

Univerzita Pardubice

Fakulta elektrotechniky a informatiky

Návrh a realizace systému identifikace a ověření pro IoT
Václav Jelínek

Diplomová práce
2016

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: 2015/2016

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Václav Jelínek**
Osobní číslo: **I14259**
Studijní program: **N2646 Informační technologie**
Studijní obor: **Informační technologie**
Název tématu: **Návrh a realizace systému identifikace a ověření pro IoT**
Zadávající katedra: **Katedra softwarových technologií**

Z á s a d y p r o v y p r a c o v á n í :

Cílem práce je provést analýzu bezpečnostních rizik inteligentních sítí a jejich využití pro Internet of Things (IoT). V teoretické části autor provede analýzu možných bezpečnostních rizik spojených s rozvojem a využíváním inteligentních sítí s důrazem na IoT. Dále autor navrhne možnosti zabezpečení komunikace v IoT s možností využití hardwarových specifikací prvků využívaných v IoT (Ardunino, Raspberry Pi 2). V praktické části autor navržené řešení realizuje a otestuje. Praktická část bude realizována buď pomocí vhodného simulátoru nebo s využitím dostupného hardware, dle navrženého řešení z teoretické části.

Rozsah grafických prací:

Rozsah pracovní zprávy: 60

Forma zpracování diplomové práce: tištěná

Seznam odborné literatury:

BEHMANN, Fawzi a Kwok WU. Collaborative internet of things (C-IoT): for future smart connected life and business. Hoboken: John Wiley and Sons, Inc., 2015, pages cm. ISBN 9781118913741.

HU, Fei. Security and Privacy in Internet of Things (Iots) : Models, Algorithms, and Implementations. 1. PortlandUnited States: Productivity Press, 2016. ISBN 9781498723183.

Vedoucí diplomové práce:

Mgr. Josef Horálek, Ph.D.

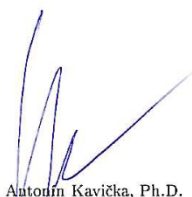
Katedra informačních technologií

Datum zadání diplomové práce: 31. října 2015

Termín odevzdání diplomové práce: 13. května 2016



prof. Ing. Simeon Karamazov, Dr.
děkan



prof. Ing. Antonín Kavička, Ph.D.
vedoucí katedry

V Pardubicích dne 15. listopadu 2015

Prohlášení autora

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše. Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 12. 5. 2016

Bc. Václav Jelínek

Poděkování

Rád bych poděkoval Mgr. Josefu Horálkovi, Ph.D za cenné rady a informace při vedení mé diplomové práce. Také děkuji své rodině za podporu během celého studia.

Anotace

Práce se zabývá Internetem věcí a bezpečností. V teoretické části jsou popsány možnosti využití Internetu věcí, současná situace v České republice a také používané přenosové sítě. Poslední kapitola teoretické části zahrnuje bezpečnost Internetu věcí a možné útoky. Dále obsahuje různá doporučení pro zlepšení bezpečnosti. Praktická část je zaměřena na realizaci systému pro ověření a identifikaci zařízení v Internetu věcí. Je zde popsán způsob ověření, jeho postup a funkcionality uživatelského webového rozhraní.

Klíčová slova

IEEE, Internet věcí, zabezpečení, autentizace, ZigBee, 6LoWPAN

Title

Design and implementation of identification and authentication system for IoT

Annotation

The thesis deals with the Internet of Things and security. In theoretical part there are described possibilities of using the Internet of Things, current situation in Czech Republic and used transmission networks. Last chapter of theoretical part focuses on security and possible attacks. This part also contains recommendations related to a security improvement. Practical part focuses on realization of system for device authentication and identification in the Internet of Things. There is described method of authentication, its procedure and function of user web interface.

Keywords

IEEE, Internet of Things, security, authentication, ZigBee, 6LoWPAN

Obsah

Seznam zkratek	8
Seznam obrázků	9
Úvod	11
1 Internet věcí (IoT).....	12
1.1 Využití IoT	13
1.2 Situace v současnosti	16
1.3 Přenosové bezdrátové sítě.....	17
1.3.1 Wireless PAN	18
1.3.2 Wireless LAN	19
1.3.3 Wireless MAN	19
1.3.4 Wireless WAN	20
1.4 Standard IEEE 802.15.4.....	20
1.4.1 Prvky sítě WPAN IEEE 802.15.4	21
1.4.2 Topologie	21
1.4.3 Architektura IEEE 802.15.4.....	22
1.4.4 Struktura super rámce	24
1.4.5 Struktura rámce	25
1.5 ZigBee.....	26
1.5.1 Typy zařízení	27
1.5.2 Topologie	27
1.5.3 Model ZigBee	29
1.6 6LoWPAN	31
1.6.1 Architektura 6LoWPAN	33
1.6.2 Model 6LoWPAN.....	34
1.6.3 Adaptační vrstva 6LoWPAN	36
1.6.4 IPv6.....	39
1.7 Jiné technologie	41
1.7.1 LoRa.....	41
1.7.2 Z-Wave	42
1.7.3 SIGFOX	43

2	Analýza bezpečnostních rizik	44
2.1	Bezpečnostní rizika	45
2.2	Typy útoků	49
2.2.1	Pasivní útoky	50
2.2.2	Aktivní útoky	51
2.3	Doporučení	54
2.3.1	Autentizace	55
2.3.2	Autorizace	56
2.3.3	Accounting	56
3	Návrh a implementace	57
3.1	Použité technologie a hardware	57
3.1.1	Raspberry Pi	58
3.1.2	MySQL	59
3.1.3	Apache	59
3.1.4	OpenSSL	59
3.1.5	Další využití technologie	60
3.2	DS2401	63
3.2.1	1-Wire sběrnice	64
3.2.2	Schéma zapojení DS2401	64
3.3	Navrhovaný systém	66
3.4	Autentizace	67
3.4.1	Zabezpečená komunikace	67
3.4.2	Generování certifikátů	69
3.4.3	Ověření	70
3.4.4	Spuštění	71
3.5	Návrh Databáze	72
3.6	Konfigurace serveru	73
3.7	Konfigurace klienta	78
3.8	Uživatelská aplikace	79
4	Závěr	82
	Literatura	84

Seznam zkratek

6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks
AP	Access Point
DHCP	Dynamic Host Configuration Protocol
FFD	Full Functional Device
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
ISP	Internet Service Provider
LAN	Local Area Network
LR-WPAN	Low Rate Wireless Personal Area Network
MAC	Medium Access Control
NAT	Network Address Translation
PHY	Physical layer
RFC	Request For Comments
RFD	Reduced Function Device
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network

Seznam obrázků

Obrázek 1 Topologie WLAN	19
Obrázek 2 Topologie sítě podle IEEE 802.15.4.....	21
Obrázek 3 LR-WPAN architektura zařízení	22
Obrázek 4 Struktura super rámce	24
Obrázek 5 Struktura aktivní periody s GTS	25
Obrázek 6 Schéma pohledu PPDU	26
Obrázek 7 ZigBee topologie	27
Obrázek 8 Referenční model ZigBee	29
Obrázek 9 6LoWPAN architektura	33
Obrázek 10 TCP/IP a 6LoWPAN model	35
Obrázek 11 Příklad komprese IPv6 hlaviček 6LoWPAN (Hui, 2009)	37
Obrázek 12 6LoWPAN fragment hlavička	38
Obrázek 13 6LoWPAN složení hlavičky (Hui, 2009)	38
Obrázek 14 SIGFOX mapa pokrytí (Technologie SIGFOX, 2016)	43
Obrázek 15 IoT síťová architektura (Securing the Internet of Things, 2015).....	46
Obrázek 16 Schéma pasivního útoku	50
Obrázek 17 Schéma aktivního útoku	51
Obrázek 18 Ukázka MITM útoku	52
Obrázek 19 Ukázka DDoS útoku	53
Obrázek 20 Raspberry Pi model B+ (Upton, 2014)	58
Obrázek 21 Průchod paketu	60
Obrázek 22 DS2401 přehled	63
Obrázek 23 DS2401 paměťová mapa	64
Obrázek 24 Schéma zapojení DS2401	65
Obrázek 25 Schéma sítě	66
Obrázek 26 TLS Handshake	67
Obrázek 27 Schéma autentizace.....	70
Obrázek 28 Tabulka zařízení	72
Obrázek 29 Tabulka účtování	72
Obrázek 30 Tabulka uživatelů	73
Obrázek 31 Přehled zařízení	79

Obrázek 32 Pravidla mobilní telefon	80
Obrázek 33 Pravidla	80
Obrázek 34 Logování	81
Obrázek 35 Záložka Ping	81

Úvod

Žijeme v moderní době, která s sebou nese nové technologie a možnosti. Některé vznikají za účelem pomoci lidstvu, jiné zase kvůli pohodlnosti či lenosti. Před 20 lety si jen stěží někdo dokázal představit, že skoro každý člověk bude vlastnit chytrý mobilní telefon s dotykovým displejem, internetem, a v takové velikosti, aby se vyšel to kapsy. Když si Škopkovi ve filmu Zdeňka Trošky pořídili počítač, spolu s farářem Otíkem byli jediní, kdo v Hořticích vlastnil počítač. Dnes má počítač skoro každá domácnost a ne jen jeden. V dnešní době existují i roboti, kteří za nás uklidí, auta, která dokážou sama řídit. Člověk je inteligentní tvor a odjakživa se snaží si vše zjednodušit. Historie mluví za vše, kdy pralidé z kamenů a klacků začali vyrábět lepší a sofistikovanější nástroje a zbraně. I díky tomu je lidstvo tam, kde dnes je.

Vývoj technologií jde neustále kupředu. Vznikají inteligentní sítě a chytré domácnosti. Čím dále více se zvyšuje snaha přidat do každé věci nějaký stupeň inteligence pomocí senzorů, či čidel a vytvořit tak „chytré zařízení“. Například České Radiokomunikace si dokáží představit chytrou popelnici, která sama pozná, že je plná a řekne si o vyvezení. ČEZ zase experimentuje s chytrou sítí pro měřidla energií. Před pár lety sci-fi, dnes běžná realita. S trendem ovládání věcí na dálku pomocí Internetu vzniká pojem Internet věcí. Nejedná se pouze o zhasínání světel, či regulaci tepla. Dnešní technologie jsou tak pokročilé, že je možné vytvořit ucelený systém ovládání, který bude zcela automatický.

