému.^[2]

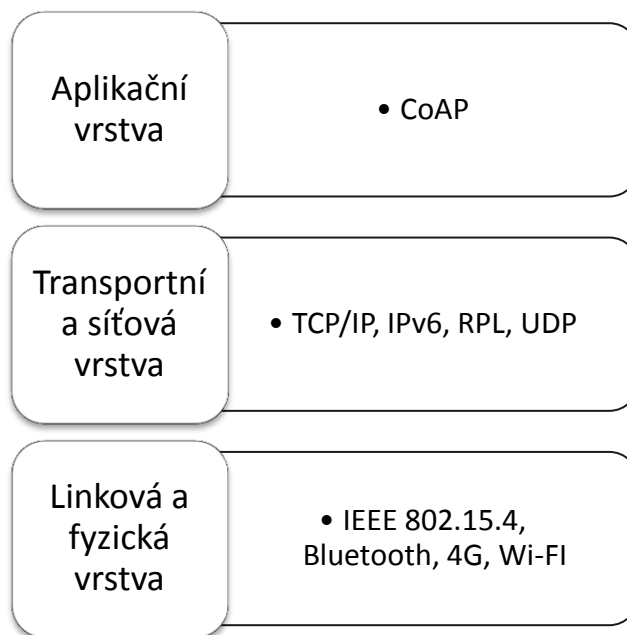


Schéma 3: Přehled komunikačních technologií IoT

2.1 Transportní a síťová vrstva

Komunikaci v transportní a síťové vrstvě zajišťuje stejně jako u klasického Internetu protokolová sada TCP/IP, rozšířená o IPv6 a protokol UDP. Pro směrování byl vyvinut nový standard RPL, protože konvenční směrovací protokoly jsou pro použití v IoT příliš náročné.

2.1.1 TCP/IP

Transmission Control Protocol (TCP) je síťový komunikační protokol, který pracuje na transportní vrstvě standardu OSI². Používá se k navázání spolehlivého spojení mezi dvěma zařízeními a k obousměrnému přenosu dat.^[14]

Internet Protocol (IP) je základním komunikačním protokolem pro výměnu dat v rámci počítačových sítí. K rozlišení zařízení v síti se používá IP adresa a data jsou zabalena do tzv. paketů. V rámci paketu jsou k datům přidána další metadata, ve kterých je například uvedena adresa příjemce a odesílatele, kódy pro detekci chyby, apod.^[15]

² Open System Interconnection (OSI) je konceptuální model definovaný Mezinárodní organizací pro normalizaci (ISO), který rozděluje síťovou komunikaci do sedmi vrstev podle poskytovaných služeb.^[17]

Spojením protokolů TCP a IP se vytvořil standard pro prakticky veškerou komunikaci v Internetu. V sadě protokolů TCP/IP se používají i další protokoly jako například ARP, ICMP, TCP, UDP nebo SCTP.^[16]

2.1.2 Proč TCP/IP?

Pro komunikaci v rámci IoT byla vybrána architektura TCP/IP a to nejen díky svému širokému rozšíření v současném Internetu, díky které mohou chytrá zařízení spolupracovat s již existujícími sítěmi, aplikacemi a službami. Při vybírání architektury byly stanoveny následující parametry, které si IoT vyžádala:^[4]

1. Schopnost rozvíjet se – ačkoli máme dnes představu o tom, kam IoT směřuje, nemůžeme vědět, jaký směr nabere v budoucnu a proto je třeba, aby se mohla architektura rozvíjet společně s IoT.
2. Velikost – sítě chytrých zařízení se skládají z mnoha uzlů a jejich zvyšující se počet bude zvyšovat nároky na počet adres potřebných ke směrování a řízení celé komunikace. Architektura se musí být schopná nadále rozšiřovat.
3. Rozdílnost aplikací – velký počet aplikací znamená velký počet rozdílů mezi jednotlivými aplikacemi. Architektura tak musí být vhodná jak pro využití v domácnosti, tak v průmyslu.
4. Rozlišnost komunikačních technologií – chytrá zařízení používají jak komunikaci po metalickém vedení, tak komunikaci bezdrátovou a často i kombinace těchto dvou. Architektura musí umět tyto rozdíly zvládnout.
5. Spolupráce s existujícími systémy a navzájem mezi samotnými zařízeními
6. Standardizace – mechanismy a protokoly architektury musí být standardizovány za použití otevřených standardů a dobře zavedeného standardizačního procesu. Stejně tak i patenty musí být volně dostupné.
7. Vyrovnání s potenciálně ztrátovou komunikací v síti
8. Délka použití – většina instalací chytrých sítí (zejména ve velkém měřítku) je určena k mnohaletému fungování. To znamená, že je kladen velký požadavek na výkon, který musí být zároveň energeticky úsporný a zároveň musí vydržet po celou životnost sítě.

9. Nízká energetická náročnost – chytrá zařízení jsou napájena z baterií, které nemohou být jednoduše vyměněny nebo nabity. Existují také zařízení, která dokáží získávat energii z okolí (jako například ze solární energie nebo z elektromagnetické energie). V každém případě energetická náročnost architektury musí být nízká, aby bylo dosaženo optimální životnosti celé sítě.

10. Nízká cena

Architektura TCP/IP se ukázala jako nejvhodnější řešení. K vybrání této architektury významně přispělo také zavedení protokolu IPv6.

2.1.3 Internet Protocol version 6

IPv6 (Internet Protocol version 6) je šestá revize standardu IP a je evolucí doposud používaného IPv4. IPv6 vznikl v polovině 90. let 20. století zejména jako reakce na rychlé vyčerpávání adres pro IPv4 u kterého se pro adresu používalo pouze 32 bitů, což umožňovalo použití 2^{32} adres (přibližně 4,2 miliard). Délka adresy u IPv6 je 128 bitová, takže je možné použít až 2^{128} adres (přibližně 340 undeciliónů).^[18]

Ačkoli se počátkem nového tisíciletí předpokládalo, že adresy vydrží ještě 20 let (hlavně díky používání nových řešení na bázi klasického IPv4), adresní prostor byl zejména kvůli nástupu chytrých zařízení vyčerpán 3. února 2011^[19]. IPv6 však není možné zavést kvůli velikosti Internetu ze dne na den a přechod se tak odehrává postupně. Nový protokol byl standardizován organizací Internet Engineering Task Force (IETF) a spuštěn v roce 1998.^[20] Dnes po více než sedmnácti letech využívá protokol IPv6 dle dat společnosti Google 10.8% uživatelů, kteří přistupují na jejich servery.^[21]

2.1.4 Směrování

IP sítě disponují směrovacím protokolem, jehož hlavní funkcí je stanovení „nejlepší“ cesty k cíli na základě různých parametrů. Například Routing Information Protocol (RIP) považuje za nejlepší cestu tu s nejmenším počtem uzlů, naopak podle protokolu Open Shortest Path First (OSPF) je nejlepší cesta ta, která stojí nejméně.^[4]

O směrování se starají routery nebo koncové stanice. Tato zařízení si vytváří směrovací tabulku, ve které si uchovávají informace o okolních uzlech. Díky těmto informacím se pak směrovač rozhodne, jakou nejlepší cestou paket odešle.^[4]

Směrování je klíčovou složkou v zajištění rychlosti a spolehlivosti komunikace v síti, obzvlášť se stále se rozšiřujícím počtem uzlů, jejichž počet se bude i díky rozvoji IoT nadále zvyšovat.^[4]

Síť složená z chytrých zařízení se však od té tradiční významně liší. Tradiční IP sítě jsou složeny z routerů napájených ze sítě, s pamětí RAM v řádech mega nebo gigabytů, s rozsáhlou flash pamětí, s jedním nebo více výkonných procesorů a jsou do sítě připojeny například optickým kabelem, který zajišťuje rychlý a spolehlivý přenos dat. Naopak síť chytrých zařízení je složena ze zařízení s nízkým výkonem a s poměrně nespolehlivým a pomalým datovým přenosem.^[4]

Low-power and Lossy Networks

Low-power and Lossy Networks (LLN) je označení pro síť složené z omezených chytrých zařízení, které jsou mezi sebou propojeny poměrně nestabilním a nízkorychlostním spojením.^[4]

Směrování v LLN se od klasického liší zejména v tom, že většina existujících směrovacích protokolů nebere při rozhodování v úvahu charakteristiku routeru. Používání dynamické metriky uzlu (například na základě průměrného zpoždění ve frontě) bylo studováno před mnoha lety v kontextu sítě ARPANET. Na základě mnoha obav (risk oscilace trasy, zejména v případě zahlcení, atd.) od něj ale bylo opuštěno. S příchodem LLN však začalo být nutné brát v úvahu charakteristiku uzlu, protože routery se významně liší výkonem, velikostí paměti nebo zdrojem energie.^[4]

Ještě zásadnějším rozdílem mezi LLN a tradičními IP sítěmi je míra bitové chybovosti (BER). U optického nebo Ethernetového spojení je obvykle bitová chybovost extrémně nízká a jejich systémy někdy dokáží chybu detekovat a opravit. Komunikace v LLN má velmi proměnlivou a často nepředvídatelnou kvalitu spojení způsobenou mnoha faktory z prostředí (jako například rušení, šum, apod.).^[4]

Použití ztrátových uzlů má přímý vliv na design směrovacího protokolu, protože ve většině směrovacích protokolů je jedním z nejkritičtějších komponentů čas konvergence (čas potřebný k nalezení/výpočtu alternativní trasy kolem nefunkčního síťového zařízení). Jakmile je porucha detekována je provoz přesměrován na alternativní trasu. Pokud by byl podobný přístup použitý v LLN mohlo by to vést k různým druhům oscilace a směrovacím smyčkám, které by v případě poruchy narušily směrovací protokol.^[4]

Směrování v LLN si vyžaduje odpovídající reakci během těchto poruch v síti. Po detekci chyby je provoz lokálně přesunut na další uzel bez okamžitého globálního přepočtu tras v síti. Chyba může být pouze přechodná a spouštění celosíťové konvergence by bylo nejen zbytečné, ale mohlo by vést k výměně protokolových zpráv, které by nežádoucím způsobem spotřebovávaly energetické a síťové zdroje.^[4]

Současný internet	LLN
Uzly jsou routery.	Uzly jsou senzory/pohony a routery.
Počet uzlů v řádu stovek.	Řádově vyšší počet uzlů.
Uzly a spojení je stabilní.	Spojení je velmi nestabilní a uzly přestávají fungovat daleko častěji.
Omezení uzlů nebo šířka pásma spojení typicky nejsou problémem.	Uzly a spojení jsou velmi omezené.
Směrování si není vědomé aplikací.	Směrování si musí být vědomé aplikací.

Tabulka 3: Rozdíl ve směrování v současném Internetu a v LLN

Za účelem nalezení směrovacího protokolu, který by vyhovoval charakteristikám LLN byla organizací Internet Engineering Task Force (IETF) ustanovena pracovní skupina Routing Over Low-power and Lossy networks (ROLL), která stanovila detailní požadavky pro směrování v LLN a snažila se najít už existující IP protokol, který by tyto požadavky splňoval. Žádný z existujících protokolů však požadavkům nevyhovoval a tak pracovní skupina ROLL přišla s novým protokolem nazvaným RPL.^[4]

Routing Protocol for Low-power and Lossy Networks

Routing Protocol for Low-power and Lossy Networks (RPL) je dálkový vektorový³ směrovací protokol navržený speciálně pro LLN. RPL převádí fyzickou topologii sítě do logické tak, že si vytvoří Directed Acyclic Graph⁴ (DAG). Celý graf se skládá z alespoň jedné instance a v každé instanci je celá topologie rozdělena do několika

³ Distance Vector Routing Protocol (DVRP) je jeden ze dvou hlavních směrovacích protokolů v IP. DVRP používá ke směrování jen dva faktory: vzdálenost a vektor. Vzdálenost představuje počet kroků nebo hostů, přes které musí zpráva projít. Vektor popisuje trajektorii zprávy přes danou sadou síťových uzlů.^[22]

⁴ DAG je typ orientovaného grafu s kruhovými cykly, ve kterém neexistuje trasa, která by začínala a končila ve stejném bodě.^[23]

Destination Oriented DAG (DODAG), aby byla umožněna větší škálovatelnost sítě. Každý DODAG je optimalizován tak, aby poskytl rozdílnou kvalitu služby. Cesty z každého uzlu jsou spojeny s kořenem DODAGu. Toto řešení nabízí redundantní cesty, které jsou pro LLN nutností a RPL tak může v případě poruchy provozu nabídnout více než jednu cestu mezi uzly.^{[4] [24]}

Dalšími významnými vlastnostmi RPL je jeho vysoká modulárnost, velmi malá stopa (potřebný výpočetní výkon v uzlu a velikost dat při přenosu v síti) a podpora širokého spektra metrik. Rané implementace RPL ukazují, že ke svému provozu potřebuje pouze několik kilobytů Flash paměti a několik kilobytů RAM.^[4]

2.1.5 UDP

User Datagram Protocol (UDP) je nejjednodušším protokolem v sadě TCP/IP, který slouží k přenosu datagramů mezi uzly. Datagram je tvořen z hlavičky obsahující služební informace (cílový a zdrojový port, délku dat a kontrolní součet) a samotná data. I přes to, že hlavička datagramu obsahuje kontrolní součet, je přenos v rámci UDP nespolehlivý. Protokol negarantuje doručení datagramů k cíli, jejich duplicitu a ani to, že budou doručeny ve stejném pořadí, v jakém byly odeslány.^[4]

Díky těmto vlastnostem je UDP jednoduchý, nenáročný a umožňuje rychlý přenos dat vhodný pro přenášení údajů ze senzorů v IoT.

2.2 Linková a fyzická vrstva

Pro komunikaci v linkové a fyzické vrstvě byl vyvinut nový standard IEEE 80.15.4. a Bluetooth with Low Energy. Dále se zde využívají již široce rozšířené technologie 4G a Wi-Fi.

2.2.1 IEEE

Institute of Electrical and Electronics Engineers (IEEE) je pracovní skupina zaměřená na vývoj standardů pro Personal Area Networks (PAN) a bezdrátových sítí na krátkou vzdálenost.^[25]

IEEE 802.15.4

Standard IEEE 802.15.4 byl vyvinut pro nízkorychlostní (Low Rate - LR) přenos dat mezi zařízeními s nízkou spotřebou energie, dlouhou životností baterie a velmi nízkou složitostí. Definuje fyzickou i linkovou vrstvu OSI modelu.^[26]

Vlastnosti IEEE 802.15.4:

- Rychlost přenosu dat: 250, 40 a 20 kbit/s.
- Dosah: v ideálních podmínkách 1000m, v běžných podmínkách 10 – 75 metrů.
- 2 adresní módy: 16 a 64 bitové.
- CSMA-CA⁵.
- Řízení spotřeby k zajištění nízké spotřeby energie.
- 16 kanálů v pásmu 2.4 GHz, 10 kanálů v pásmu 915 MHz a jeden kanál v pásmu 868 MHz.

Na bázi IEEE 802.15.4 pracují sítě ZigBee, 6LoWPAN, WirelessHART a ISA100.11a.

Bluetooth

Bluetooth (standardizovaný IEEE pod číslem 802.15.1) je standard bezdrátové technologie, pracující na krátké vzdálenosti, vyvinutý společností Ericsson v roce 1994. Existuje ve dvou navzájem nekompatibilních verzích: Bluetooth Basic Rate/Enhanced Data Rate a Bluetooth with Low Energy. Existují také čipsety obsahující obě verze.^[28]

Bluetooth with Low Energy

Někdy také označovaný jako Bluetooth Smart, Version 4.0+ nebo Wibree byl vyvinut speciálně pro IoT. Vyznačuje se zejména nízkou spotřebou, která je tak důležitá v sítích složených z chytrých zařízeních. Spotřeba je snížena díky tomu, že přenos není kontinuální jako u klasického Bluetoothu, ale probíhá pouze v krátkých dávkách.^[29]

⁵ Carrier Sense Multiple Access with Collision Advance (CSMA/CA) je síťový protokol používaný k předcházení kolizí v síti. Před odesláním paketu stanice určitý čas poslouchá, jestli na kanálu už nevysílá jiná stanice. Pokud je kanál volný, stanice začne vysílat.^[27]

	Klasická Bluetooth technologie	Bluetooth with Low Energy
Pásmo	2,4 – 2,483 GHz	
Dosah	100m	>100m
Přenosová rychlost	1 - 3 Mbit/s	1Mbit/s
Spotřeba energie	1W	0,01 – 0,5 W

Tabulka 4: Srovnání Bluetooth technologie a Low Energy technologie^[30]

Bluetooth však není v pravém smyslu slova komunikační technologií IoT, protože nezprostředkovává přímé spojení s internetem, ale pouze M2M komunikaci. Nelze ho však opomenout, protože jeho použití je v rámci chytrých zařízení velmi rozšířené. Je tak součástí řetězce v rámci IoT, ale spojení s internetem zajišťuje jiné zařízení.^[31]

2.2.2 Mobilní datové sítě

Mobilní datové sítě (4G/3G/GSM) používané hlavně pro provoz mobilních telefonů jsou vhodné pro chytrá zařízení, která pracují na velkou vzdálenost. Jejich velkou nevýhodou je však spotřeba energie, která je v IoT často kritickým parametrem.^[31]

	GSM	3G	4G
Pásmo	380 – 1900 MHz	1,8 – 2,1 GHz	2 – 8 GHz
Přenosová rychlost	35 – 384 kbit/s	384kbit/s - 10Mbit/s	3 - 20Mbit/s

Tabulka 5: Srovnání mobilních datových sítí^[32]

Důležitou vlastností mobilních datových sítí (zejména sítě 4G) je jejich bezpečnost a spolehlivost. Hodí se tak například pro použití v bezpečnostních systémech.^[31]

2.2.3 Wi-Fi

Wi-Fi je označení standardu IEEE 802.11, který definuje bezdrátovou LAN (WLAN). Wi-Fi je bezdrátovou verzí Ethernetové⁶ sítě a bývá používána společně. Ačkoli se výraz Wi-Fi všeobecně používá jako označení WLAN, jde pouze o obchodní značku Wi-Fi Alliance, která takto certifikuje zařízení splňující její standardy.^[33]

⁶ Ethernet je řada síťových technologií používaných v LAN, kde jsou zařízení (počítače) propojeny fyzickým prostředkem (síťovým kabelem).^[35]

Wi-Fi pracuje ve frekvenčním pásmu 2,4 a 5 GHz, dosah signálu je přibližně 50 m a může dosahovat rychlosti až 600 Mbit/s. Hlavní výhodou použití Wi-Fi je její rozšíření v domácnostech a v kancelářích, což z ní dělá ideální volbu pro chytrá zařízení pracující v těchto prostorech. Mezi nevýhody patří nízká spolehlivost a bezpečnost.^{[31] [32]}

Wi-Fi HaLow

Wi-Fi HaLow (respektive 802.11ah), je poměrně nový standard, který má za úkol rozšířit dosah Wi-Fi signálu a snížit jeho spotřebu energie tak, aby vyhovoval požadavkům IoT. Nabízí téměř dvojnásobný dosah signálu a lepší penetraci prostředím.^[34]

2.3 Aplikační vrstva

2.3.1 CoAP

Constrained Application Protocol (CoAP) je webový protokol vyvinutý k použití v omezených uzlech a sítích IoT. CoAP používá stejně jako HTTP úspěšný model REST: servery zpřístupňují zdroje pod URL a klienti k těmto metodám přistupují pomocí metod jako GET, PUT, POST a DELETE. Díky tomu jsou tyto dva protokoly navzájem zcela kompatibilní a webový klient ani nemusí poznat, že přistupuje k senzoru. K fungování CoAPu stačí pouhých 10 KiB RAM paměti a 100 KiB kódového prostoru.^[36]

3 RIZIKA IOT

3.1 Odposlouchávání komunikace

Díky tomu, že většina chytrých zařízení komunikuje v nelicencovaném pásmu, která sice nabízejí možnost levného připojení, ale na druhou stranu představují velkou bezpečnostní hrozbu, protože kdokoli má do těchto pásem přístup a může tuto komunikaci odposlouchávat.^[37]

3.1.1 Způsoby odposlouchávání komunikace

Sniffing

Sniffing je nejpoužívanějším způsobem odposlouchávání síťové komunikace. Útočník pomocí nástroje zvaného Packet sniffer nebo Packet analyzer zachytává pakety (vytváří jejich kopie), které proudí v síti (ať už přes vodiče nebo bezdrátově) a následně je analyzuje nebo dešifruje (pokud je komunikace zašifrovaná). Sniffery mohou být softwarové programy nebo hardwarové zařízení.^[38]

Man-in-the middle attack

Dalším oblíbeným způsobem odposlouchávání komunikace je tzv. Man-in-the middle attack, kdy například útočník zaútočí na TCP připojení mezi klientem a serverem. Útočník rozloží tuto komunikaci do dvou nových spojení, jedno mezi klientem a útočníkem a druhé mezi útočníkem a serverem. Útočník se tak tváří jako proxy server a nejen, že může celou komunikaci odposlouchávat, ale může i s daty manipulovat nebo přidávat vlastní.^[39]

3.1.2 Možné následky

Útočníci se tak mohou dostat nejen k přihlašovacím údajům nebo k informacím o platební/kreditní kartě, ale i k telemetrickým datům o uživateli. Ty lze získat například z nositelných zařízení, jako jsou fitness náramky. Candid Wueest, vědec pracující ve společnosti Symantec, provedl v roce 2014 experiment na konferenci Black Hat, kde byl pomocí Raspberry Pi schopný odposlouchávat komunikaci chytrých fitness náramků a zjistit tak hardwarové adresy zařízení nebo kdy jejich majitel přišel a odešel.^[40]

Telemetrické údaje pak mohou být použity například při vloupání, kdy zloděj má informace o pohybu obyvatelů domu nebo monitoruje komunikaci mezi chytrými zařízeními v domácnosti, která uživatele sledují za ně. Tato data mohou být zneužita

i obchodníky k monitorování zákazníků. Dozví se například, jak se zákazník pohybuje po prodejně nebo sledováním jeho tělesných funkcí zjistí, jak reaguje na nabídky a na základě těchto dat mohou upravovat obchodní strategii.

Data o platebních kartách mohou být zneužity k vlastnímu obohacení nebo prodány. Přihlašovací údaje lze použít k přístupu k zařízení nebo do celého systému, a nebo mohou být stejně jako informace o platebních kartách prodány. Mimo tato data jsou se útočníci schopni dostat i k citlivým údajům o uživateli, kterými ho mohou vydírat.

3.1.3 Řešení

Řešením problému s odposlechy je použití šifrování, které je však výpočetně náročné, vytěžuje omezený hardware chytrých zařízení a spotřebovává drahocennou energii. Šifrování musí probíhat na všech článcích celého komunikačního řetězce, od dat ze senzorů až po konečné zařízení, které data zpracovává.

Šifrovací protokoly, které je možné použít v IoT jsou Transport Layer Security (TLS), jeho předchůdce Secure Sockets Layer (SSL) používající asymetrické kódování a Advanced Encryption Standard (AES), které používá symetrické kódování.^{[41] [42]}

Dalším možným řešením je použití bezpečnějšího prostředí licencovaného pásma, kde pracují například mobilní datové sítě.^[31]

3.2 Získání přístupu k zařízení

Získání přístupu k chytrému zařízení představuje větší ohrožení než odposlouchávání komunikace, protože může dojít nejenom ke ztrátě citlivých dat, ale i ke škodě na majetku, zdraví a dokonce i ke smrti.

3.2.1 Způsoby získání přístupu

Bezpečnostní nedostatky zařízení

K získání přístupu k zařízení se nejčastěji využívá bezpečnostních nedostatků, kterých existuje celá řada. Většinou jde o softwarové chyby, které útočníci odhalí a zneužijí je. Může jít například o ukradnutí tokenu, který v sobě uchovává přihlašovací identitu, o tzv. Time-of-Check-to-Time-of-Use útok, který cílí na schopnost ověření legitimity softwarového updatu a mnoho dalších.^[1]

Lidská chyba

Uživatelé jsou v drtivé většině případů tím nejslabším článkem v řetězci zabezpečení. Velkým problémem je zejména nezměnění standardních přihlašovacích údajů, které jsou snadno dohledatelné (většinou přímo na webových stránkách výrobce). Pouhá změna hesla však nestačí. Uživatelé se také dopouští velkého bezpečnostního ohrožení, když si nastavují snadno uhodnutelná hesla jako je „heslo“ nebo „12345.“ Dalším problémem je neaktualizování zařízení, kdy už známá chyba není patchem opravena a útočník ji tak může lehce zneužít. Významnou roli také hraje lidská nepozornost a počítačová negramotnost, která může vést k instalaci malwaru nebo jiných škodlivých aplikací či k prozrazení přihlašovacích údajů při phishingu.^[1]

Prolomení hesla

Útočníci se také mohou pokusit prolomit heslo a tak získat přístup do systému. K prolomení hesla se používá mnoho metod, mezi které patří například výše zmíněný phishing, při kterém se útočník snaží pomocí podvodného mailu získat od uživatele přihlašovací údaje. Dalšími populární metodou je slovníkový útok, kdy útočník zkouší slova ze slovníku nebo útok brutální silou, při kterém se snaží útočníkův algoritmus projít všechny možné alfanumerické kombinace.^[43]

3.2.2 Možné následky

Stejně jako při odposlouchávání komunikace mohou útočníci získat přístup k citlivým datům uživatele, ale rozsah potenciálně ukradených dat je daleko větší. Útočníci jsou nejen schopni sledovat data ze zařízení, ale také je ovládat, což může mít nedozírné následky.