Tato práce se zabývá tzv. Internetem věcí a otázkou bezpečnosti. Jelikož se jedná o nové a velmi rychle se rozvíjející téma, je možné, že již po půl roce nemusí být práce aktuální a některé věci mohou být jinak, než je zde uvedeno. Práce je rozdělena do dvou částí – teoretické a praktické.

Teoretická část nejprve popisuje Internet věcí, možnosti jeho využití a současný stav v České republice. Poté se zaměřuje na přenosové sítě a relativně nové technologie, které lze v Internetu věcí využít. U těchto technologií jsou uvedeny základní principy, typy použitých topologií a typy zařízení. Další část se zabývá otázkou bezpečnosti zařízení. Poslední část teoretické části se zaměřuje na možné typy síťových útoků. Jsou zde zmíněny pasivní a aktivní útoky, a možná doporučení, která by měla zlepšit bezpečnost zařízení.

V praktické části je navržen a implementován systém identifikace a ověření pro zařízení v Internetu věcí. Dále jsou v této části popsány použité technologie, hardware a konfigurace zařízení. V závěru je ukázána funkcionality webového rozhraní.

1 Internet věcí (IoT)

Pojem Internet je mezi námi dlouhou dobu a každý z nás ho zná. Z malé vědecké sítě se stala globální všudypřítomná síť, kterou pravidelně využívá více než miliarda lidí. Internet je otevřený inovacím. V dnešní době žijeme ve společnosti, kdy inovace a vývoj došel tak daleko, že nám normální Internet nestačí a chceme mnohem víc. „Vše co lze i nelze připojme do Internetu!“.

Internet of Things (IoT, internet věcí) je síť spojující „věci“. V současné době je to velmi žhavé téma, o kterém je slyšet čím dál víc a postupně se stává velmi důležitým i pro velké firmy. Člověk jako pohodlný a líný tvor planety, chce mít vše jednodušší. Proč chodit nakupovat, když by to mohla zvládnout sama chladnička? Proč rozsvěcet světla, když by to zvládl jednoduchý inteligentní systém? Tyto lidské vlastnosti a otázky napomáhají k rozvoji technologiím a bezdrátovým sítím, které to umožňují. Příkladem toho může být IoT. Není to však úplně nový pojem nebo koncept. Poprvé pojem „internet věcí“ použil Kevin Ashton v roce 2000 na MIT (Massachusetts Institute of Technology). Napsal: *„I could be wrong, but I'm fairly sure the phrase "Internet of Things" started life as the title of a presentation I made at Procter & Gamble (P&G) in 1999. Linking the new idea of RFID in P&G's supply chain to the then-redhot topic of the Internet was more than just a good way to get executive attention“* (Ashton, 2009)

Internet věcí popisuje svět navzájem propojených zařízení, jichž může být nespočet. Skládá se z fyzických a virtuálních objektů „věcí“ propojených přes síť. Objekty jsou vybaveny senzory, čipy, procesory a funkcemi pro připojení k síti. Mohou spolu komunikovat, sbírat data, posílat data. Hlavním rozdílem od klasického internetu je, že objekty IoT nejsou jen počítače, jak je zvykem. Propojené objekty mohou být různé druhy zařízení od spotřební elektroniky, jako jsou chytré televize, ledničky až po malé senzory, čidla či automobily. Většina věcí připojených v IoT jsou velmi jednoduchá zařízení, která se často označují jako „chytrá zařízení“ nebo „embedded zařízení“. Zařízení však nemusí být chytrá sama o sobě, ale stávají se chytrými ve spojení s ostatními zařízeními. Více propojených zařízení dokáže vytvořit ucelený systém, který se může rozhodovat vlastní „inteligencí“ bez zásahu člověka. Všechny zařízení daného systému pak spolu komunikují inteligentním a automatizovaným způsobem. (Miller, 2015)

IoT kombinuje zařízení pro sběr dat a provádějící činnosti na základě získaných dat. Některá připojená zařízení obsahují senzory, které dokáží vnímat věci okolo sebe (teplota, světlo, pohyb). Tato zařízení posílají shromážděná data do jiných zařízení, která jsou určena pro

provádění určité činnosti. Jednoduchým příkladem může být chytré parkoviště. Každé parkovací místo bude mít zařízení se senzorem, které bude kontrolovat obsazenost místa. V případě, že se parkovací místo uvolní nebo obsadí, zařízení se senzorem pošle data dalšímu zařízení. To bude provádět určitou činnost (informovat o obsazenosti jednotlivých parkovacích míst). Pokud přijede řidič s inteligentním autem, bude ihned vědět, kde může zaparkovat.

1.1 Využití IoT

Možnosti IoT nejsou jen o tom, že si budeme moci zjistit obsazenost parkovacích míst, na dálku ovládat osvětlení v domácnosti, nastavit teplotu kotle. IoT má využití v mnoha průmyslových a vědeckých oborech. Například sledování výroby v továrnách, či předpověď katastrof pomocí senzorů rozmístěných po planetě. (Miller, 2015)

O IoT projevuje zájem celá řada velkých hráčů jako je Intel, Cisco, T-Mobile. IoT lze aplikovat např. v chytrých městech, automobilech, domácnostech, energetice, ochraně životního prostředí, zemědělství, bezpečnosti, cestovním ruchu.

Vzhledem k tomu, že se IoT stále vyvíjí, další potenciál je v kombinaci technologií a konceptů jako je například Cloud Computing, Big Data, robotika. Tyto pojmy nejsou nové, ale v součinnosti a jejich kombinaci mohou přinést nové způsoby chápání IoT.

IoT je stále ve vývoji zejména z těchto faktů:

- žádný jasný přístup pro jedinečné identifikování věcí a adresování prostoru v globálním měřítku,
- malý pokrok ve výměně informací v heterogenním prostředí,
- problémy s důvěrou a vlastnictvím dat v IoT, dodržení bezpečnosti a soukromí ve složitém prostředí,
- složitý rozvoj v podnikání,
- nedostatečná možnost testování ve velkém měřítku,
- praktické aspekty, jakou jsou roamingové poplatky, pronájem za umístěné senzory.

Překonání všech překážek, by znamenalo lepší využití potenciálu IoT.

V následujícím seznamu jsou příklady pro využití IoT v různých oblastech, což ukazuje, proč je IoT jedním ze strategických trendů příštích let. (Vermesan a Friess, 2013, s. 33-36)

Města

- Inteligentní parkování – monitorování parkovacích míst ve městě.
- Dopravní zácpy – sledování provozu, vozidel a chodců pro optimalizaci jízdních a pěších tras.
- Inteligentní osvětlení – inteligentní a adaptivní osvětlení pouličních lamp na základě počasí.
- Sběrné služby – sledování úrovně odpadků v kontejnerech pro optimální vyvážení.
- Inteligentní dopravní systém – inteligentní silnice a dálnice, které dokážou upozornit řidiče na neočekávané události, případně poradit jinou trasu.

Životní prostředí

- Detekce lesních požárů – sledování spalín a detekce požárů ve vyznačených oblastech.
- Kvalita ovzduší – měření emisí CO₂ z továren, automobilů a toxických plynů vznikajících ve fabrikách.
- Sesuny půdy a laviny – monitorování vlhkosti půdy, vibrací a hustoty půdy k detekování nebezpečí.
- Zemětřesení – včasné upozornění na hrozící zemětřesení monitorováním v místech otřesů.

Energetika

- Smart Grid – sledování spotřeby energie..
- Zásoby – monitorování hladiny vody, ropy a zemního plynu v zásobnících.

Zdravotnictví

- Detekce pádů – rychlá pomoc pro seniory a zdravotně postižené osoby.
- Dozor pacientů – stav pacientů v nemocnicích a v domově důchodců.
- Ultrafialové záření – varování před vysokou hodnotou UV.

Domácnosti

- Energie – ušetření nákladů a prostředků, díky monitorování spotřeby.
- Ovládání spotřebičů – zapínání a vypínání spotřebičů na dálku.
- Zabezpečení – kontrola oken a vstupních dveří.

Z těchto uvedených příkladů lze říci, že IoT má velmi různorodé uplatnění, slouží různým uživatelům a každá oblast má jiné potřeby. (Vermesan a Friess, 2013, s. 37-39)

Z pohledu IoT existují tři důležité uživatelské kategorie:

- jednotlivci,
- komunity občanů (města, země, nebo společnost jako celek),
- podniky.

V první skupině může být důležité zvýšení bezpečnosti jednotlivců nebo jejich rodinných příslušníků. Příkladem může být dálkové ovládání poplašných alarmů nebo detekce cizí aktivity. Umožnit mnohem pohodlnější vykonávání činností, zlepšení životního stylu i snížení nákladů na bydlení. (Vermesan a Friess, 2013, s. 37-39)

Společnost lidí má různé potřeby, často ve střednědobém až dlouhodobém časovém měřítku. Asi ta nejdůležitější potřeba je bezpečnost společnosti, na základě nedávných katastrof. Například jaderná katastrofa v Japonsku, zemětřesení, teroristické útoky, tsunami. Jedním požadavkem společnosti může být schopnost předvídat podobné události. Další požadavek může být sledování různých znečišťujících látek v životním prostředí (Vermesan a Friess, 2013, s. 37-39)

Podniky jakožto třetí kategorií uživatelů IoT, mají různé potřeby a odlišné požadavky. Některé z nich mohou být použity v IoT:

- Zvýšení produktivity – je cílem většiny podniků, ovlivňuje úspěch a ziskovost podniku.
- Rozdílnost trhu – podnik se snaží odlišit z přesyceného trhu (podobné výrobky a služby), IoT může být jednou z odlišností.
- Náklady – snaha snížení provozních nákladů podniku. IoT lze použít pro lepší využití zdrojů, získávání lepších informací v rozhodovacím procesu.

1.2 Situace v současnosti

Internet věcí si razí cestu k nám do České Republiky. Jako první se do IoT vrhly T-Mobile a České Radiokomunikace. Přípravují vlastní mobilní sítě pro IoT, které budou fungovat pro komunikaci zařízení na nelicencovaném pásmu 868 MHz. Společnosti chystají sítě na rozdílných technologiích a potencionálních standardech. Obě společnosti mají dobré podmínky pro testování sítí pro IoT. Mohou využít stávající infrastruktury vysílačů a nemusí platit za licenční frekvenční pásmo.

České Radiokomunikace spustili dne 21. 5. 2015 pilotní provoz unikátní bezdrátové technologie pro IoT. Technologie spočívá ve využití datového protokolu, umožňující efektivní a bezpečnou obousměrnou komunikaci čidel a senzorů. Testovaná síť je založena na otevřeném standardu LoRa, která se vyznačuje nízkou spotřebou, vysokým dosahem a nízkými provozními náklady. (Vstupujeme do internetu věcí, 2015) Použitou technologii chválí i sám obchodní ředitel firmy Sichrovský: „*Ve výsledcích LoRa výrazně předčí veškeré alternativní dostupné technologie, čímž se otevírá široké pole využití pro chytrou domácnost, chytré město, chytré měření, chytrou výrobu, apod. Internet věcí zásadně přispěje k zefektivnění celé řady lidských činností a povede ke zjednodušení každodenního života*“. (Internet věcí- zahájení pilotního provozu, 2015).

Dne 21. 1. 2016 se ČRa na základě vyhodnocení pilotního provozu pro odečet plynoměrů, rozhodla vybudovat síť pokrytí vybraných míst České republiky. Testy u technologie LoRa ukázaly vynikající výsledky zejména velkého dosahu. Kvalitních hodnot technologie Lora dosáhla i při velmi nízkém vysílacím výkonu, který má významný vliv na prodloužení výdrže baterií v senzorech a zařízení. LoRa umožňuje nejen monitoring a sběr dat, ale i ovládání zařízení na dálku. K samotnému IoT říká obchodní ředitel ČRa: „*Internet věcí jsme vyhodnotili jako vysoce perspektivní oblast budoucnosti a nechceme promarnit v přípravách ani jeden den*“. (Budujeme síť pro internet věcí na technologii Lora, 2016).

T-Mobile plánuje v roce 2016 pokrýt ČR sítí pro IoT. Připojil se k francouzskému projektu SIGFOX a testuje IoT jako provozovatel. Oproti LoRa je SIGFOX komerční a poměrně uzavřenou technologií. SIGFOX je francouzská společnost, která technologii vyvíjí a stará se o tok dat. Zákazníkům poskytuje přístup k centrálnímu cloudu a pomocí SDK a API (vývojářská sada a aplikační rozhraní) si zákazník dokáže vytvořit vlastní aplikaci. Síť má zajistit především přenos krátkých textových zpráv (periodické odesílání GPS lokace, naměřených hodnot). SIGFOX přináší velmi dlouhou životnost baterií a nízké náklady na

implementaci technologie do zařízení. Pro T-Mobile plánuje vytvořit minimálně 350 základnových stanic pro celoplošné pokrytí ČR. (Vašina a Hába 2015)

Nové příležitosti se však chytí ještě třetí hráč a to Free.Things.cz. Tato společnost vznikla před pár týdny a chce využít potenciálu IoT. Využívá otevřenou platformu LoRa stejně jako České Radiokomunikace, ovšem budování sítě je realizováno v rámci lokálních ISP (poskytovatelů internetu). Free.Things.cz cílí zejména na domácí uživatele, malé a střední firmy. Pro lokální ISP, může tato technologie znamenat konkurenční výhodu a obchodní příležitost, oproti ostatním lokálním ISP. (Things, 2016)

1.3 Přenosové bezdrátové sítě

Internet věcí využívá ke svému chodu velkou řadu technologií a zařízení. Jedná se o velmi široké spektrum, které zahrnuje nejen komunikaci mezi jednotlivými věcmi, ale také jejich autonomní provoz či identifikaci objektů. IoT pro svou komunikaci využívá přenosové sítě, které jsou jeho důležitou součástí. Důležité je zmínit, že jednotlivé směry IoT jsou velmi různorodé a pouze jedna technologie je nepokryje.

Přenosových sítí je velké množství. V této práci budou podrobně rozebrány jen ty stěžejní pro IoT. Přenosové sítě můžeme rozdělit na dvě kategorie, a to drátové sítě a bezdrátové sítě. Výhodnější pro IoT jsou bezesporu bezdrátové sítě, které budou dále popsány.

Hlavní výhodou bezdrátových sítí je jejich mobilita a škálovatelnost. Při vytváření nové sítě není potřeba pokládat kabeláž a lze ji snadno rozšířit o další prvky. Přináší možnost výstavby sítě i tam, kde by to jinak nebylo možné (například senzorová síť na severním pólu). Bezdrátové technologie umožňují prvkům sítě (zařízením) pohyb. V následujících odstavcích budou stručně popsány jednotlivé typy bezdrátových sítí. Typy bezdrátových sítí lze rozdělit následovně.

1.3.1 Wireless PAN

Bezdrátová osobní síť WPAN (Wireless Personal Area Network) – jedná se o malou bezdrátovou osobní síť, která propojuje zařízení na malé vzdálenosti. Nejpoužívanější technologie ve WPAN sítích je Bluetooth, IrDA, UWB a ZigBee. Tento typ sítě popisuje rodina standardů IEEE 802.15.

Bluetooth

Bluetooth je bezdrátová komunikační technologie, která umožňuje pohodlné bezdrátové připojení, například mezi počítačem a kompatibilním zařízením Bluetooth (mobilní telefony, klávesnice). Technologie Bluetooth je definována standardem IEEE 802.15.1 a pracuje v pásmu 2,4 GHz. Nejnovější verze Bluetooth je 4.2, která nabízí mnohem nižší energetickou spotřebu, vyšší míru zabezpečení, vyšší rychlost přenosu a konektivitu, pro podstatně širší množinu zařízení. (Bluetooth core specification, 2015)

IrDA

IrDA (Infrared Data Association) je komunikační technologie, která se hojně využívala u starších mobilních telefonů. Postupem času byla nahrazována Bluetooth. Dnes se však začíná do mobilních zařízení vracet. Jako příkladem může být pohodlné ovládání televizoru pomocí mobilního telefonu. Pro komunikující zařízení platí, že musí být ve vzájemném dosahu (ve vzájemné přímé viditelnosti). IrDA vysílá a přijímá modulované infračervené světlo o vlnové délce 875 nm.

ZigBee

ZigBee je bezdrátová komunikační technologie postavená na standardu IEEE 802.15.4, která je podrobněji popsána v kapitole 1.5.

1.3.2 Wireless LAN

Místní bezdrátová síť WLAN (Wireless Local Area Network) – spojuje dvě nebo více zařízení pomocí určité distribuční metody. Tyto sítě jsou velmi oblíbené v domácnostech pro jejich snadnou instalaci a použití. Základní standard pro WLAN je IEEE 802.11, který zahrnuje celou rodinu norem, označovaných pomocí doplňkových písmen na konci, např. 802.11b, 802.11ac atd. Pro WLAN síť založené na standardech rodiny 802.11 jsou typické dvě topologie: ad-hoc (peer-to-peer) a infrastruktura.



Obrázek 1 Topologie WLAN

U ad-hoc spolu zařízení komunikují přímo, z toho důvodu musí být stanice, které spolu komunikují v rádiovém dosahu. V topologii infrastruktura se jednotlivé stanice připojují k přístupovému bodu AP (Access Point) a komunikující zařízení nemusí být v přímém dosahu.

Standard pro bezdrátové sítě IEEE 802.11 vznikl v červenci roku 1997. Ke své činnosti využívá bezlicenční pásmo 2,4 GHz do 2,4835 GHz a 5,47 GHz do 5,725 GHz.

1.3.3 Wireless MAN

Bezdrátová metropolitní síť WMAN (Wireless Metropolitan Area Network) – síť zařízení, která je určena pro velké geografické oblasti, jakou jsou městské oblasti. Často poskytuje integrované komunikační služby jako je přenos dat, hlasu, obrazu a videa. MAN sítě jsou optimalizovány pro větší geografické vzdálenosti, než například LAN, počínaje několika bloky budov až po celé město. Poskytuje střední až vysoké přenosové rychlosti dat. Podle IEEE 802-2014 může být vlastněna a provozována jednou organizací, obvykle je však využívána mnoha jedinci a organizacemi. Využívá technologie WiMax definovanou standardem IEEE 802.16. Umožňuje přenos dat bez nutnosti přímé viditelnosti na velké vzdálenosti (až desítky kilometrů).

1.3.4 Wireless WAN

Rozsáhlá bezdrátová síť WWAN (Wireless Wide Area Network) – často se označuje jako „širokopásmá síť“. Pokrývá velké oblasti, jako například města, za použití anténních a satelitních systémů udržovaných poskytovateli bezdrátových služeb. Současné WWAN sítě jsou známy jako sítě 2., 3. a 4. generace (2G, 3G, 4G). Od WLAN se zejména liší použitím mobilních sítí, jako GSM (GPRS a EDGE) a novějších UMTS, HSDPA a LTE.

1.4 Standard IEEE 802.15.4

Standard IEEE 802.15.4 vychází ze standardu IEEE 802.15. Celá rodina těchto standardů popisuje komunikaci pro WPAN sítě. Standard IEEE 802.15 je tvořena celkem 7 standardy, popisujícími jednotlivé možnosti bezdrátových sítí. Například nový standard z roku 2011 IEEE 802.15.6 definuje Body Area Network (BAN) technologii, která optimalizuje zařízení pro provoz v lidském těle. Dále bude popsána 4. skupina IEEE 802.15.4.