Velkým problémem jsou dětské chůvičky a webové kamery, kterým uživatelé nezměnili přihlašovací údaje. V roce 2014 se na Internetu objevil web, který tyto nezabezpečené kamery indexoval a počet postižených zařízení se vyšplhal až k 73 011. Dnes je tento web už nedostupný, ale problém nadále přetrvává. Díky nezabezpečeným nebo špatně zabezpečeným kamerám může útočník získat vizuální data o celé domácnosti, podniku, či jiném prostranství. Nejen, že jde o obrovský zásah do soukromí, ale je možné tato data použít i pro sledování nebo jinou trestnou činnost. Podobně jsou na tom i chytré televize, u kterých lze získat přístup ke kameře nebo k mikrofonu.^{[1] [44]}

V chytrých domácnostech může získání kontroly nad zařízeními vést k drobným nepříjemnostem, jako je například manipulace s chytrými světly, ale také k poškození

majetku, kdy útočník například naruší chod chytré trouby a ta začne hořet. Dalším rizikem je překonání bezpečnostního systému a neoprávněného vniknutí.

Ve firemním prostředí je ohrožení převzetím kontroly ještě markantnější, protože škody mohou být daleko větší. Stačí upravit data ze senzorů ve výrobě a celá várka může být zničena, popřípadě může dojít k poškození strojů nebo k ublížení na zdraví. Velkou bezpečnostní hrozbou představují také chytrá zařízení, která si donesou sami zaměstnanci. Tato zařízení se připojují k firemní síti a mohou jí významně ohrozit. Nejen u běžných chytrých zařízení, ale i u chytrých hodinek nebo kávovarů může bezpečnostní nedostatek vést ke kompromitaci celé sítě. Stejně jako u chytrých domácností také hrozí překonání zabezpečovacího systému.^{[5] [45]}

Největší škody by však napáchal útok na chytrá města. Útočníci mohou narušit chod dopravy upravením semaforů, zhasínat pouliční osvětlení, vypnout elektřinu nebo se nabourat do informačních systémů a manipulovat s nimi.

V bezpečí nejsou ani chytrá vozidla, u kterých může dojít k ohrožení zdraví účastníků provozu, potažmo až ke smrti. To velmi dobře ilustrovali hackeři Charlie Miller s Chrisem Valaskem v experimentu pro internetový magazín Wired v roce 2015. V experimentu se jim podařilo vzdáleně získat přístup prostřednictvím multimediálního systému k jedoucímu Jeepu Cherokee. Nejen, že mohli ovládat multimediální systém, ale dostali se i k ovládání motoru a brzd.^[46]

3.2.3 Řešení

1. Výuka uživatelů – je třeba je poučit o možných rizicích a jak jim předcházet například tím, že si na svých zařízeních změní standardní přístupové heslo nebo nebudou používat snadně uhodnutelná hesla. Musí se změnit i politika výrobců, kteří se snaží dělat zařízení tak, aby je bylo možné okamžitě použít a uživatel nebyl zatěžován možnostmi nastavení, díky kterým by bylo možné zabezpečení zvýšit.
2. Zlepšení zabezpečení zařízení – výrobci musí dbát více na zabezpečení zařízení, řádně je testovat a řešit vzniklé nedostatky ještě před vypuštěním na trh. Současná praxe je většinou taková, že se výrobci snaží uvést produkt na trh co nejdříve a zanedbávají tak řešení bezpečnostních nedostatků, nebo na úkor nižší ceny produktu nevěnují zabezpečení dostatečnou pozornost.

3. Zlepšení způsobů identifikace uživatele – nestačí pouze přihlášení jménem a heslem. Dobrým řešením je dvoufázové přihlášení, které však není vždy pro uživatele pohodlné. Ideálním řešením je implementace biometrických identifikačních systémů, které jsou spolehlivé a zároveň po uživateli nevyžadují zapamatování uživatelských jmen a hesel.
4. Vydávání patchů a jejich snadná (a automatická) instalace – opravování chyb pomocí patchů je zásadní a jedná se o běžnou praxi. U IoT však vzniká problém v tom, že jestliže má uživatel zařízení od různých výrobců, musí každé zařízení aktualizovat zvlášť a to často ještě ručně. Je třeba tento proces zcela zautomatizovat, aby byly chyby v zařízeních co nejdříve opraveny a zároveň aby nebyly kladeny velké nároky na uživatele.
5. Instalace tzv. Kill Switche – pomocí Kill Switche je možné chytré zařízení vypnout. Používá se například u chytrých vozidel, kdy v případě poruchy nebo nebezpečí může řidič převzít nad vozidlem kontrolu. Uplatnění by však našlo u všech chytrých zařízení, kdy by bylo možné v případě poruchy či útoku vypnout jeho „chytrou funkci.“ Například pokud by byla od útokem chytrá lednička, uživatel by pomocí Kill Switche vypnout její software, ale její základní funkce (mražení) by fungovala dál.

3.3 Ztráta soukromí

Nejdiskutovanějším tématem v rámci IoT je otázka ztráty soukromí. Jak chytré produkty čím dál více pronikají do lidských životů, shromažďují o nich obrovské množství dat. Ta se ocitají v rukou firem na základě dlouhých smluvních podmínek, které si drtivá většina uživatelů ani nečte.

3.3.1 Možné následky

O data z IoT mají velký zájem reklamní společnosti, kterým by tato data mohla významně pomoci s cílením reklamy. V budoucnu by tak například mohla chytrá váha zjistit, že její uživatel přibral. O tom by se dozvěděla chytrá televize a ukazovala by kontextové reklamy na prostředky na hubnutí a lednice by zase uživateli nabízela na svém displeji nízkotučný jogurt.^[47]

Dalším subjektem, který má o tyto data velký zájem je vláda, která by prostřednictvím chytrých zařízení mohla monitorovat své obyvatele.

3.3.2 Řešení

V první řadě musí společnost upravit své smluvní podmínky tak, aby měl uživatel přehled a kontrolu nad tím, jaká data jsou o něm shromažďována a jak je s nimi nakládáno. Společnosti musí respektovat rozhodnutí zákazníka, který si nepřeje být profilován a aby o něm nebyla shromažďována data. ^[5]

Poté je nutné zavedení zákonů, které by přesně stanovovaly, jak smí společnosti s osobními údaji uživatelů nakládat a samozřejmě respektování těchto zákonů jak samotnou vládou, tak i společnostmi. ^[5]

4 APLIKACE IOT V DOMÁCNOSTECH

4.1 Chytrá domácnost

Chytrá domácnost je domácnost, ve které jsou nainstalovány pokročilé automatizační systémy, které nabízejí svým obyvatelům sofistikované monitorování a kontrolu nad funkcemi budovy. Chytrá domácnost může například ovládat světla, teplotu, multimediální zařízení, zabezpečení, okna a dveře, a mnoho dalších funkcí. Aplikace se nejčastěji ovládají prostřednictvím aplikace ve smartphonu nebo tabletu.^[48]

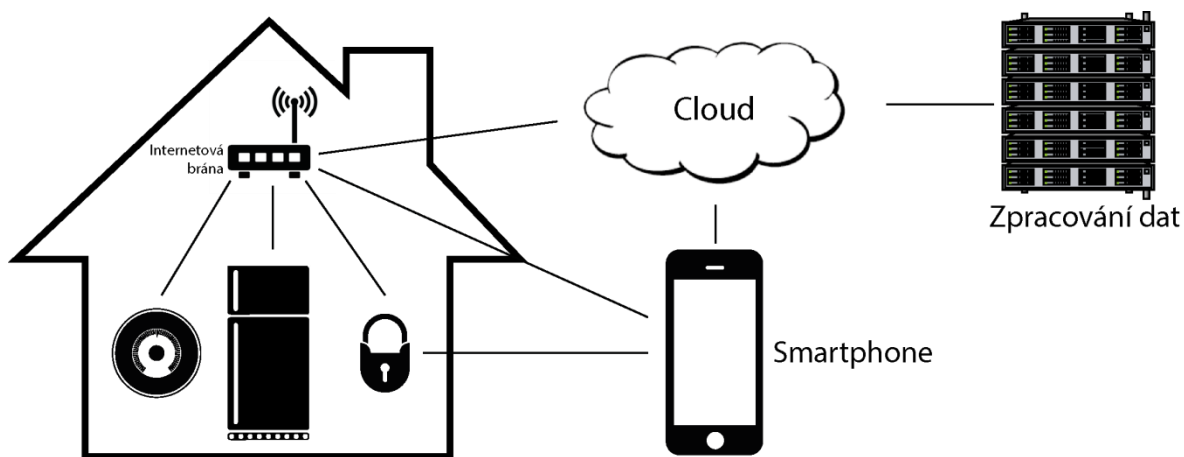


Schéma 4: Komunikace zařízení v chytré domácnosti

Zákazníci, kteří chtějí svou domácnost vybavit chytrými zařízeními mají na výběr ze tří možností:

1. Pořídí si samostatné chytré zařízení. U této varianty je třeba mít na paměti, že zařízení různých výrobců mohou být navzájem nekompatibilní a k jejich provozu jsou třeba různé aplikace, což může jejich použití značně zkomplikovat. Tato zařízení jsou určena pro širokou veřejnost a tak k instalaci i k používání nejsou třeba velké technické znalosti. Zákazníci si také mohou kupovat zařízení samostatně a nemusí utrácet velké finanční prostředky za komplexní řešení specializovaných firem.
2. Využijí služeb specializovaných firem, které jim kompletní řešení sestaví na míru. Tyto společnosti většinou využívají produkty vlastní značky a vlastního aplikačního ekosystému. Velkou výhodou této varianty je, že všechna zařízení se obsluhují prostřednictvím jedné aplikace a zákazníci mohou využívat zákaznické podpory. To s sebou samozřejmě nese vyšší pořizovací náklady a také velkou komplexnost celého systému. V tuzemsku k největším společnostem

zabývajících se chytrými domácnostmi patří Larx (využívá technologii Loxone), Ropreoso (využívá technologii Crestron) nebo Haidy (využívá vlastní technologii).

3. Sestaví si chytré zařízení sami. Tato varianta je vhodná zejména pro kutily a technické nadšence. Základem těchto zařízení jsou miniaturní počítače (respektive základní desky), které je možné prostřednictvím modulů dále rozšiřovat nebo k nim zařízení jednoduše připojit např. přes USB nebo Wi-Fi. Funkce zařízení si pak uživatel naprogramuje ve vývojovém prostředí. Nejrozšířenějšími zařízeními jsou Raspberry Pi, Arduino a Intel Galileo.



Obrázek 1: Raspberry Pi, Arduino a Intel Galileo (zdroj: Wikipedie)

4.2 Chytrá zařízení pro domácnosti

Oblast použití	Chytré zařízení
Prostředí	Osvětlení, monitoring vzduchu, vysavače, termostaty.
Elektroinstalace	Zásuvky, centrální jednotky.
Zabezpečení	Kamery, senzory, zámky, zvonky.
Multimédia	Televize.
Kuchyň	Prakticky všechny elektrospotřebiče.
Koupelna	Pračka, baterie/sprchové hlavice.
Zahrada	Péče o rostliny, sekačky trávy.
Ostatní	Péče o domácí mazlíčky.