Standard IEEE 802.15.4 byl navržen pro zařízení s nízkou přenosovou rychlostí a malou spotřebou energií, které jsou schopny na krátkou vzdálenost fungovat několik měsíců, a to napájené pouze bateriemi. Definuje fyzickou vrstvu PHY (Physical layer) a vrstvu přístupu k médiu MAC (Medium Access Control) pro LR-WPAN¹. LR-WPAN je jednoduchá, nízkonákladová síť, která umožňuje komunikaci, kde jsme omezeni výkonem zařízení. Základní charakteristiky sítě:

- unikátní 64 bitová adresace nebo krátká 16 bitová adresa,
- přenos informací pomocí sítě typu hvězda nebo peer-to-peer,
- přenosová rychlost 250 kb/s, 40 kb/s a 20 kb/s,
- vícenásobný přístup pomocí metod předcházení kolizí CSMA-CA a ALOHA,
- nízká spotřeba energie,
- indikátor kvality (LQI²),
- obsahuje 16 kanálů v pásmu 2450 MHz, 10 kanálů v pásmu 915 MHz a 1 kanál v pásmu 868 MHz. (IEEE Computer Society., 2011)

¹ LR-WPAN = Low Rate Wireless Personal Area Network

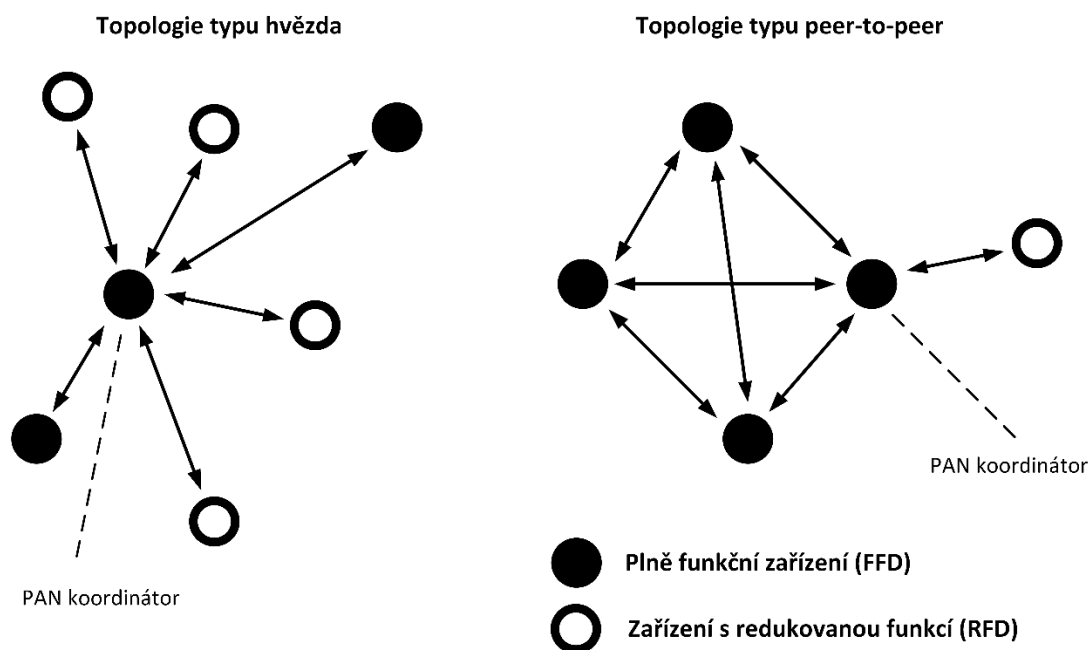
² LQI = Link quality indicator

1.4.1 Prvky sítě WPAN IEEE 802.15.4

Ve standardu IEEE 802.15.4 jsou dva typy zařízení. Plně funkční zařízení FFD³ a zařízení s omezenou funkcí RFD⁴. FFD zařízení je schopné zastupovat úlohu koordinátora sítě, RFD toto nedokáže. RFD je zjednodušené koncové zařízení, které se připojuje k jinému FFD a využívá minimálně hardwarové prostředky. Takové zařízení jsou všechny senzory a spínače. Naopak FFD musí kontrolovat komunikaci a přeposílat zprávy od příchozích FFD nebo RFD zařízení. (IEEE Computer Society., 2011)

1.4.2 Topologie

Standard IEEE 802.15.4 podporuje komunikaci v topologiích: peer-to-peer topologie a hvězdicová topologie.



Obrázek 2 Topologie sítě podle IEEE 802.15.4

Topologie typu hvězda umožňuje komunikaci mezi zařízeními a jedním centrálním prvkem (PAN koordinátor). Všechna zařízení v síti mají unikátní adresu. Zařízení používají rozšířené adresy pro komunikaci bez zásahu PAN koordinátora, nebo zkrácené adresy, které jsou

³ FDD = Full Functional Device

⁴ RFD = Reduced Functional Device

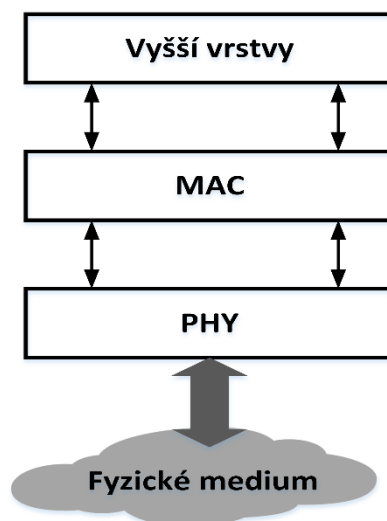
definovány PAN koordinátorem. Koordinátor je většinou napájen přímo ze sítě, zatímco všechna ostatní zařízení mohou být napájena pomocí baterií.

Peer-to-peer topologie má PAN koordinátora. Peer-to-peer topologie umožňuje vytvořit složitější síť typu mesh. Zařízení spolu mohou komunikovat, pokud jsou vzájemně v dosahu. Také mohou posílat zprávy typu multiple hops z jednoho zařízení na druhé. (IEEE Computer Society., 2011)

1.4.3 Architektura IEEE 802.15.4

IEEE 802.15.4 architektura je definována pomocí jednotlivých bloků kvůli zjednodušení standardu. Tyto bloky představují jednotlivé vrstvy. Každá vrstva zodpovídá za jednu část standardu a nabízí služby vyšším vrstvám.

LR-WPAN zařízení obsahuje PHY vrstvu, která obsahuje radiofrekvenční vysílač spolu s jeho kontrolním low-level mechanismem a MAC podvrstvou, která poskytuje přístup k fyzickému médium. Obrázek 3 ukazuje uspořádání jednotlivých vrstev. (IEEE Computer Society., 2011)



Obrázek 3 LR-WPAN architektura

Horní vrstva znázorněna na obrázku 3 představuje síťovou vrstvu, která poskytuje prostředky pro konfiguraci sítě, práci a směrování zpráv. Nad síťovou vrstvou je aplikační vrstva, která poskytuje funkce zařízení. Definice těchto vrstev je mimo rozsah tohoto standardu.

Fyzická vrstva PHY

PHY poskytuje dvě služby: PHY data service a PHY management service. PHY data service umožňuje přenos a příjem datových jednotek PDDUs po fyzickém rádiovém kanálu. PHY vrstva je zodpovědná:

- aktivaci a deaktivaci radiového vysílače,
- detekci energie (ED) na aktuálním kanálu,
- indikaci kvality pro přijímané pakety (LQI),
- detekci kolizí (CSMA-CA),
- výběr frekvenčního kanálu,
- vysílání a přijímání dat. (IEEE Computer Society, 2011)

Rádiové zařízení musí pracovat na jedné z bezlicenčních skupin:

- 868-868,6 MHz Evropa,
- 902-928 MHz Amerika,
- 2400-2483,5 MHz svět.

Vrstva přístupu k mediu MAC

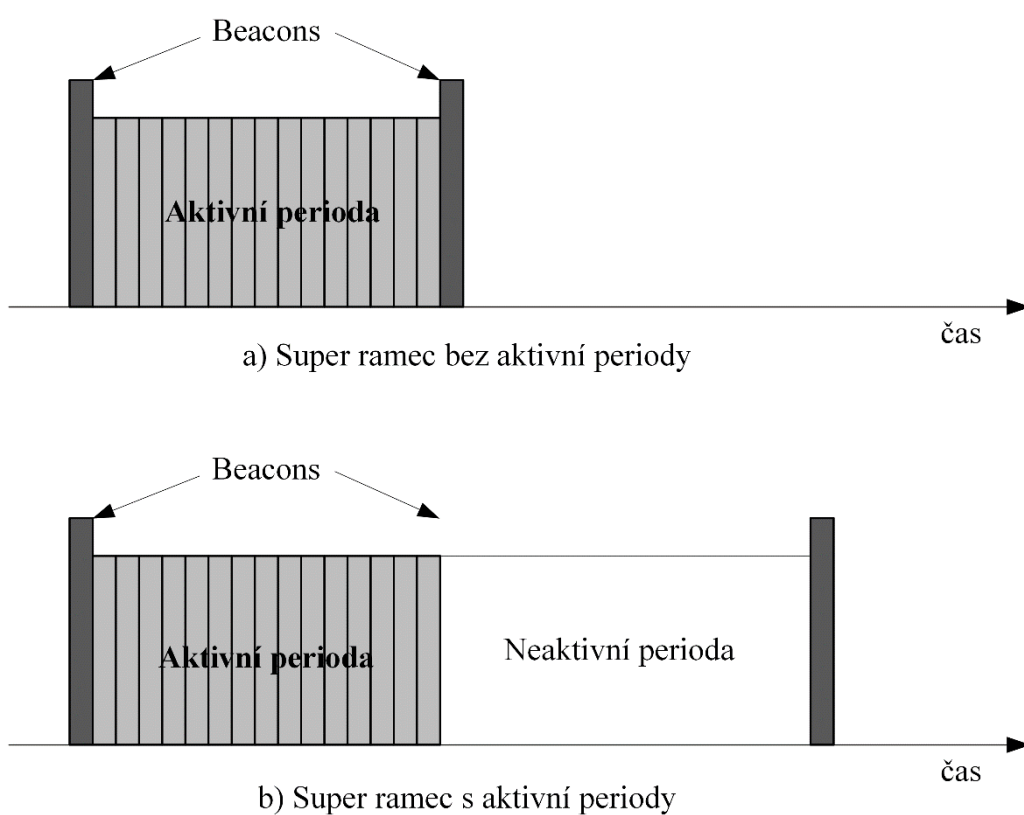
MAC podvrstva poskytuje také dvě služby a to MAC data service a MAC management service interfacing. MAC management service interfacing slouží k řízení entit MLME service access point (SAP), jinak také MLME-SAP⁵. Data service MAC umožňují přenos a příjem datových jednotek MPDUs přes vrstvu PHY data service. MAC podvrstva zpracovává všechny přístupy k fyzickému rádiovému kanálu a je zodpovědný za následující úkoly:

- generování síťových beacons, pokud se jedná o koordinátora,
- synchronizaci beacons,
- podpora PAN asociace a disociace,
- podpora zabezpečení zařízení,
- mechanismus CSMA-CA pro přístup ke kanálu,
- poskytování spolehlivého spojení mezi dvěma MAC objekty. (IEEE Computer Society, 2011)

⁵ MLME-SAP = MAC sublayer management entity service access point

1.4.4 Struktura super rámce

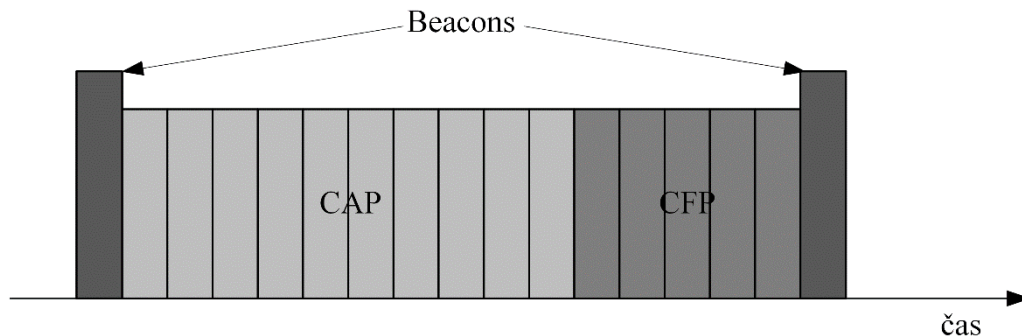
Tento standard umožňuje volitelně použití struktury super rámce (superframe). Formát super rámce je definován koordinátorem. Super rámec je ohraničený síťový beacon posílaný koordinátorem sítě a je rozdělen do 16 slotů stejné délky. Super rámec může mít volitelně aktivní a neaktivní část, jak je znázorněno na obrázku 4. Neaktivní částí se docílí režimu nízké spotřeby (sleep režimu). Přenos beacon rámce začíná na začátku prvního slotu každého super rámce. Pokud koordinátor nebude používat strukturu super rámce, nebudou se posílat beacon rámce. Beacon rámce jsou použity k synchronizaci připojených zařízení, k identifikaci PAN a k popsání struktury super rámce. (IEEE Computer Society., 2011)



Obrázek 4 Struktura super rámce

Jakékoli zařízení, které chce komunikovat v době CAP (contention access period) mezi dvěma beacons soupeří s jiným zařízením pomocí mechanismu CSMA-CA nebo ALOHA. Pro nízkou latenci aplikací nebo aplikací, které vyžadují specifickou šířku pásma, koordinátor přidělí části aktivního super rámce dané aplikaci. Tyto části se v překladu nazývají zaručené časové úseky GTSs (guaranteed time slots). GTSs z contention-free periody (CFP) jsou vždy na konci aktivního super rámce bezprostředně za CAP, jako je zobrazeno na obrázku 5. PAN koordinátor přiděluje až sedm z GTSs a GTS nemá zabírat více než jednu periodu. Nicméně velká část CAP

zůstává pro přístup jiných síťových zařízení nebo nových zařízení, které se chtějí připojit k síti. Veškeré transakce soupeření jsou dokončeny před zahájením CFP. Také všechna zařízení vysílající pomocí GTS zaručují, že jejich transakce skončí před dalším GTS nebo koncem CFP.



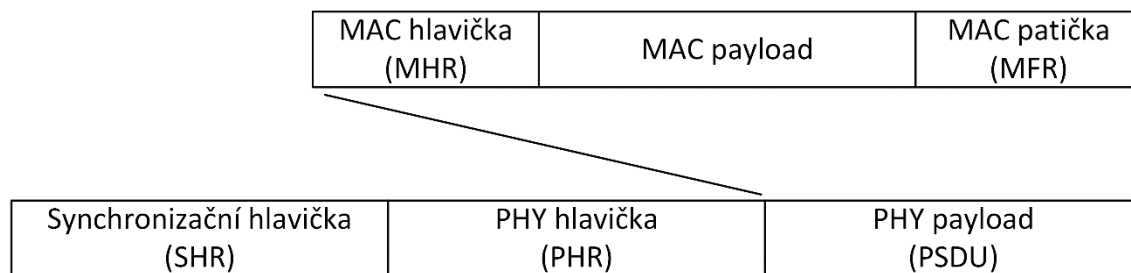
Obrázek 5 Struktura aktivní periody s GTS

1.4.5 Struktura rámce

Standard 802.15.4 definuje čtyři MAC rámce. Struktury rámců jsou navrženy tak, aby bylo dosaženo co nejmenší složitosti a velké robustnosti při přenosu dat na rušném kanálu. (IEEE 805.15.4, 2011)

- **Beacon frame** – rámec používaný koordinátorem pro zasílání beacons. Slouží k synchronizaci zařízení v síti, využívá se ke konfiguraci sítě. Zejména v módu, v němž umožňuje uvádět klientské zařízení do spánkového režimu.
- **Data frame** – rámec sloužící pro přenos všech dat.
- **Acknowledgment frame** – rámec využívaný k potvrzení komunikace.
- **MAC command frame** – slouží pro veškerou konfiguraci, centralizovanou konfiguraci, nastavování a řízení klientských zařízení v síti.

Tyto MAC rámce jsou předávány do PHY vrstvy jako PSDU, kde se stanou PHY payload. PPDU jsou zobrazeny na obrázku 6.



Obrázek 6 Schéma pohledu PPDU

1.5 ZigBee

ZigBee je relativně nová technologie vystavěná na standardu IEEE 802.15.4, který definuje dvě spodní vrstvy. ZigBee definuje vrstvy nad tímto standardem. ZigBee je jednoduchý bezdrátový komunikační standard určený pro tvorbu sítí krátkého dosahu WPAN. Poskytuje cenově nenákladnou, nízko příkonovou, bezdrátovou síť pro použití v průmyslových a senzorových sítích. Snaží se vyplnit mezeru mezi rozšířenými technologiemi jako je WiFi a Bluetooth. Je zde velká skupina zařízení, pro která nejsou Bluetooth a WiFi ideálním řešením.

ZigBee vyvíjí ZigBee Alliance. Jedná se o neziskové sdružení firem, které má přes 450 členů. Vytváří otevřené a globální standardy, které pomáhají definovat IoT pro použití ve spotřebitelských, obchodních a průmyslových odvětvích.

V této práci je technologie ZigBee popsána na obecné úrovni, nezabývá se konkrétními verzemi ZigBee. (Stachowicz, 2011, Koton, 2006, ZigBee Specification , 2012)

1.5.1 Typy zařízení

ZigBee disponuje třemi typy zařízení: koordinátor, router a koncové zařízení. (ZigBee Specification, 2012)

Koordinátor

Jedná se o centrální prvek sítě, přesněji kořen stromu sítě, který umožňuje přemostění do jiné sítě. V každé síti je jeden koordinátor. Je to FFD zařízení, které zodpovídá za celkovou správu sítě (spouští síť, rozhoduje, jakým způsobem jsou přidělovány adresy, dovoluje zařízení opustit či vstoupit do sítě).

Router

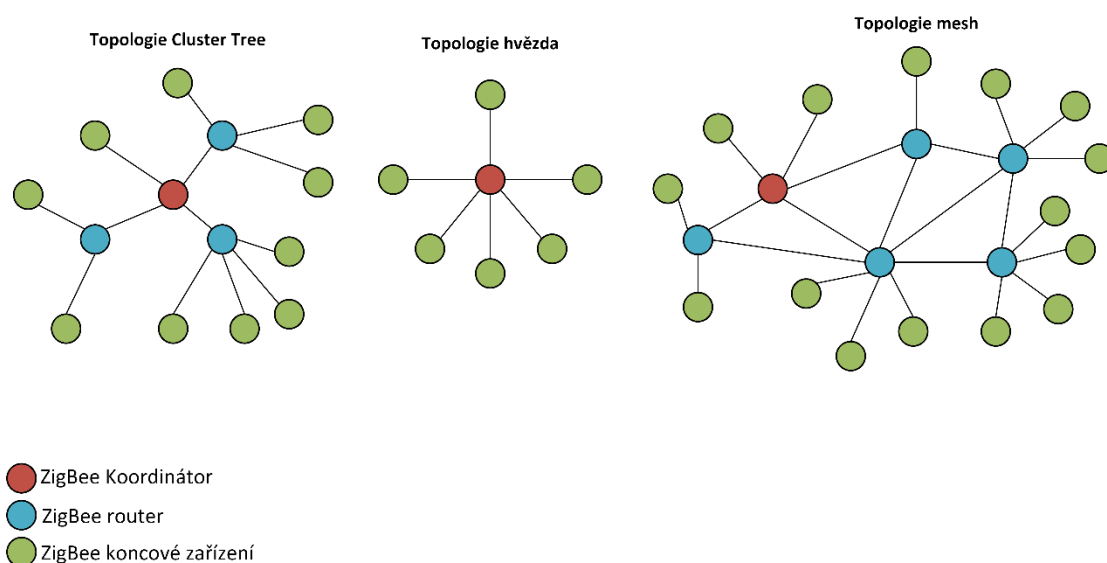
Router neboli směrovač je FFD zařízení. Používá se pro rozšíření sítě. Funkcí směrovače je najít nejlepší cestu k cíli. Má podobné funkce jako koordinátor kromě založení sítě.

Koncové zařízení

Koncové zařízení je RFD, které může být připojeno k routeru nebo koordinátoru. Typicky se jedná o různá čidla a senzory. Mají omezené funkce, což zajišťuje větší výdrž na bateriích.

1.5.2 Topologie

ZigBee podporuje několik topologií zobrazených na obrázku 7. (Stachowicz, 2011, Koton, 2006, ZigBee Specification, 2012)



Obrázek 7 ZigBee topologie

Topologie Star (hvězda)

Topologie hvězda je velmi jednoduchá. Všechna zařízení komunikují přímo s koordinátorem. Sít' je poměrně výkonná, protože většina zařízení použije pouze 2 přeskoky „hopy“ k dosažení cíle. Rovněž je rozložení sítě velmi jednoduché, není třeba složitých směrovacích protokolů. Má to však i své nevýhody. Pokud vypadne koordinátor, přestane fungovat celá sít'. Rozsah je obvykle 30 až 100 m.