Tabulka 6: Přehled použití chytrých zařízení v domácnosti

4.2.1 Prostředí

Osvětlení

Chytrá světla jsou určena především ke zvýšení energetické efektivity a pohodlí uživatele. Využívají technologii LED (Light Emitting Diode) a dokáží se rozsvěcovat a zhasínat v závislosti na prostředí, času nebo i přítomnosti uživatele. Ten pak může měnit intenzitu světla, u některých modelů i jeho barvu a také si vytvářet profily. Patří sem například Philips Hue, LIFX nebo GE Link Smart LED.^[49]



Obrázek 2: Philips Hue^[49]

Monitoring vzduchu

Zařízení spadající do této kategorie provádí rozbor částic a těkavých organických látek ve vzduchu a na základě těchto dat pak vyhodnocují kvalitu vzduchu. Mohou být vybaveny i detektorem kouře, mohou měřit teplotu, vlhkost nebo obsah oxid uhličitý. Zástupci této kategorie jsou například Awair, Birdi nebo Cube Sensors.^[50]



Obrázek 3: Cube Sensors^[51]

Vysavače

Funkcí chytrých vysavačů je autonomní nebo vzdáleně řízené vysávání podlah. První model pod názvem Trilobite byl představen už v roce 1997. Vysavače se orientují díky senzorům, které sledují celé jeho okolí a mohou se tak vyhýbat překážkám nebo rozpoznat už vysáté prostory. Dnes chytrým vysavačům vévodí model Roomba od společnosti iRobot, který se stal téměř synonymem pro celý segment. Dalšími zástupci jsou produkty společnosti Neato nebo Infinuvo.^[52]



Obrázek 4: Roomba 980^[52]

Termostaty

Chytré termostaty jsou stejně jako klasické termostaty určené ke kontrolování teploty a úspoře energií. Oproti těm klasickým se však dokáží učit návykům uživatele – kdy vstává, kdy chodí spát, jakou má v určitém ročním období oblíbenou teplotu, kdy není doma a kdy se bude vracet – a na základě těchto dat dokáží samy regulovat teplotu. Jedním z prvních a zároveň jedním z nejpoblárnějších chytrých termostatů je Nest. Dalšími produkty v této kategorii jsou Ecobee nebo termostat od společnosti Honeywell.^[53]



Obrázek 5: Nest^[53]

4.2.2 Elektroinstalace

Zásuvky

Chytrá zásuvka je zařízení, které se zapojuje přímo do klasické zásuvky a sama funguje jako zásuvka, takže v podstatě jde o rozšíření klasické zásuvky. Spotřebiče se do chytré zásuvky připojují úplně stejně, jako do klasické. Jejich výhodou je, že mohou být vzdáleně ovládané, dokáží monitorovat spotřebu a některé jsou i programovatelné, takže se mohou zapínat či vypínat v určitou dobu nebo na základě určitých událostí. Zástupci této kategorie jsou Belkin WeMo Insight Switch, SmartThings SmartPower Outlet nebo Aeon Labs Smart Energy Switch.^[54]

Nedávno se objevila chytrá zásuvka ResetPlug, která je navržena speciálně pro routery. ResetPlug dokáže monitorovat internetové připojení a v případě poruchy sama router restartuje.^[55]



Obrázek 6: ResetPlug^[55]

Centrální jednotky

Centrální jednotky nebo huby se používají k centralizovanému ovládnání a programování chytrých zařízení. Díky tomu není třeba 10 různých aplikací pro 10 různých zařízení, ale pouze jedna. Při nákupu centrální jednotky je třeba mít na paměti, že ne všechna zařízení jsou kompatibilní s hubem dané značky, i když kompatibilita mezi produkty na trhu je na velmi dobré úrovni. Patří sem například SmartThings Hub, Staples Connect nebo Quirky Wink.^[56]



Obrázek 7: SmartThings Hub^[56]

4.2.3 Zabezpečení

Kamery

Chytré kamery umožňují uživatelům vzdáleně monitorovat prostory a to prostřednictvím živého nebo nahraného videozáznamu. Některé modely jsou vybaveny alarmem nebo mohou uživateli zaslat upozornění na pohyb, některé nabízejí obousměrný zvukový přenos a některé jsou určené pro monitorování dětí (tzv. chůvičky). Tuto kategorii reprezentují produkty D-Link HD Wireless N Day/Night Outdoor Cloud Camera, Icontrol Networks Piper NV nebo Nest Cam.^[57]



Obrázek 8: Icontrol Networks Piper NV^[57]

Senzory

Nejen že chytré senzory dokáží o svém stavu vzdáleně informovat, ale mohou i posílat upozornění při změně stavu, při překročení určité hodnoty nebo při určitých událostech (například systém může poslat uživateli upozornění o otevřeném okně při odchodu z domova). Chytré senzory můžeme použít na oknech a na dveřích (např. SmartThings Multi Sensor) nebo jako detektory pohybu (např. SmartThings Motion Sensor).^[58]



Obrázek 9: SmartThings Multi Sensor^[58]

Zámky

Chytré zámky jsou v současnosti jedním z nejpoblíbenějších chytrých zařízení. Odemknutí je možné na dálku prostřednictvím internetu, zadáním PINu nebo smartphonem (nejčastěji se využívá technologie NFC⁷). Všechny tyto varianty mohou být doplněny i o možnost odemknout zámek klasickým klíčem. Chytré zámky dokáží monitorovat stav zámku, informovat vlastníka o otevření či o pokusu o neoprávněný přístup a samozřejmě dokáží i spustit alarm. Mezi nejoblíbenější modely patří Kwikset Kevo Smart Lock, August Smart Lock nebo Schlage Connect Touchscreen Deadbolt.^[60]



Obrázek 10: Kwikset Kevo Smart Lock^[60]

Zvonky

Kombinací klasického zvonku, kamery a reproduktoru vznikly chytré zvonky. Díky konektivě dokáží posílat upozornění o zazvonění vlastníkovi, který může s dotyčnou osobou komunikovat prostřednictvím kamery, reproduktoru a mikrofonu zabudovaném ve zvonku. Vlastníkovi k tomu stačí jen jeho smartphone, takže může s návštěvníkem mluvit prakticky odkudkoli. Některé modely jsou vybaveny i senzorem pohybu nebo dokáží rozpoznat pravidelné návštěvníky. Zástupci této kategorie jsou například Doorbot, SkyBell WiFi nebo Chui.^[61]



Obrázek 11: Doorbot^[61]

⁷ Near Field Communication (NFC) je bezdrátová technologie přenosu dat na krátkou vzdálenost (několik cm). U smartphonů se používá například k platbám (podobně jako u bezkontaktních platebních karet) nebo k identifikaci.^[59]

4.2.4 Multimédia

Televize

Chytrá televize je vylepšením klasické televize o připojení k internetu. Díky tomu je možné sledovat tzv. video na vyžádání, které umožňuje uživatelům sledovat video dle vlastního výběru bez předepsaného televizního programu. Tento systém si získává čím dál větší popularitu a nabízí ho například Amazon, Netflix nebo Hulu. Mimo to je možné sledovat i další weby s video obsahem jako je YouTube nebo Stream.cz, stejně tak je možné procházet internetové stránky nebo používat aplikace. Klasické televizní kanály mohou prostřednictvím chytrých televizí nabízet další obsah, jako videoarchiv, widgety na obrazovku, apod. V tuzemsku tuto funkci nabízí například Česká televize nebo Prima Cool.^[62]

Nabídka na trhu chytrých televizí je velmi široká. Mezi největší výrobce patří Samsung, LG nebo Panasonic. Stejně tak existuje mnoho platform. Samsung používá Smart Hub a Tizen OS, LG pracuje na platformě WebOS a Panasonic používá Firefox OS.^[63]



Obrázek 12: Chytrá televize LG^[63]

4.2.5 Kuchyně

Chytrá zařízení najdou v kuchyni využití ve všech elektronických (ale i v některých neelektronických) zařízeních. Od chytrých ledniček, které dokáží identifikovat uložené potraviny, hlídat jejich datum spotřeby nebo navrhnout recepty podle inventáře, přes chytré kávovary, pánvičky, trouby až k chytrým talířům. Vybraná zařízení a jejich funkce jsou shrnuty v následující tabulce.^[64]

Typ zařízení	Model	Funkce
Lednice	LG Smart ThinQ LFX31995ST	Nastavení různých teplot, LCD obrazovka, monitoring spotřeby a inventáře, správa nákupních seznamů.
Pánvička	Pantelligent Smart Frying Pan	Monitoring teploty, instrukce ke smažení.
Trouba	LG Smart ThinQ cooker	Vzdálený přístup, pečicí programy, samočistící systém.
Váha	Orange Chef Countertop	Výpočet nutričních hodnot potravin, sledování stravovacích návyků.
Kávovar	Siemens Coffee Maker	Vzdálený přístup, automatická příprava různých druhů kávy.
Talíř	SmartPlate	Sledování stravovacích návyků.
Vidlička	HAPIfork	
Myčka	Whirlpool Gold	Rozpoznání počtu a špinavosti nádobí, vzdálený přístup, ruční zaměření velmi špinavého nádobí.

Tabulka 7: Chytrá zařízení pro použití v kuchyni^{[64] [65] [65]}

4.2.6 Koupelna

Pračky

Hlavními přednostmi chytrých praček jsou monitoring spotřeby energií, vzdálený přístup nebo informace o stavu praní přímo ve smartphonu. Letos se dokonce objevila pračka Smart Top Load od společnosti Whirlpool, která sleduje stav čisticích prostředků a pokud docházejí, dokáže je sama objednat v internetovém obchodě Amazon. Produkci chytrých praček se zabývá i společnost LG se svým modelem Twin Wash nebo Samsung s modelem F900.^{[66] [67] [68]}



Obrázek 13: Samsung F900^[68]

Baterie/sprchové hlavice

Primárním úkolem chytrých baterií a sprchových hlavice je šetřit vodu a finanční prostředky spojené s její spotřebou. Toho tato zařízení dosahují možností zadat požadovanou teplotu vody pomocí dotykové obrazovky (odpadá tak nutnost míchání studené a teplé vody, při čemž se zbytečně spotřebovává voda) jako tomu je u baterie Nomos nebo zvýšením efektivnosti průtoku vody. Chytré sprchové hlavice jdou v tomto směru ještě dál – jako například Hydrao, které hlídá spotřebu vody při každém sprchování a podává o něm uživateli informace prostřednictvím LED diod umístěných v hlavici.^{[69] [70]}



Obrázek 14: Hydrao^[70]

4.2.7 Zahrada

Péče o rostliny

Chytrá zařízení najdou uplatnění i na zahradě. Mohou monitorovat půdu, sluneční svit a teplotu jako Koubachi Wi-Fi Plant Sensor, zjistit ideální rostliny pro výsadbu v dané oblasti jako EasyBloom Plant Sensor, vzdáleně se postarat o zavlažování jako WaterPoint nebo se starat o hydroponické pěstování jako Indoor Garden. Dalším oblíbeným zařízením jsou chytré rozprašovače, které dokáží rozhodnout o zavlažování na základě předpovědi počasí a dat ze senzorů. Takovým zařízením je Blossom Smart Watering Controller.^{[71][72]}



Obrázek 15: Indoor Garden^[71]

Sekačky trávy

Úkolem chytrých sekaček je autonomní sekání trávy. Většina modelů spolupracuje s metalickým vodičem, kterým uživatel ohraničí pracovní prostor. Uživatel potom může nastavit trasu pohybu nebo se sekačka pohybuje náhodně. Aby se vyhnuly překážkám, jsou vybaveny senzory, které sledují okolí přístroje. Sekačky dokáží samy vyložit posekanou trávu na určité místo a pokud jim dochází baterie, tak se samy přesunou k dobíjecí stanici a po nabití pokračují v práci. Některé modely umí vzdáleně informovat uživatele o průběhu sekání a v případě problému ho upozornit. Mezi chytré sekačky patří například Honda Miimo, Husqvarna Automower nebo John Deere Tango.^[73]



Obrázek 16: Husqvarna Automower^[73]

4.2.8 Ostatní

Péče o domácí mazlíčky

V oblasti péče o domácí mazlíčky existují dva typy chytrých zařízení – zvířecí chůvičky, které fungují stejně jako dětské chůvičky nebo chytrá krmítka, která mohou být aktivovaná na dálku nebo automaticky a některé modely dokáží i monitorovat zásobu krmení nebo nastavit velikost porce. Mezi tato zařízení patří například Hoison Smart Feeder nebo Petnet SmartFeeder. Existují také kombinace těchto zařízení, jako například PetChatz HD Greet & Treat Camera^{[74] [75]}



Obrázek 17: PetChatz HD Greet & Treat Camera^[75]

II. PRAKTICKÁ ČÁST

5 VÝVOJOVÉ DESKY PRO VÝUKU MIKROPOČÍTAČŮ

5.1 Desky Arduino

Open-sourcové desky Arduino, které se v Evropě prodávají pod názvem Genuino jsou určeny pro výuku v oblasti mikropočítačů. Tyto desky nabízí široké spektrum rozšiřujících modulů (tzv. shieldů). Ty je možné snadno připojit do vstupně-výstupních pinů. Hardware je navíc vybaven multiplatformním vývojovým prostředím Arduino Integrated development environment (IDE). Produkty Arduino vynikají také nízkou cenou a velkou uživatelskou komunitou.^{[76][77]}

Arduino v současné době nabízí základní desky ve 4 kategoriích:^[78]

1. Entry level – desky určené pro začátečníky.
2. Enhanced features – řada pro pokročilé vývojáře, jsou vybaveny výkonnějším hardwarem a pokročilými funkcemi.
3. IoT – řada určená speciálně pro použití v chytrých zařízeních. Předností produktů této kategorie je integrované síťové připojení (Wi-Fi a Ethernet), předinstalovaná Linuxová distribuce a malé rozměry.
4. Wearable – speciální miniaturní desky, které jsou určené pro nositelná chytrá zařízení.