Topologie Mesh

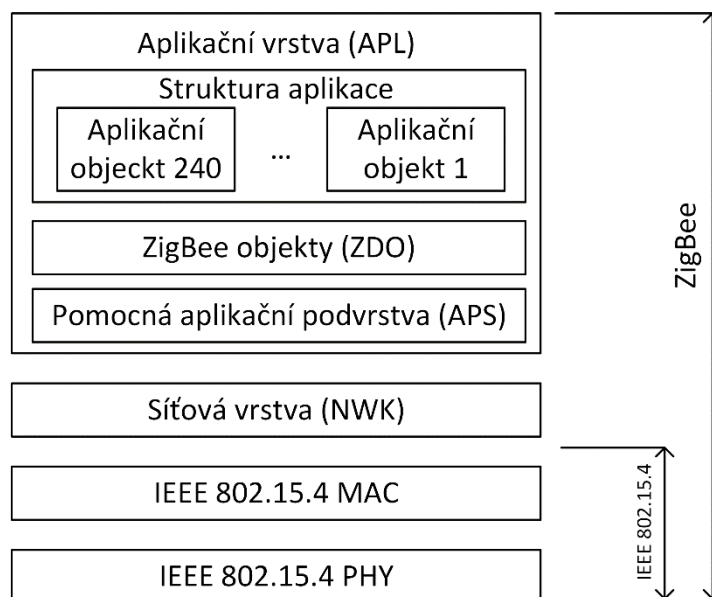
Je to nejužitečnější a nejflexibilnější ZigBee topologie. Směrovače mají alespoň dvě směrovací cesty pro komunikaci s koordinátorem. Směrovač může vybrat nejefektivnější cestu (s co nejmenší cenou) nebo se vyhnout překážkám. Mezi hlavní výhody patří spolehlivost, robustnost a dlouhý dosah (více směrovačů může prodloužit dosah sítě nebo eliminovat místa se slabým signálem). Na druhou stranu směrování zvyšuje režii a latenci. Nevýhodou výkonnějších směrovačů je jejich cena a složitost. (ZigBee Specification, 2012)

Topologie Cluster Tree

Někdy se nazývá jako hybridní, protože je to kombinace topologie hvězda a mesh. Obvykle se však tento typ topologie nepoužívá, protože má příliš nevýhod z ostatních topologií a málo výhod. Vyžaduje směrovače, které jsou složitější, ale stále poskytuje pouze jednu cestu ke koordinátorovi. Také poskytuje větší dosah, než hvězdicová topologie, ale ne tak velký, jako u mesh topologie. (ZigBee Specification, 2012)

1.5.3 Model ZigBee

Referenční model ZigBee je založen na standardu IEEE 802.15.4, který definuje dvě spodní vrstvy modelu. Vrstvy PHY a MAC standardu IEEE 802.15.4 jsou podrobně popsány v kapitole 1.4.3. Nad těmito vrstvami definuje ZigBee Alliance síťovou vrstvu (NWK) a aplikační vrstvu (APL).



Obrázek 8 Referenční model ZigBee

Aplikační vrstva (APL)

Aplikační vrstva obstarává několik funkcí, které pracují společně a poskytují veškeré nezbytné služby pro aplikace. Hlavní složky aplikační vrstvy jsou: ZigBee Device Object (ZDO), Application Framework a Application Support Sub-layer (APS). Úkolem APS je udržování vazebních tabulek, které umožňují propojit dvě zařízení na základě jejich služeb a potřeb. Přeposílá zprávy mezi vzájemně propojenými zařízeními. ZDO jsou umístěny v Application Framework. ZDO je zodpovědný za definování funkce zařízení v síti (router, koordinátor nebo koncové zařízení). (Stachowicz, 2011, Koton, 2006, ZigBee Specification, 2012)

Application support sub-layer (APS) – Jedná se o pomocnou aplikační podvrstvu. Poskytuje rozhraní mezi APL a síťovou vrstvou (NWK) pomocí obecných služeb, které jsou používány objekty aplikací. APS poskytuje služby Application Support Sub-layer Data Entity Service Access Point (APSDE-SAP) a Application Support Sub-layer Management Entity Service Access Point (APSME-SAP). APSDE-SAP zajišťuje službu přenosu dat mezi více zařízeními

na stejné síti a APSME-SAP je zodpovědná za objevování a vázání prostředků a správu databáze APS Information Base (AIB). (Stachowicz, 2011)

Application Framework – V aplikační Framework jsou umístěny jednotlivé aplikační objekty. V tomto prostředí objekty přijímají a vysílají data pomocí APSDE-SAP, které také zahrnuje žádost a potvrzení. Může zde být až 240 aplikačních objektů s koncovým bodem 0 a indexací 1 až 240. Koncový bod 0 se používá pro datové rozhraní ZDO a koncový bod 255 je využíván pro zasílání dat ke všem objektům. (Stachowicz, 2011)

ZigBee device Object (ZDO) – ZDO je zodpovědný za inicializaci APS. Definuje roli zařízení v síti (například koordinátor nebo koncové zařízení), zavádí anebo odpovídá na žádosti o spojení, zřizuje zabezpečené spojení mezi zařízeními sítě a spravuje síť. ZDO používají pro přenos dat APSDE-SAP a pro řízení sítě APSME-SAP. (Stachowicz, 2011)

Network Layer (NWK)

Povinností síťové vrstvy (NWK) je zabezpečení rámců a jejich směrování k cílovým uzlům. Hledá a udržuje směrovače mezi zařízeními, objevuje přímé sousedy. Koordinátor v ZigBee síti je také zodpovědný za spouštění sítě a přidělování adres zařízením. (Stachowicz, 2011)

1.6 6LoWPAN

V současné době je v IoT využito široké škály proprietárních technologií, které stěžují integraci do větších sítí na bázi Internetu. V dokumentu RFC 4919 jsou popsány předpoklady, problémy a cíle 6LoWPAN⁶:

- zařízení založené na IP lze snadno připojit k jiným IP sítím bez nutnosti bran nebo proxy,
- IP sítě umožňují využívat stávající síťové infrastruktury,
- technologie založené na IP již existují, jsou dobře známy a je známo, že fungují,
- otevřené a dostupné specifikace (oproti uzavřeným a komerčním řešením).

Pouze výkonné embedded zařízení by dokázala nativně fungovat v Internetu. Přímá komunikace s IP sítěmi vyžaduje mnoho internetových protokolů, které často vyžadují operační systém. Klasické internetové protokoly jsou pro embedded zařízení náročné a to z těchto důvodů:

Bezpečnost: IPv6 obsahuje volitelnou podporu pro IPSec (IP Security popsanou v RFC 4301), autentizaci a šifrování. Tyto techniky mohou být příliš složité a to zejména pro jednoduchá vestavěná zařízení.

Webové služby: Internetové služby v dnešní době spoléhají na webové služby, zejména TCP, http, SOAP a XML.

Management: Řízení pomocí SNMP (Simple Network Management Protocol), webové služby mohou být často neefektivní a složité.

Frame size: Současné internetové protokoly vyžadují spojení s dostatečnou délkou rámců (pro IPv6 1280 bytů). To může být problém pro nízkoenergetická zařízení.

Tyto požadavky v praxi omezují zařízení v IoT, který musí disponovat výkonným procesorem, operačním systémem s plnou podporou TCP/IP a musí být schopný komunikovat pomocí IP. (Shelby 2009, str. 5) Bezdrátové vestavěné zařízení a sítě pro IoT jsou obzvláště náročné na internetové protokoly:

⁶ 6LoWPAN = IPv6 over Low-Power Wireless Personal Area Networks

Napájení a připojení: U zařízení napájená bateriemi je potřeba zajistit co nejdelší životnost. Toho lze docílit co nejméně častou komunikací a připojením k síti. Avšak základním předpokladem IP je, že zařízení jsou vždy připojená (aktivní).

Mesh topologie: Většina bezdrátových vestavěných sítí používá mesh topologii. Tím dosahují požadovaného pokrytí. Současné IP směrování nemusí být snadno použitelné na tyto sítě.

Šířka pásma a velikost rámce: Nízko-energetické bezdrátové technologie mají obvykle omezenou šířku pásma řádově mezi 20 kbit/s až 250 kbit/s a velikost rámce 40 bajtů až 200 bajtů. U mesh topologií šířka pásma klesá, protože kanál je sdílený a rychle se snižuje více skokovým směrováním. Standard IEEE 802.15.4 má velikost rámců 127 bajtů a minimální velikost rámců IPv6 je 1280 bajtů dle RFC 2460, což vyžaduje použití mechanismu fragmentace.

Spolehlivost: Standardní internetové protokoly nejsou optimalizovány pro bezdrátové sítě s nízkou spotřebou energie. Například TCP není schopné rozlišit pakety, které byly zahozeny kvůli přetížení nebo pakety které se ztratily. (Shelby 2009, str. 6)