5.1.1 Entry Level

Arduino Uno

Uno je nejpoužívanější a nejlépe zdokumentovanou deskou společnosti Arduino. Díky své robustnosti je ideálním produktem pro začátečníky. Deska je vybavena mikrokontrolérem Atmega328P, USB a napájecím konektorem, ICSP⁸ headerem a resetovacím tlačítkem.^[78]



Obrázek 18: Arduino a Genuino Uno^[78]

Arduino 101

Desky Arduino 101 v sobě kombinují robustnost desek Uno s nejnovejšími technologiemi. Jsou vybaveny modulem Intel Curie a dvoujádrovým procesorem. Oproti Unu jsou desky 101 ještě navíc vybaveny akcelerometrem, gyroskopem, pohybovým senzorem a Bluetooth LE konektivitou. Ostatní parametry jsou shodné.^[78]



Obrázek 19: Arduino a Genuino 101^[78]

⁸ In-Circuit Serial Programming (ICSP) je schopnost čipů, díky které je možné je naprogramovat přímo uvnitř obvodu.^[80]

Arduino Pro

Za vývojem desky Pro stojí společnost SparkFun Electronics a je dostupná ve dvou verzích: První je vybavená mikrokontrolérem ATmega168, který pracuje na frekvenci 9 MHz a díky provoznímu napětí 3,3 V může být napájena z baterie. Druhá, výkonnější verze je postavena na jádru ATmega328 s pracovní frekvencí 16 MHz. Ke svému provozu však potřebuje napětí 5 V. Oba mikrokontroléry podporují UART⁹ komunikaci.^[78]

Deska je dále vybavena jackem pro připojení baterie, vypínacím přepínačem, tlačítkem pro reset, otvory pro připojení napájecího kabelu a ICSP header. Ke komunikaci s deskou je potřeba FTDI¹⁰ kabel nebo modul Sparkfun breakout board.^[78]

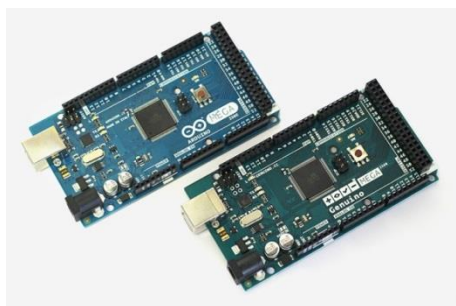


Obrázek 20: Arduino Pro^[78]

5.1.2 Enhanced features

Arduino Mega 2560

Desky Arduino Mega 2560 jsou díky velkému počtu pinů určeny pro komplexnější projekty jako jsou 3D tiskárny nebo roboti. Na rozdíl od Uno jsou desky vybaveny mikrokontrolérem ATmega2560 a mají navíc 4 UART porty.^[78]



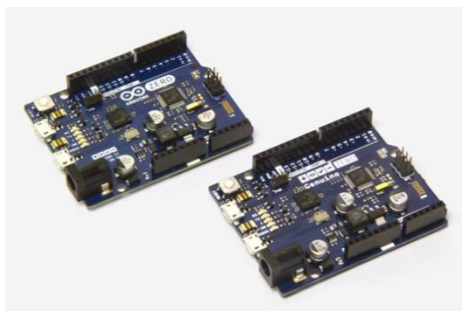
Obrázek 21: Arduino a Genuino Mega 2560^[78]

⁹ Universal asynchronous receiver/transmitter (UART) je hardwarové zařízení, které převádí data mezi paralelní a sériovou komunikací.^[81]

¹⁰ Kabely FTDI vyráběné stejnojmennou společností převádí sériovou komunikaci na USB signály.^[82]

Arduino Zero

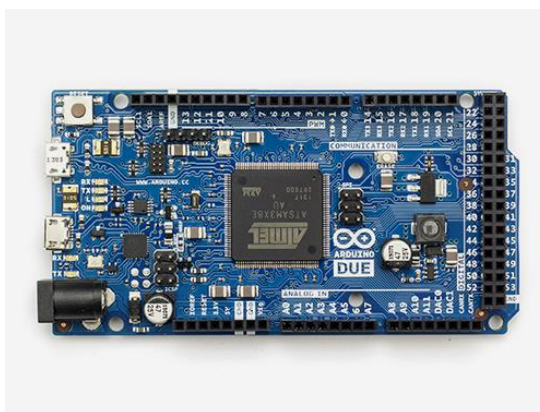
Zero je vylepšením desky Uno. Nabízí podstatně větší výkon, za kterým stojí mikrokontrolér SAMD21 MCU založený na ARM architektuře. Jednou z hlavních předností Zera je integrovaný debugger od společnosti Atmel, který poskytuje plné rozhraní pro debugování bez potřeby přídavného hardwaru. Oproti Unu je Zero vybaveno micro USB konektorem a dvěma UART porty. Ostatní vybavení zůstalo stejné.^[78]



Obrázek 22: Arduino a Genuino Zero^[78]

Arduino Due

Due je nejvýkonnější deskou v nabídce společnosti Arduino a je vhodná pro velké a výkonné projekty. Je vybavena mikrokontrolérem AT91SAM3X8E, který je stejně jako u desky Zero založen na architektuře ARM. Na rozdíl od Una je deska Due navíc vybavena dvěma USB konektory, tlačítkem pro vymazání Flash paměti, čtyřmi UART porty, headery SPI¹¹ a JTAG¹² a velkým počtem pinů.^[78]



Obrázek 23: Arduino Due^[78]

¹¹ Serial Peripheral Interface (SPI) je komunikační rozhraní používané k výměně dat mezi mikrokontrolérem a perifériemi.^[83]

¹² JTAG je technologie, určená k diagnostice tištěných spojů a zařízení na desce.^[84]

5.1.3 IoT

Arduino Yún

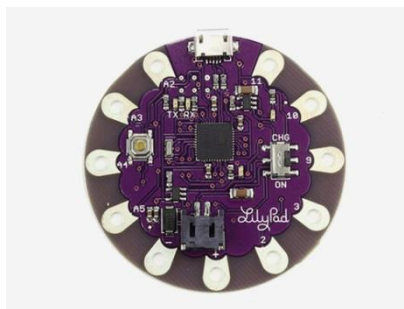
Yún byla navržena speciálně pro projekty IoT. Deska je osazena mikrokontroléry ATmega32u4 a Atheros AR9331 s podporou Linuxové distribuce OpenWrt-Yun. Na desce jsou zabudované konektory Ethernet, Micro USB, USB, slot pro Micro SD karty a Wi-Fi modul zajišťující konektivitu.^[78]



Obrázek 24: Arduino Yún^[78]

5.1.4 Wearable

Řada Wearable byla vyvinuta pro použití v nositelných projektech a je možné je přišít přímo na textil. Všechny desky jsou vybaveny USB připojením, resetovacím tlačítkem a po vyjmutí zdroje el. energie i omyvatelné ve studené vodě (kromě desky SimpleSnap, která má integrovanou baterii). Do této kategorie se řadí modely Gemma, LilyPad USB, LilyPad Main Board, LilyPad Simple a LilyPad SimpleSnap. O provoz desek se starají mikrokontroléry ATtiny85 (Gemma), ATmega32u4 (LilyPad USB) a ATmega328V (ostatní modely).^[78]



Obrázek 25: LilyPad Arduino USB^[78]

Typ	Provozní napětí [V]	Flash paměť [KB]	SRAM [KB]	EEPROM [KB]	Frekvence [MHz]	Digitální I/O piny	Analogové I/O piny	PWM ¹³ piny
Uno	5	32	2	1	16	14	6	6
101	3,3/5	196	24	-	32	14	6	4
Pro	3,3/5	16/32	1	0,515/1	8/16	14	6	6
Mega 2560	5	256	8	4	16	54	16	15
Zero	3,3	256	32	-	48	20	6/1	5
Due	3,3	512	96	-	84	54	12/2	12
Yún	5	32	2,5	1	16	20	12/0	7
Gemma	3,3	8	0,512	0,512	8	3	1/0	2
LilyPad Simple	2,7/5,5	32	2	1	8	9	4/0	5
LilyPad Main Board	2,7/5,5	16	1	0,512	8	14	6/0	6
LilyPad USB	3,3	32	2,5	1	8	9	4/0	4
LilyPad Simple Snap	2,7/5,5	32	2	1	8	9	4/0	5

Tabulka 8: Srovnání vybraných parametrů desek Arduino^[78]

¹³ Pulse-width Modulation (PWM) je technika získávání analogových výstupů pomocí digitálních prostředků. Digitální ovládání vytváří obdelníkový signál, tedy zapínací a vypínací signály. Mezisignály jsou simulovány podle různého trvání impulsu.^[79]

5.1.5 Shieldy

Shieldy jsou speciální moduly, které se dají jednoduše připojit do pinů desek Arduino a rozšířit tak jeho funkce. Podle dat společnosti Arduino je v současné době na trhu 317 shieldů od 125 výrobců. Největším výrobcem shieldů je společnost Sparkfun, která se podílí i na vývoji desek Arduino. Funkce shieldů jsou téměř neomezené: od síťových modulů, přes LCD obrazovky, klávesnice, solární panely, kamery až po pohony motorků.^[83]



Obrázek 26: GPRS shield od společnosti Seed Studio^[83]

5.2 Desky Intel

Pro výuku mikropočítačů jsou vhodné i desky od společnosti Intel, které jsou certifikované společností Arduino a jsou tak hardwarově i softwarově kompatibilní s shieldy pro tuto platformu. Desky jsou prodávány pod názvem Galileo a v současnosti existují dvě generace, které oproti Arduino nabízí podstatně vyšší výkon.^[84]

Intel Galileo Gen. 1

První generace desek Galileo je poháněna mikrokontrolérem Intel Quark SoC X1000 a jedná se o první desku na platformě Arduino, která podporuje připojení karet mini-PCI Express. Další je deska vybavena konektory pro Ethernet, USB, RS-232 konektorem pro sériovou komunikaci, slotem pro Micro-SD karty, restartovacími tlačítky, headery ICSP a JTAG a UART piny.^[85]



Obrázek 27: Intel Galileo Gen 1^[85]

Intel Galileo Gen 2

Oproti první generaci přibyla podpora napájení desky z baterie a konektor Ethernetu byl vylepšen o technologii Power Over Ethernet, díky které může být deska napájena přímo z Ethernetového kabelu.^{[86] [87]}



Obrázek 28: Intel Galileo Gen 2^[86]

Typ	Provozní napětí [V]	RAM [MB]	SRAM [KB]	EEPROM [KB]	Frekvence [MHz]	Digitální I/O piny	Analogové I/O piny	PWM piny
Gen 1	5	Až 256	512 + 256MB DRAM	11	400	14	6/0	6
Gen 2	3,3/5	Až 256	512	8	400	14	6/0	6

Tabulka 9: Srovnání vybraných parametrů desek Intel^{[85] [86]}

6 VÝVOJOVÉ DESKY PRO VÝUKU PROGRAMOVÁNÍ

6.1 Raspberry Pi

Raspberry Pi je řada jednodeskových počítačů, které byly vyvinuty stejnojmennou nadací pro výuku počítačových věd. Desky jsou poháněny procesory architektury ARM a grafickými kartami od společnosti Broadcom. Standardně pracují na operačním systému Linux. Doporučeným programovacím jazykem je Python, ale je možné použít většinu populárních programovacích jazyků, jako např. C, C++, Java nebo Ruby. Externí zařízení je možné připojit přes USB, HDMI nebo GPIO¹⁴ piny. U všech modelů kromě Raspberry Pi Zero je také možné využít připojení CSI nebo DSI.^[88]

Raspberry Pi 1

První generace Raspberry Pi se v současnosti prodává ve dvou variantách A+ a B+. Obě varianty jsou vylepšením původních verzí, které byly značeny bez plusů a nyní už se nevyrábí. Rozdíly mezi modely jsou zejména v konektorech a konektivitě: model A+ má pouze jeden USB konektor, zatímco model B+ má čtyři USB konektory a jeden konektor pro Ethernet. Desky jsou shodně poháněny procesorem ARM1176JZF-S a jsou napájeny z micro USB konektoru. Dále jsou vybaveny čtyřiceti GPIO piny, 3,5mm jackem pro audio výstup, HDMI konektorem, slotem pro micro SD karty, CSI slotem pro připojení kamery a DSI slotem pro výstup videa.^{[89] [90]}



Obrázek 29: Raspberry Pi 1 Model B+ ^[90]

¹⁴ General-purpose input/output (GPIO) jsou vstupně-výstupní programovatelné piny. ^[91]

Raspberry Pi 2 Model B

Druhá generace s sebou přinesla zvýšení výkonu v podobě dvojnásobného zvětšení RAM paměti a nového čtyřjádrového 32 bitového procesoru ARM Cortex-A7 CPU. Díky novému procesoru může Raspberry Pi 2 spustit většinu ARM linuxových distribucí nebo Windows 10. Deska je zpětně kompatibilní s první generací.^[92]

Raspberry Pi 3 Model B

Stejně jako druhá generace přinesla i ta třetí nový 64 bitový procesor ARM Cortex-A53 se čtyřmi jádry. Přibyly i nové možnosti konektivity prostřednictvím integrovaného Wi-Fi, Bluetooth a Bluetooth LE připojení. Deska je zpětně kompatibilní s předchozími generacemi.^[93]