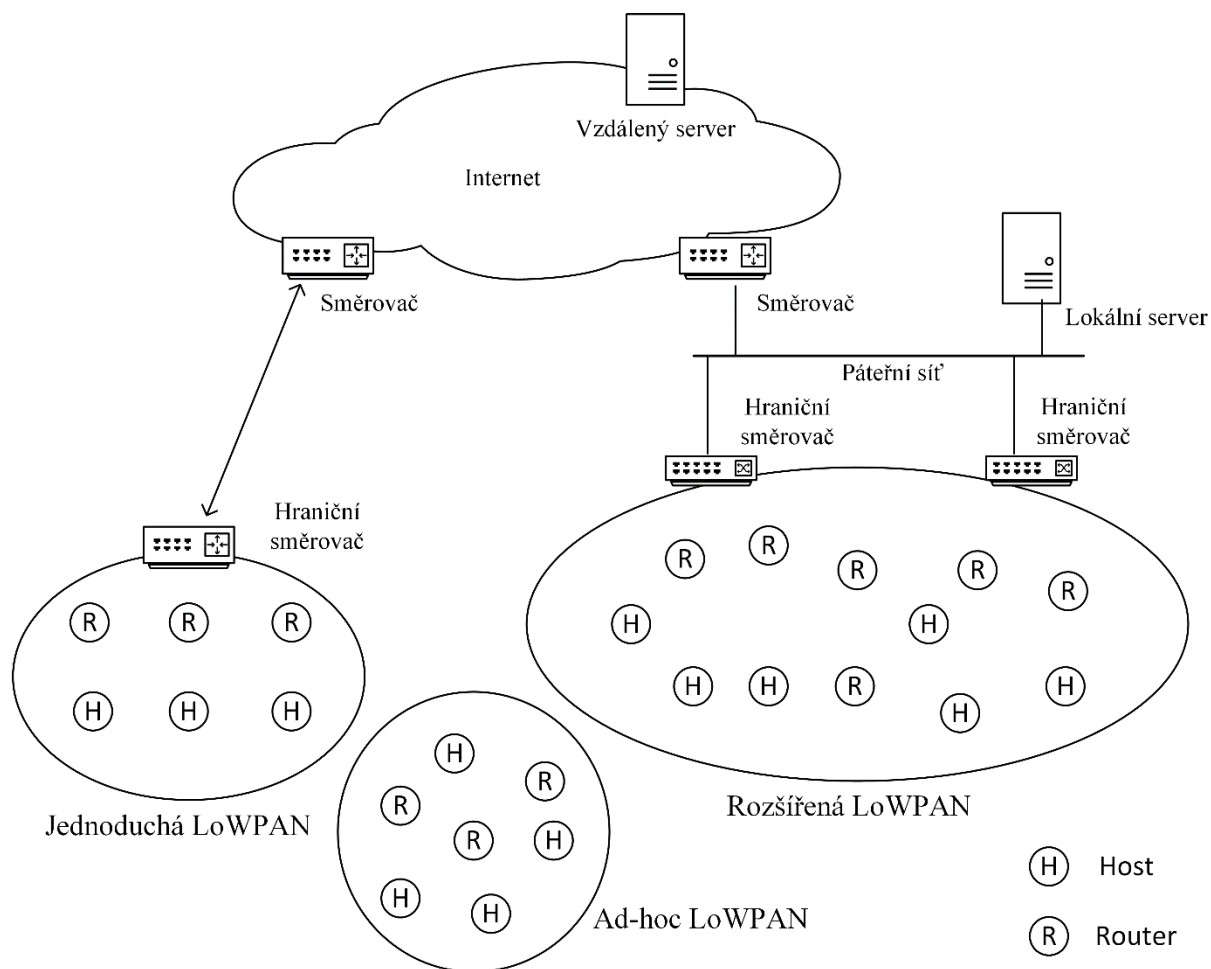
Pracovní skupina IETF⁷ 6LoWPAN byla vytvořena, aby vyřešila tyto problémy a umožnila použití IPv6 v nízko-energeticky náročných bezdrátových sítích. Výsledkem 6LoWPAN je efektivní rozšíření IPv6 v těchto bezdrátových sítích. (Shelby 2009, str. 6)

6LoWPAN je otevřený standard, který je definován pomocí dokumentů RFC 4944, RFC 6282 a RFC 6775. 6LoWPAN pracuje s protokolem IPv6 a slouží pro přenos dat v rámci IEEE 802.15.4.

⁷ IETF = Internet Engineering Task Force

1.6.1 Architektura 6LoWPAN

6LoWPAN sítě jsou propojeny s jinými IP sítěmi prostřednictvím hraničních směrovačů. Hraniční směrovač je velmi důležitý, protože poskytuje komunikaci dovnitř a ven z 6LoWPAN sítě. Hraniční směrovače mají typicky funkce pro správu a jsou zahrnuty do celkové správy sítě. Síť může mít více hraničních směrovačů, pokud mají společnou páteřní síť. (Shelby 2009, str. 13) Na obrázku 9 je ukázka LoWPAN sítí.



Obrázek 9 6LoWPAN architektura

LoWPAN se skládá z uzlů, které mohou představovat hosta nebo směrovač spolu s jedním nebo více hraničními směrovači. Zařízení v síti mají stejný IPv6 prefix, který je distribuován prostřednictvím hraničního směrovače. Aby se usnadnilo fungování sítě, jednotlivá zařízení se registrují u hraničního směrovače. Tato operace je součástí ND (Neighbor Discovery), která je základním mechanismem IPv6. Uzly mohou být ve více sítích zároveň (tzv. multi-homing). Uzly se mohou volně pohybovat po celé síti, mezi hraničními směrovači a dokonce i mezi samotnými sítěmi. Změna topologie může být způsobena podmínkami bezdrátových kanálů,

bez fyzického pohybu. Více hopové mesh topologie v LoWPAN lze dosáhnout buď prostřednictvím směrování na linkové vrstvě (Mesh-Under) nebo s použitím IP směrování (Route-Over). Obě tyto techniky jsou podporovány v 6LoWPAN. (Shelby 2009, str. 14)

Komunikace mezi LoWPAN uzly a IP uzly funguje způsobem end-to-end, stejně jako mezi běžnými IP uzly. Každý uzel v 6LoWPAN je označen na základě jedinečné IPv6 adresy a je schopen odesílat a přijímat IPv6 pakety. Typicky 6LoWPAN podporuje ICMPv6, jako je například ping a používá UDP protokol (User Datagram Protocol).

Hlavní rozdíl mezi jednoduchou 6LoWPAN a rozšířenou 6LoWPAN sítí je existence více hraničních směrovačů, které mají stejný IPv6 prefix. Víceúrovňové 6LoWPAN se mohou navzájem překrývat a to dokonce i na stejném kanálu. Při přesunu uzlu z jedné sítě do druhé se jeho IP adresa mění. Hraniční směrovač je obvykle připojený k internetu přes páteřní síť, nebo pomocí buněčné sítě a DSL. Při nasazení sítě může být výhodnější použít jednoduché sítě na společné páteřní síti a to kvůli lepší správě.

6LoWPAN nevyžaduje ke svému provozu infrastrukturu. Může však používat topologii Ad-hoc. V této topologii musí být jeden směrovač (router) nakonfigurován tak, aby působil jako zjednodušený hraniční směrovač. Ten provádí dvě základní funkce. Generuje unikátní unicast adresu a spravuje tabulku sousedů (ND). Z pohledu LoWPAN sítě typu Ad-hoc funguje stejně jako jednoduchá LoWPAN síť s výjimkou lokálního prefixu IPv6 a absence cesty mimo síť. (Shelby 2009, str. 15)

1.6.2 Model 6LoWPAN

Na obrázku 10 je ukázka porovnání vrstevného modelu 6LoWPAN a typického vrstevného modelu TCP/IP. Model 6LoWPAN je téměř totožný s modelem TCP/IP. 6LoWPAN podporuje pouze protokol IPv6 pro který je připravena malá vrstva, nazývána jako LoWPAN adaptační vrstva. Adaptační vrstva byla definována pro optimální fungování IPv6 přes IEEE 802.15.4. Nejběžnější přenosový protokol u 6LoWPAN je UDP (RFC 768). TCP protokol není běžně v 6LoWPAN používán kvůli výkonosti a komplexnosti. 6LoWPAN dále využívá také protokol ICMPv6 (RFC 4333). Aplikační protokoly jsou často samotné aplikace a to v binárním formátu, i když je čím dál více standardních aplikačních protokolů. (Shelby 2009, str. 16)



Obrázek 10 TCP/IP a 6LoWPAN model

Linková a fyzická vrstva

Linková vrstva a fyzická vrstva IEEE 802.15.4 je popsána v kapitole 1.4.3 Architektura IEEE 802.15.4.

Adaptační vrstva 6LoWPAN

Nejdůležitější vrstvou 6LoWPAN je vrstva adaptační, která je mezi linkovou a síťovou vrstvou. Definuje způsob komunikace pro LoWPAN síť pomocí IPv6, kdy přizpůsobuje IPv6 pakety na rámce pro LoWPAN. Skládá se ze tří částí: komprese hlaviček, fragmentace a směrování z linkové vrstvy na síťovou vrstvu. (Shelby 2009, str. 17)

Síťová vrstva

Stará se o směrování a zajišťuje správu sítě, sestavuje spojení od začátku až po jeho konec. O směrování v 6LoWPAN se starají protokoly Router Over, které se dělí na LOAD, DYMO-LOWA a HiLow. Také obsahuje protokol ICMP (Internet Control Message Protocol). ICMP slouží pro odesílání chybových zpráv. Například oznámení, že požadovaná služba nebo uzel není dostupný, a dále také k dotazům (například ping).

Transportní vrstva

Slouží pro samotný přenos dat. Využívá protokolu UDP (User Datagram Protocol). UDP je nespolehlivý a nespojový protokol, zato poskytuje rychlé a efektivní přenosové služby. Transportní vrstva také zodpovídá za poskytování údajů příslušným procesům aplikací.

Aplikační vrstva

O aplikační vrstvě lze říci, že je to vrstva aplikací. Jsou to programy (procesy), které využívají přenosu dat po síti. Aplikační protokoly používají vždy jen jednu službu.