Raspberry Pi Zero

Raspberry Pi Zero je nejlevnějším a zároveň nejmenším modelem z celého portfolia. Deska je vybavena vylepšeným procesorem ARM1176JZF-S, kterému oproti první generaci narostl výkon o 40%. Kvůli úspoře místa musely být zmenšeny a odstraněny některé konektory. Model Zero je tak vybaven dvěma micro-USB a mini-HDMI konektorem, slotem na micro-SD karty, čtyřiceti GPIO zásuvkami a zásuvkou na kompozitní video.^[94]



Obrázek 30: Raspberry Pi Zero^[95]

Typ	Provozní napětí	CPU	GPU	SDRAM	GPIO piny
Model 1 A+	5 V	700 Mhz	250 MHz	512 MB	40
Model 1 B+				900 MHz	
Model 2 B		1,2 GHz			
Model 3 B		1 GHz	250 MHz	512 MB	
Zero					

Tabulka 10: Srovnání vybraných parametrů desek Raspberry^{[89] [90] [92] [93] [94]}

6.2 Gizmosphere

Gizmosphere stejně jako Raspberry Pi je jednodeskový a open-sourcový počítač vyráběný společností AMD. Oproti Raspberry Pi nabízí vyšší výkon, ovšem je téměř 4x dražší.^[96]

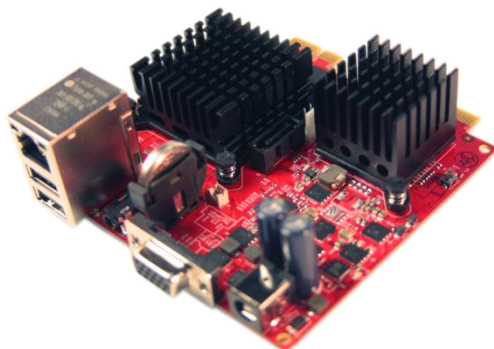
Gizmo 1

První generace se prodává v tzv. Explorer kitu, který obsahuje:^[97]

- Desku Gizmo 1
- Desku Explorer – rozšiřovací I/O deska pro Gizmo 1, která obsahuje alfanumerickou klávesnici, micro displej a zásuvky pro připojení externích zařízení.
- Vývojový nástroj Sage SmartProbe JTAG – umožňuje programování a debugování všech komponentů na desce. Bezplatná doba použití softwaru je 20 hodin.
- Grafické vývojové prostředí Sage EDK – třicetidenní bezplatná verze vývojového a debugovacího prostředí určeného pro práci se softwarem.
- SageBIOS – předinstalovaný open source BIOS, který mimojiné nabízí stejné chování jako BIOS u tradičních počítačů.
- Flash disk s linuxovou distribucí SLAX a s dokumentací.
- Ethernet a USB kabely, napájecí zdroj a návod.

Deska Gizmo 1 je vybavena dvoujádrovým procesorem AMD Embedded G-Series G-T40E APU a integrovanou grafickou kartou Radeon HD 6250. Dále je vybavena konektorem pro Ethernet, SATA a VGA, dvěma konektory USB (a dalšími pěti

rozhraními) a čtyřmi konektory pro zvuk. Mimo to je karta na hraně vybavena vysoko a nízko rychlostními konektory, ke kterým je možné připojit speciální rozšiřující karty. Tyto karty mohou obsahovat konektory jako například PCIe, SATA nebo piny GPIO a PWM.^[98]

Obrázek 31: Gizmo 1^[98]

Gizmo 2

Druhá generace je vybavena novou grafickou kartou Radeon HD 8210E a procesorem AMD Embedded G-Series SoC - GX210HA složeným ze dvou jader Jaguar, která jsou založena na stejné architektuře, jaká je používaná na herních konzolách. Dále byl nahrazen VGA port HDMI portem, byl přidán mSATA port pro připojení SSD disků, slot pro MicroSD karty a osm GPIO pinů.^[99]

Obrázek 32: Gizmo 2^[99]

Typ	CPU	GPU	RAM
Gizmo 1	1 GHz	280 MHz	1GB
Gizmo 2		300 MHz	

Tabulka 11: Porovnání vybraných parametrů desek Gizmosphere^[99]

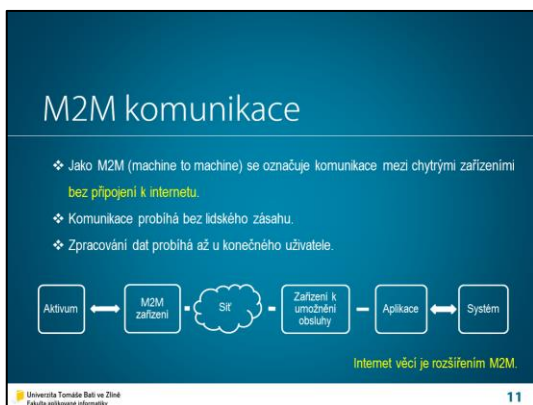
7 VÝUKOVÁ PREZENTACE

Součástí praktické části je i výuková prezentace. Prezentace shrnuje všechny informace uvedené v této bakalářské práci.

Osnova prezentace:

1. Internet věcí – v této kapitole se posluchači dozví, co se skrývá pod pojmy Internet věcí a chytré zařízení, kde všude najde IoT uplatnění a jaká je situace na tuzemském i globálním trhu.
2. Síťová komunikace v Internetu věcí – tato část představuje nové, ale i už zavedené komunikační technologie, na kterých pracují chytrá zařízení v IoT. Jedná se o technologie M2M, TCP/IP, IPv6, RPL, UDP, IEEE 802.15.4, mobilní datové sítě, Wi-Fi, CoAP.
3. Rizika Internetu věcí – tato kapitola seznamuje posluchače s riziky spojené s používáním chytrých zařízení a nabízí možná řešení.
4. Aplikace Internetu věcí v domácnostech – tato část obsahuje přehled chytrých zařízení pro domácnost a jejich funkce.

Screenshots prezentace:



ZÁVĚR

V teoretické části byl objasněn pojem Internetu věcí včetně jeho vzniku a současné i budoucí, předpokládané situaci na trhu.

V kapitole o komunikačních technologiích byly rozebrány nové i tradiční síťové technologie, na kterých chytrá zařízení pracují. Díky tomu, že se jedná o velké množství malých a výkonově omezených zařízení, bylo nutné některé současné komunikační technologie upravit tak, aby vyhovovaly nárokům na nízkou spotřebu a nízký výpočetní výkon.

Popsaná rizika spojená s používáním chytrých zařízení ukazují, že otázka bezpečnosti je často mezi výrobci opomíjenou záležitostí, která je zanedbávána na úkor nižší ceny produktů nebo rychlejšího uvedení na trh. Je nutné, aby výrobci k této problematice přistupovali s daleko větší zodpovědností, protože chytrá zařízení shromažďují velké množství osobních dat, která mohou být lehce zneužita. Zodpovědnost však neleží pouze na výrobcích, ale i na samotných uživatelích. Ti musí být řádně seznámeni se všemi riziky a s možnostmi, jak svá zařízení ochránit. Musí také mít možnost kontroly nad daty, která o nich chytrá zařízení shromažďují.

Z přehledu využití Internetu věcí v domácnosti je patrné, že chytrá zařízení, která jsou teprve na počátku svého vývoje už teď najdou uplatnění v mnoha oblastech lidského života.

V praktické části byl sestaven přehled vývojových desek, které jsou vhodné pro výuku studentů v oblasti Internetu věcí. Pro studium mikropočítačů jsou vhodné zejména desky Arduino, které nabízejí širokou uživatelskou základnu, nízkou cenu a velké množství rozšiřujících modulů. To vše je možné ovládat z multiplatformního vývojového prostředí. Pro výuku programování se hodí desky Raspberry Pi. Ty stejně jako mikropočítačové desky Arduino vynikají velkou uživatelskou základnou, nízkou cenou a možností připojení konvenčních zařízení.

Výuková prezentace shrnula všechny informace obsažené v této bakalářské prezentaci a poslouží studentům ke studiu Internetu věcí.

SEZNAM POUŽITÉ LITERATURY

- [1] DHANJANI, Nitesh. *Abusing the Internet of Things*. Sebastopol: O'Reilly Media, Inc., 2010. ISBN 063-6-920-03354-7.
- [2] HÖLLER, Jan. *From machine-to-machine to the Internet of things: introduction to a new age of intelligence*. Amsterdam: Elsevier Academic Press, 2014. ISBN 9780080994017.
- [3] KUROSE, James F. a Keith W. ROSS. *Počítačové sítě*. Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.
- [4] VASSEUR, Jean-Philippe. a Adam. DUNKELS. *Interconnecting smart objects with IP: the next Internet*. Burlington, MA: Morgan Kaufmann Publishers/Elsevier, c2010. ISBN 0123751659.
- [5] VERMESAN, Dr. Ovidiu a Dr. Peter FRIESS. *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*. Aalborg: River Publishers, 2013. ISBN 978-87-92982-73-5.
- [6] Internet of Things (IoT). *Techopedia* [online]. 2016 [cit. 2016-05-01]. Dostupné z: <https://www.techopedia.com/definition/28247/internet-of-things-iot>
- [7] ASHTON, Kevin. That 'Internet of Things' Thing. *RFID Journal* [online]. 2009 [cit. 2016-05-01]. Dostupné z: <http://www.rfidjournal.com/articles/view?4986>
- [8] Micro-electromechanical systems (MEMS). *IoT Agenda* [online]. Newton, 2016 [cit. 2016-05-01]. Dostupné z: <http://internetofthingsagenda.techtarget.com/definition/micro-electromechanical-systems-MEMS>
- [9] CMU SCS Coke Machine. *Carnegie Mellon University* [online]. Pittsburgh, 2005 [cit. 2016-05-01]. Dostupné z: <http://www.cs.cmu.edu/~coke/>
- [10] ČERNÝ, Michal. Zvířata on-line. *Respekt*. 2016, 27(5). ISSN 0862-6545.
- [11] LUETH, Knud Lasse. IoT market analysis: Sizing the opportunity. *IoT Analytics* [online]. 2015 [cit. 2016-05-03]. Dostupné z: <http://iot-analytics.com/wp/wp-content/uploads/2015/03/2015-March-Whitepaper-IoT-Market-analysis-Sizing-the-opportunity.pdf>
- [12] ČUCHNA, Matěj. IDC: Digitální transformace míří do podniků, český trh IoT poroste o pětinu ročně. *ChanellWorld* [online]. 2016 [cit. 2016-05-04]. Dostupné

- z: <http://channelworld.cz/analyzy/idc-digitalni-transformace-miri-do-podniku-cesky-trh-iot-poroste-o-petinu-rocne-15760>
- [13] VICHEREK, Jiří. Seznam českých startupů, které řeší Internet of Things!. *Startitup.cz* [online]. 2016 [cit. 2016-05-03]. Dostupné z: <http://startitup.cz/seznam-ceskych-startupu-ktere-resi-internet-of-things/>
- [14] Transmission Control Protocol (TCP). *Techopedia.com* [online]. 2016 [cit. 2016-05-04]. Dostupné z: <https://www.techopedia.com/definition/5773/transmission-control-protocol-tcp>
- [15] Internet Protocol (IP). *Techopedia.com* [online]. 2016 [cit. 2016-05-04]. Dostupné z: <https://www.techopedia.com/definition/5366/internet-protocol-ip>
- [16] TCP/IP Networking Protocols. *The Computer Technology Documentation Project* [online]. 2016 [cit. 2016-05-04]. Dostupné z: <http://www.comptechdoc.org/independent/networking/protocol/protnet.html>
- [17] Open Systems Interconnection Model (OSI Model). *Techopedia.com* [online]. 2016 [cit. 2016-05-04]. Dostupné z: <https://www.techopedia.com/definition/24205/open-systems-interconnection-model-osi-model>
- [18] Vlastnosti protokolu. *IPv6.cz* [online]. 2016 [cit. 2016-05-04]. Dostupné z: https://www.ipv6.cz/Vlastnosti_protokolu
- [19] IPv4 Address Report. *Potaroo.net* [online]. 2016 [cit. 2016-05-04]. Dostupné z: <http://www.potaroo.net/tools/ipv4/index.html>
- [20] DEERING, S. a R. HINDEN. Internet Protocol, Version 6 (IPv6) Specification. *The Internet Engineering Task Force* [online]. 1998 [cit. 2016-05-04]. Dostupné z: <https://www.ietf.org/rfc/rfc2460.txt>
- [21] IPv6 Statistics. *Google.com* [online]. 2016 [cit. 2016-05-04]. Dostupné z: <https://www.google.com/intl/en/ipv6/statistics.html>
- [22] Distance Vector Routing Protocol (DVRP). *Techopedia.com* [online]. 2016 [cit. 2016-05-04]. Dostupné z: <https://www.techopedia.com/definition/26985/distance-vector-routing-protocol-dvrp>
- [23] Directed acyclic graph. *National Institute of Standards and Technology* [online]. 2004 [cit. 2016-05-04]. Dostupné z: <https://xlinux.nist.gov/dads//HTML/directAcycGraph.html>

- [24] KHAN, MUHAMMAD RASHID. Performance and route stability analysis of RPL protocol [online]. Stockholm, 2012 [cit. 2016-05-29]. Dostupné z: <http://www.diva-portal.org/smash/get/diva2:557323/FULLTEXT01.pdf>. Masters' Degree Project. KTH Electrical Engineering.
- [25] ABOUT. *IEEE 802.15* [online]. 2005 [cit. 2016-05-04]. Dostupné z: <http://www.ieee802.org/15/about.html>
- [26] IEEE 802.15 WPAN Task Group 4. *IEEE 802.15* [online]. 2005 [cit. 2016-05-04]. Dostupné z: <http://www.ieee802.org/15/pub/TG4.html>
- [27] Carrier Sense Multiple Access/with Collision Avoidance (CSMA/CA). *Techopedia.com* [online]. 2016 [cit. 2016-05-04]. Dostupné z: <https://www.techopedia.com/definition/11271/carrier-sense-multiple-access-with-collision-avoidance-csmaca>
- [28] Bluetooth core specification. *Bluetooth* [online]. 2016 [cit. 2016-05-07]. Dostupné z: <https://www.bluetooth.com/specifications/bluetooth-core-specification>
- [29] Low Energy. *Bluetooth* [online]. 2016 [cit. 2016-05-07]. Dostupné z: <https://www.bluetooth.com/what-is-bluetooth-technology/bluetooth-technology-basics/low-energy>
- [30] WISTAO. Comparison of Bluetooth Different Versions [online]. 2012 [cit. 2016-05-07]. Dostupné z: <http://wistao.blogspot.cz/2012/09/comparison-of-bluetooth-different.html>
- [31] WILLIAMS, Lee. 4G LTE Versus Wi-Fi Versus Bluetooth. *Remote Magazine* [online]. 2016 [cit. 2016-05-07]. Dostupné z: <http://www.remotemagazine.com/main/articles/4g-lte-versus-wi-fi-versus-bluetooth-what-every-aspiring-iot-entrepreneur-needs-to-know/>
- [32] RS COMPONENTS. 11 Internet of Things (IoT) Protocols You Need to Know About. *DesignSpark* [online]. 2015 [cit. 2016-05-07]. Dostupné z: <http://www.remotemagazine.com/main/articles/4g-lte-versus-wi-fi-versus-bluetooth-what-every-aspiring-iot-entrepreneur-needs-to-know/>
- [33] Definition of Wi-Fi. *PC Magazine* [online]. 2016 [cit. 2016-05-07]. Dostupné z: <http://www.pcmag.com/encyclopedia/term/54444/wi-fi>

- [34] Wi-Fi HaLow. *Wi-Fi Alliance* [online]. 2016 [cit. 2016-05-07]. Dostupné z: <http://www.wi-fi.org/discover-wi-fi/wi-fi-halow>
- [35] Ethernet. *Techopedia.com* [online]. 2016 [cit. 2016-05-07]. Dostupné z: <https://www.techopedia.com/definition/5280/ethernet>
- [36] RFC 7252 Constrained Application Protocol. *CoAP* [online]. 2016 [cit. 2016-05-07]. Dostupné z: <http://www.wi-fi.org/discover-wi-fi/wi-fi-halow>
- [37] VALERIO, Pablo. IoT Security: Industry Finally Waking Up To The Dangers. *Information Week* [online]. 2016 [cit. 2016-05-07]. Dostupné z: <http://www.informationweek.com/iot/iot-security-industry-finally-waking-up-to-the-dangers/a/d-id/1324529>
- [38] Sniffer. *Techopedia.com* [online]. 2016 [cit. 2016-05-07]. Dostupné z: <https://www.techopedia.com/definition/4113/sniffer>
- [39] Man-in-the-middle attack. *OWASP* [online]. 2015 [cit. 2016-05-07]. Dostupné z: https://www.owasp.org/index.php/Man-in-the-middle_attack
- [40] NAPEL, Mano Ten. Wearables and Quantified Self Demand Security-First Design. *Wired* [online]. 2014 [cit. 2016-05-07]. Dostupné z: <http://www.wired.com/insights/2014/10/wearables-security-first-design/>
- [41] PUBNUB. A New Approach to IoT Security. *PubNub.com* [online]. 2015 [cit. 2016-05-07]. Dostupné z: https://www.pubnub.com/static/papers/IoT_Security_Whitepaper_Final.pdf
- [42] GOLUBOFF, Mariano. AES vs SSL/TLS: Encryption for the internet of things. *Electronic Products Magazine* [online]. 2015 [cit. 2016-05-07]. Dostupné z: http://www.electronicproducts.com/Computer_Peripherals/Communication_Peripherals/AES_vs_SSL_TLS_Encryption_for_the_internet_of_things.aspx?id=113
- [43] WINDER, Davey. Top ten password cracking techniques. *Alphr* [online]. 2011 [cit. 2016-05-12]. Dostupné z: <http://www.alphr.com/features/371158/top-ten-password-cracking-techniques>
- [44] MS. SMITH. Peeping into 73,000 unsecured security cameras thanks to default passwords. *Network World* [online]. 2014 [cit. 2016-05-12]. Dostupné z: <http://www.networkworld.com/article/2844283/microsoft-subnet/peeping-into-73-000-unsecured-security-cameras-thanks-to-default-passwords.html>

- [45] ROBERTS, Paul. Enterprise IoT Risk Is Getting Real. *Qualys Blog* [online]. 2014 [cit. 2016-05-12]. Dostupné z: <https://blog.qualys.com/securitylabs/2014/10/17/enterprise-iot-risk-is-getting-real>
- [46] GREENBERG, Andy. Hackers Remotely Kill a Jeep on the Highway—With Me in It. *Wired* [online]. 2015 [cit. 2016-05-12]. Dostupné z: <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>
- [47] NIGHTINGALE, Rob. 7 Reasons Why The Internet of Things Should Scare You. *Makeuseof* [online]. 2015 [cit. 2016-05-12]. Dostupné z: <http://www.makeuseof.com/tag/7-reasons-the-internet-of-things-should-scare-you/>
- [48] What is a "Smart Home"? *Smart House Energy* [online]. 2016 [cit. 2016-05-14]. Dostupné z: <http://smarthomeenergy.co.uk/what-smart-home>
- [49] Smart lighting solutions: Here are seven options to choose from. *Pocket-lint* [online]. 2016 [cit. 2016-05-14]. Dostupné z: <http://www.pocket-lint.com/news/130002-smart-lighting-solutions-here-are-seven-options-to-choose-from>
- [50] Guide to Indoor Air Quality Monitoring Devices for the Healthy Home. *Energy Circle* [online]. 2016 [cit. 2016-05-14]. Dostupné z: <http://www.energycircle.com/guide/guide-indoor-air-quality-monitoring-devices-healthy-home>
- [51] CubeSensors1.png. *SciencePLX* [online]. 2016 [cit. 2016-05-14]. Dostupné z: <http://scienceplx.com/wp-content/uploads/2015/06/CubeSensors1.png>
- [52] E-MAN, Martin. What is the best Robot Vacuum? *Build Your Smart Home* [online]. 2015 [cit. 2016-05-14]. Dostupné z: <http://buildyoursmarthome.co/reviews/best-robot-vacuum/>
- [53] HENRY, Alan. Five Best Smart Thermostats. *Lifehacker* [online]. 2015 [cit. 2016-05-14]. Dostupné z: <http://lifehacker.com/five-best-smart-thermostats-1717145893>
- [54] LEE, Joel. Which Smart Plug Is the Best One for You? *Makeuseof* [online]. 2015 [cit. 2016-05-14]. Dostupné z: <http://www.makeuseof.com/tag/best-smart-plugs/>
- [55] LISZEWSKI, Andrew. When Your Internet Goes Out, This Smart Plug Resets Your Router Until It Works Again. *Gizmodo* [online]. 2016 [cit. 2016-05-14].

- Dostupné z: <http://gizmodo.com/when-your-internet-goes-out-this-smart-plug-resets-you-1774424411>
- [56] PROSPERO, Mike. The Best Smart Home Hub Is Just Less Bad Than Others. *Gizmodo* [online]. 2016 [cit. 2016-05-14]. Dostupné z: <http://www.tomsguide.com/us/best-smart-home-hubs,review-3200.html>
- [57] COLON, Alex. The Best Home Security Cameras of 2016. *PC Magazine* [online]. 2016 [cit. 2016-05-14]. Dostupné z: <http://www.pcmag.com/article2/0,2817,2475954,00.asp>
- [58] Smart home monitoring and power. *PC World* [online]. 2016 [cit. 2016-05-14]. Dostupné z: http://www.pcworld.co.uk/gbuk/smart-tech/smart-tech/smart-home/smart-home-monitoring-and-power/1072_8100_71177_xx_xx/xx-criteria.html
- [59] Near Field Communication (NFC). *Techopedia.com* [online]. 2016 [cit. 2016-05-14]. Dostupné z: <https://www.techopedia.com/definition/27583/near-field-communication-nfc>
- [60] CHASE, Jon. The Best Smart Lock. *The Wirecutter* [online]. 2016 [cit. 2016-05-14]. Dostupné z: <http://thewirecutter.com/reviews/the-best-smart-lock/>
- [61] LECLAIR, Dave. What Is A Smart Doorbell, And Which Should You Buy? *Makeuseof* [online]. 2014 [cit. 2016-05-14]. Dostupné z: <http://www.makeuseof.com/tag/what-is-a-smart-doorbell-and-which-should-you-buy/>
- [62] Definition of smart TV. *PC Magazine* [online]. [cit. 2016-05-15]. Dostupné z: <http://www.pcmag.com/encyclopedia/term/61971/smart-tv>
- [63] CARTER, Jamie. The 5 best Smart TV platforms in the world 2016. *TechRadar* [online]. 2016 [cit. 2016-05-15]. Dostupné z: <http://www.techradar.com/news/television/6-best-smart-tv-platforms-in-the-world-today-1120795>
- [64] LAMKIN, Paul. Connected cooking: The best smart kitchen devices and appliances. *Wareable* [online]. 2016 [cit. 2016-05-15]. Dostupné z: <http://www.wareable.com/smart-home/best-smart-kitchen-devices>
- [65] PRICE, Dan. Smart Kitchen Appliances You'll Wonder How You Lived Without. *Makeuseof* [online]. 2015 [cit. 2016-05-15]. Dostupné z:

<http://www.makeuseof.com/tag/smart-kitchen-appliances-youll-wonder-lived-without/>

- [65] PETERS, Luke. Smart Kitchen Appliances to Add to Your Home. *Tech.co* [online]. 2016 [cit. 2016-05-15]. Dostupné z: <http://tech.co/smart-kitchen-appliances-add-home-2016-03>
- [66] LESWING, Kif. This Smart Washing Machine Will Order More Detergent From Amazon. *Fortune* [online]. 2016 [cit. 2016-05-15]. Dostupné z: <http://fortune.com/2016/01/04/whirlpool-amazon-washer-dryer/>
- [67] WOLLERTON, Megan. LG Twin Wash review. *CNET* [online]. 2015 [cit. 2016-05-15]. Dostupné z: <http://www.cnet.com/products/lg-twin-wash/>
- [68] F900 Washing Machine. *Samsung* [online]. 2016 [cit. 2016-05-15]. Dostupné z: <http://www.samsung.com/uk/consumer/home-appliances/laundry/washing-machine/WF12F9E6P4W/EU>
- [69] LEE, Joel. 3 Reasons Why Your Next Faucet Should Be a Smart Faucet. *Makeuseof* [online]. 2015 [cit. 2016-05-15]. Dostupné z: <http://www.makeuseof.com/tag/next-faucet-smart-faucet/>
- [70] ULANOFF, Lance. Smart shower head will help you cut down on all that water you're wasting. *Mashable* [online]. 2016 [cit. 2016-05-15]. Dostupné z: <http://mashable.com/2016/01/05/hydrao-smart-shower-head-ces/>
- [71] TYRSINA, Radu. 15+ Best Smart Gardening Tools and Gadgets. *Technology Personalized* [online]. 2013 [cit. 2016-05-15]. Dostupné z: <http://techpp.com/2013/10/18/smart-gardening-gadgets/>
- [72] GEBHART, Andrew. Smart home garden tech buying guide. *CNET* [online]. 2015 [cit. 2016-05-15]. Dostupné z: <http://www.cnet.com/news/smart-outdoors-buying-guide/>
- [73] Top 5 Most Advanced Robotic Lawn Mowers. *Into Robotics* [online]. 2013 [cit. 2016-05-16]. Dostupné z: <http://www.intorobotics.com/top-5-most-advanced-robotics-lawn-mowers/>
- [74] Best Automatic Pet Feeder for 2016. *Best Pet Cam* [online]. 2016 [cit. 2016-05-16]. Dostupné z: <http://bestpetcam.com/automatic-pet-feeder/>

- [75] PetChatz Review: More than a Pet Treat Cam. *Best Pet Cam* [online]. 2016 [cit. 2016-05-16]. Dostupné z: <http://bestpetcam.com/petchatz-review-more-than-a-pet-treat-cam/>
- [76] Introduction. *Arduino* [online]. 2016 [cit. 2016-05-19]. Dostupné z: <https://www.arduino.cc/en/Guide/Introduction>
- [77] Arduino Software (IDE). *Arduino* [online]. 2016 [cit. 2016-05-19]. Dostupné z: <https://www.arduino.cc/en/Guide/Environment>
- [78] Products. *Arduino* [online]. 2016 [cit. 2016-05-19]. Dostupné z: <https://www.arduino.cc/en/Main/Products>
- [79] PWM. *Arduino* [online]. 2016 [cit. 2016-05-19]. Dostupné z: <https://www.arduino.cc/en/Tutorial/PWM>
- [80] Understanding ICSP for PIC Microcontrollers. *Instructables* [online]. 2006 [cit. 2016-05-19]. Dostupné z: <http://www.instructables.com/id/Understanding-ICSP-for-PIC-Microcontrollers/>
- [81] Serial Communication. *Sparkfun* [online]. 2016 [cit. 2016-05-19]. Dostupné z: <https://learn.sparkfun.com/tutorials/serial-communication/uarts>
- [82] USB TTL Serial Cables. *FTDI Chip* [online]. 2016 [cit. 2016-05-19]. Dostupné z: <http://www.ftdichip.com/Products/Cables/USBTTLSerial.htm>
- [83] Serial Peripheral Interface (SPI). *Sparkfun* [online]. 2016 [cit. 2016-05-19]. Dostupné z: <https://learn.sparkfun.com/tutorials/serial-peripheral-interface-spi>
- [84] What is JTAG and how can I make use of it? *XJTAG* [online]. 2016 [cit. 2016-05-19]. Dostupné z: <http://www.xjtag.com/support-jtag/what-is-jtag.php>
- [83] Arduino Shield List. *Shield List* [online]. 2016 [cit. 2016-05-19]. Dostupné z: <http://shieldlist.org/>
- [84] Arduino Certified Products. *Shield List* [online]. 2016 [cit. 2016-05-20]. Dostupné z: <https://www.arduino.cc/en/ArduinoCertified/Products>
- [85] Intel Galileo. *Arduino* [online]. 2016 [cit. 2016-05-20]. Dostupné z: <https://www.arduino.cc/en/ArduinoCertified/IntelGalileo>
- [86] Intel Galileo Gen2. *Arduino* [online]. 2016 [cit. 2016-05-20]. Dostupné z: <https://www.arduino.cc/en/ArduinoCertified/IntelGalileoGen2>

- [87] BOLDUC, Taylor. What Is Power Over Ethernet (POE), and How Is It Useful to You? *Makeuseof* [online]. 2015 [cit. 2016-05-20]. Dostupné z: <http://www.makeuseof.com/tag/poe-can-improve-connectivity/>
- [88] What is a Raspberry Pi? *Raspberry Pi* [online]. 2016 [cit. 2016-05-21]. Dostupné z: <https://www.raspberrypi.org/help/what-is-a-raspberry-pi/>
- [89] Raspberry Pi Model A+. *RS Components* [online]. 2016 [cit. 2016-05-21]. Dostupné z: <http://uk.rs-online.com/web/p/processor-microcontroller-development-kits/8332699/>
- [90] Raspberry Pi Model B+. *RS Components* [online]. 2016 [cit. 2016-05-21]. Dostupné z: <http://uk.rs-online.com/web/p/processor-microcontroller-development-kits/8111284/>
- [91] GPIO: Raspberry Pi Models A and B. *Raspberry Pi* [online]. 2016 [cit. 2016-05-21]. Dostupné z: <https://www.raspberrypi.org/documentation/usage/gpio/>
- [92] Raspberry Pi 2 Model B. *RS Components* [online]. 2016 [cit. 2016-05-21]. Dostupné z: <http://uk.rs-online.com/web/p/processor-microcontroller-development-kits/8472816/>
- [93] Raspberry Pi 3 Model B. *RS Components* [online]. 2016 [cit. 2016-05-21]. Dostupné z: <http://uk.rs-online.com/web/p/processor-microcontroller-development-kits/8968664/>
- [94] Raspberry Pi Zero: The \$5 computer. *Raspberry Pi* [online]. 2016 [cit. 2016-05-21]. Dostupné z: <https://www.raspberrypi.org/blog/raspberry-pi-zero/>
- [95] The \$5 Raspberry Pi Zero is one elusive stocking stuffer. *Network World* [online]. 2016 [cit. 2016-05-21]. Dostupné z: <http://www.networkworld.com/article/3010209/opensource-subnet/the-5-raspberry-pi-zero-is-one-elusive-stocking-stuffer.html>
- [96] FAQs. *Gizmosphere* [online]. 2016 [cit. 2016-05-22]. Dostupné z: <http://www.gizmosphere.org/gizmoboard-support/faqs/>
- [97] Gizmo 1. *Gizmosphere* [online]. 2016 [cit. 2016-05-22]. Dostupné z: <http://www.gizmosphere.org/products/gizmo-explorer-kit/>
- [98] Gizmo Explorer Kit User Guide. *Gizmosphere* [online]. 2013 [cit. 2016-05-22]. Dostupné z: <http://www.gizmosphere.org/wp-content/uploads/2013/07/Gizmo-Explorer-Kit-User-Guide-Rev-2.6.pdf>

- [99] Gizmo 2. *Gizmosphere* [online]. 2014 [cit. 2016-05-22]. Dostupné z:
[http://www.gizmosphere.org/wp-
content/uploads/2014/11/4531_Gizmo2_ProBRIEF_FNL.Element14.pdf](http://www.gizmosphere.org/wp-content/uploads/2014/11/4531_Gizmo2_ProBRIEF_FNL.Element14.pdf)

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

IoT	Internet of Things
MEMS	Mikro-elektro-mechanické systémy
M2M	Machine to Machine
LAN	Local Area Network
WAN	Wide Area Network
TCP	Transmission Control Protocol
IP	Internet Protocol
OSI	Open System Interconnection
ISO	International Organization for Standardization
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
RIP	Routing Information Protocol
RAM	Random Access Memory
LLN	Low-power and Lossy Networks
IETF	Internet Engineering Task Force
ROLL	Routing Over Low-power and Lossy networks
BER	Bit Error Rate
RPL	Routing Protocol for Low Power and Lossy Networks
DVRP	Distance Vector Routing Protocol
DAG	Directed Acyclic Graph
DODAG	Destination Oriented Directed Acyclic Graph
UDP	User Datagram Protocol
IEEE	Institute of Electrical and Electronics Engineers
PAN	Personal Area Networks

WPAN	Wireless Personal Area Network
OSI	Open Systems Interconnection model
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
CoAP	Constrained Application Protocol
HTTP	Hypertext Transfer Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
LED	Light Emitting Diode
TLS	Transport Layer Security
SSL	Secure Sockets Layer
AES	Advanced Encryption Standard
IDE	Integrated development environment
PWM	Pulse-width modulation
ICSP	In-Circuit Serial Programming
ARM	Advanced RICS Machine
SPI	Serial Peripheral Interface
SD	Secure Digital
UAST	Universal asynchronous receiver/transmitter
LCD	Liquid-crystal Display
GPRS	General Packet Radio Service
SRAM	Static Random Access Memory
EEPROM	Electrically Erasable Programmable Read-Only Memory
HDMI	High-Definition Multimedia Interface
GPIO	General-purpose input/output
CPU	Central Processing Unit

GPU	Graphic Processing Unit
DSI	Display Serial Interface
CSI	Camera Serial Interface
BIOS	Basic Input/Output System

SEZNAM OBRÁZKŮ

OBRÁZEK 1: RASPBERRY PI, ARDUINO A INTEL GALILEO (ZDROJ: WIKIPEDIE).....	31
OBRÁZEK 2: PHILIPS HUE ^[49]	32
OBRÁZEK 3: CUBE SENSORS ^[51]	32
OBRÁZEK 4: ROOMBA 980 ^[52]	33
OBRÁZEK 5: NEST ^[53]	33
OBRÁZEK 6: RESETPLUG ^[55]	34
OBRÁZEK 7: SMARTTHINGS HUB ^[56]	34
OBRÁZEK 8: ICONTROL NETWORKS PIPER NV ^[57]	35
OBRÁZEK 9: SMARTTHINGS MULTI SENSOR ^[58]	35
OBRÁZEK 10: KWIKSET KEVO SMART LOCK ^[60]	36
OBRÁZEK 11: DOORBOT ^[61]	36
OBRÁZEK 12: CHYTRÁ TELEVIZE LG ^[63]	37
OBRÁZEK 13: SAMSUNG F900 ^[68]	39
OBRÁZEK 14: HYDRAO ^[70]	39
OBRÁZEK 15: INDOOR GARDEN ^[71]	40
OBRÁZEK 16: HUSQVARNA AUTOMOWER ^[73]	40
OBRÁZEK 17: PETCHATZ HD GREET & TREAT CAMERA ^[75]	41
OBRÁZEK 18: ARDUINO A GENUINO UNO ^[78]	44
OBRÁZEK 19: ARDUINO A GENUINO 101 ^[78]	44
OBRÁZEK 20: ARDUINO PRO ^[78]	45
OBRÁZEK 21: ARDUINO A GENUINO MEGA 2560 ^[78]	45
OBRÁZEK 22: ARDUINO A GENUINO ZERO ^[78]	46
OBRÁZEK 23: ARDUINO DUE ^[78]	46
OBRÁZEK 24: ARDUINO YÚN ^[78]	47
OBRÁZEK 25: LILYPAD ARDUINO USB ^[78]	47
OBRÁZEK 26: GPRS SHIELD OD SPOLEČNOSTI SEED STUDIO ^[83]	49
OBRÁZEK 27: INTEL GALILEO GEN 1 ^[85]	49
OBRÁZEK 28: INTEL GALILEO GEN 2 ^[86]	50
OBRÁZEK 29: RASPBERRY PI 1 MODEL B+ ^[90]	51
OBRÁZEK 30: RASPBERRY PI ZERO ^[95]	52
OBRÁZEK 31: GIZMO 1 ^[98]	54
OBRÁZEK 32: GIZMO 1 ^[99]	54

SEZNAM TABULEK

TABULKA 1: NEJROZŠÍŘENĚJŠÍ ODVĚTVÍ IOT	12
TABULKA 2: NEJVĚTŠÍ SPOLEČNOSTI NA TRHU IOT	13
TABULKA 3: ROZDÍL VE SMĚROVÁNÍ V SOUČASNÉM INTERNETU A V LLN	19
TABULKA 4: SROVNÁNÍ BLUETOOTH TECHNOLOGIE A LOW ENERGY TECHNOLOGIE ^[30]	22
TABULKA 5: SROVNÁNÍ MOBILNÍCH DATOVÝCH SÍTÍ ^[32]	22
TABULKA 6: PŘEHLED POUŽITÍ CHYTRÝCH ZAŘÍZENÍ V DOMÁCNOSTI.....	31
TABULKA 7: CHYTRÁ ZAŘÍZENÍ PRO POUŽITÍ V KUCHYNI ^{[64] [65] [65]}	38
TABULKA 8: SROVNÁNÍ VYBRANÝCH PARAMETRŮ DESEK ARDUINO ^[78]	48
TABULKA 9: SROVNÁNÍ VYBRANÝCH PARAMETRŮ DESEK INTEL ^{[85] [86]}	50
TABULKA 10: SROVNÁNÍ VYBRANÝCH PARAMETRŮ DESEK RASPBERRY ^{[89] [90]} ^{[92] [93] [94]}	53
TABULKA 11: POROVNÁNÍ VYBRANÝCH PARAMETRŮ DESEK GIZMOSPHERE ^[99]	54

SEZNAM SCHÉMAT

SCHÉMA 1: FUNKCE SOUČÁSTÍ CHYTRÉHO OBJEKTU.....	11
SCHÉMA 2: OBECNÉ M2M ŘEŠENÍ.....	14
SCHÉMA 3: PŘEHLED KOMUNIKAČNÍCH TECHNOLOGIÍ IOT	15
SCHÉMA 4: KOMUNIKACE ZAŘÍZENÍ V CHYTRÉ DOMÁCNOSTI	30

SEZNAM PŘÍLOH

K bakalářské práci je přiloženo CD s prací v elektronické podobě a s výukovou prezentací, která je součástí praktické části.