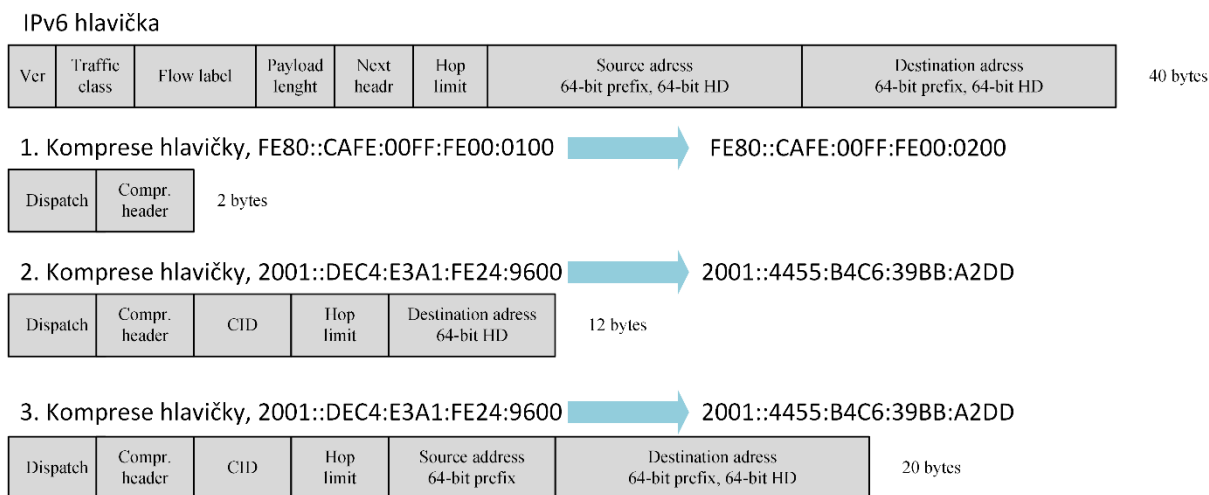
1.6.3 Adaptační vrstva 6LoWPAN

Při odesílání a přijímání dat přes vrstvy MAC a PHY se vždy používá adaptační vrstva. Například RFC 2464 definuje jak je IPv6 paket zapouzdřen v ethernet rámci. Pro 6LoWPAN je to dokument RFC 6282, který definuje, jak je datový rámec IPv6 zapouzdřen přes radiové spojení IEEE 802.15.4. Hlavní záměr pracovní skupiny IETF bylo optimalizovat přenos IPv6 paketů přes nízko-energetické a ztrátové sítě jako je IEEE 802.15.4. Za tímto účelem vznikl dokument RFC 6282. (Hui, 2009, Hui, Culler a Chakrabarti, 2009)

Kompresí hlaviček

Umožňuje kompresi IPv6 hlaviček a UDP hlaviček. Komprimuje 40 bajtů IPv6 a 8 bajtů UDP hlavičky, za předpokladu, že bylo využito běžných atributů hlavičky. Jsou zmenšovány atributy hlavičky, které mohou být odvozeny z linkové vrstvy. Způsob, jakým jsou hlavičky komprimovány, podporuje pouze IPv6, nikoli IPv4. Můžeme si všimnout, že nikde není zakázáno používat protokol TCP, avšak komprese TCP hlavičky v dokumentu RFC 6282 není. (Hui, 2009, Hui, 2009, Hui, Culler a Chakrabarti, 2009)

Standardní komprese IP hlavičky je založena na stavech, které se používají při point-to-point spojení, kde je spojení mezi koncovými body stabilní. Toto řešení je velmi účinné pro statické sítě a stabilní spojení. Komunikace přes více skoků vyžaduje hop-by-hop kompresi a dekompresi. Pro dynamicky měnící se sítě a více skokové sítě jako je 6LoWPAN radiová síť se používá jiná metoda. 6LoWPAN používá bez stavovou kompresi se sdílením kontextu, která nevyžaduje žádné stavy a nechá směrovací protokoly dynamicky vybírat trasu bez ovlivnění kompresního poměru. Na obrázku 11 jsou uvedeny 3 příklady komprese. (Hui, 2009, Hui, Culler a Chakrabarti, 2009)



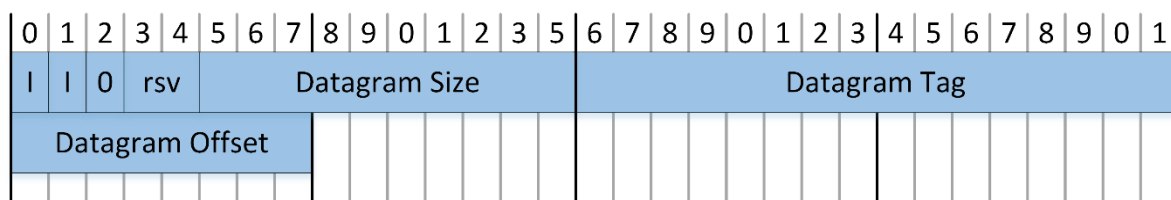
Obrázek 11 Příklad komprese IPv6 hlaviček 6LoWPAN (Hui, Culler a Chakrabarti, 2009)

1. Příklad komunikace mezi dvěma zařízeními uvnitř stejné 6LoWPAN sítě pomocí lokální adresy. Hlavička IPv6 může být komprimována pouze na 2 bajty.
2. Komunikace zařízení mimo síť 6LoWPAN síť. Je znám prefix externí sítě a IPv6 hlavička může být komprimována na 12 bajtů.
3. Úplně stejný případ jako příklad 2, jen bez znalosti prefixu externího zařízení. IPv6 hlavička lze komprimovat na 20 bajtů.

Fragmentace

Fragmentace je důležitá pro přenos rámců IPv6 přes IEEE 802.15.4 spojení. Používá se, když je určitý objem dat tak velký, že se nevejde do jednoho IEEE 802.15.4 rámce, pak je nutné rozdělit rámce IPv6 na několik menších segmentů. Fragmentace obsahuje tři části: (Hui, Culler a Chakrabarti, 2009)

- Datagram Size – určuje celkovou velikost nefragmentovaného užitečného objemu dat. Je součástí každého fragmentu a má za úkol zjednodušovat přidělování vyrovnávací paměti v přijímači, když dojde k přerušení fragmentace.
- Datagram Tag – slouží pro identifikaci množiny fragmentů, které obsahují stejné části daného objemu dat. Také se používá k porovnání stejných obsahů dat.
- Datagram Offset – identifikuje fragmenty offsetu v rámci nefragmentovaného užitečného objemu dat a je udáván pomocí 8 bitů. Pokud by byla povolena libovolná velikost bitu offsetu, vyžadovalo by se pro minimální velikost MTU 1280 bajtů 11 bitů.

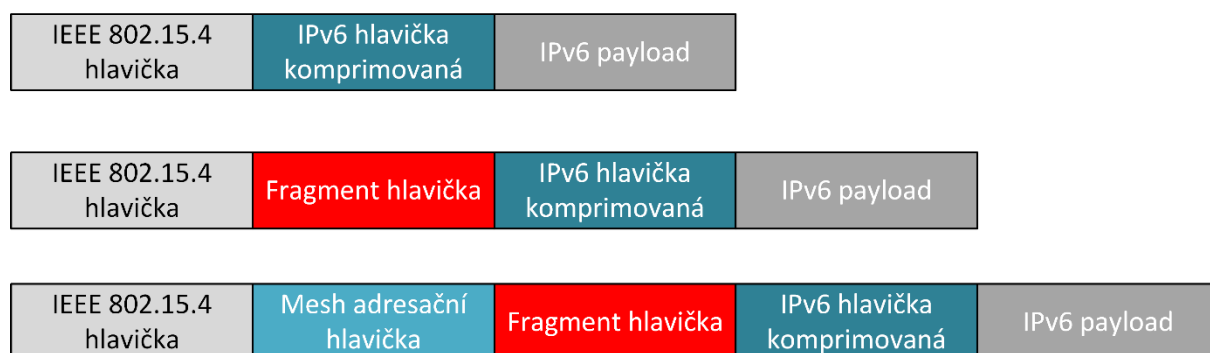


Obrázek 12 6LoWPAN fragment hlavička

Formát fragmentovaného záhlaví je ukázán na obrázku 12. První dva bity určují typ záhlaví. Třetí bit je využíván ke kompresi datagramu a první fragment obsahuje vždy nulu. Hlavička prvního fragmentu je 4 bity, následující fragmenty mají hlavičku 5 bitů. (Hui, Culler a Chakrabarti, 2009)

Formát hlavičky 6LoWPAN

6LoWPAN používá skládané hlavičky analogicky jako IPv6. Hlavička 6LoWPAN definuje schopnost každé další sub-hlavičky. Jsou definovány celkem tři sub-hlavičky: mesh adresní, fragmentovaná a komprimovaná hlavička. Mesh adresování podporuje směrování na druhé vrstvě a fragmentace podporuje přenos IPv6 MTU. Formát hlavičky je definován pomocí typu pole hlavičky, které je umístěno na začátku každé hlavičky. Hlavičky lze snadno rozložit. Tím je umožněno odstranění sub-hlavičky, která není potřeba. Hlavička typu fragmentace umožňuje zmenšovat pakety, aby se vešly do IEEE 802.15.4 rámce. Mesh hlavička se nepoužívá při posílání dat přes jeden skok (hop). (Hui, Culler a Chakrabarti, 2009)



Obrázek 13 6LoWPAN složení hlavičky (Hui, 2009)

1.6.4 IPv6

Každá věc v IoT musí být nějakým způsobem jednoznačně identifikovatelná, adresovatelná. Tím vzniká otázka, jakou adresaci zvolit. Pokud zvolíme adresaci pomocí IP (Internet Protokol) adres musíme zvážit, jakou verzi IP použijeme. Podle odhadů lze předpokládat, že v roce 2020 bude připojeno k internetu 20 miliard chytrých zařízení (van der Meulen, 2015). To jsou přibližně 3 chytrá zařízení na každého člověka. Toto neuvěřitelné číslo má překročit součet počítačů, mobilních telefonů a tabletů po celém světě. Některé odhady polemizují i o 200 miliardách zařízení (A Guide to the Internet of Things Infographic, 2015). Z toho plyne problém omezené adresace zařízení pomocí IPv4. Internet protokol IPv4 je schopný adresovat pomocí adresního prostoru 2^{32} , teoreticky disponuje tedy 4 miliardami adres. Pokud porovnáme očekávaný růst zařízení a možnosti IPv4, je zřejmé, že počet zařízení v roce 2020 několika násobně překročí možnosti IPv4. Již v dnešní době je problém s nedostatkem IPv4 adres. Samozřejmě, že ne všechna zařízení budou adresována veřejnými adresami. Bude záležet na zvoleném standardu na použité technologii a na okolí, ve kterém budou zařízení nasazena. Některé firmy a velké fabriky využijí privátní sítě z důvodu zvýšení bezpečnosti a vybudují si svoji chytrou síť. V opačném případě, mohou být adresy řešeny pomocí IPv6 nebo jinou technologií.

Internet protokol IPv6 je nástupcem protokolu IPv4. Snaží se vyřešit nejvýznamnější problém, který rozvoj internetu způsobil (rostoucí počet zařízení), a poskytnout platformu pro další jeho vývoj. Částečně se to daří, ale přechod z IPv4 na IPv6 jde relativně pomalu.

Jeho kořeny sahají do začátku devadesátých let, kdy začalo být zjevné, že se adresní prostor IPv4 tenčí. Do roku 1996 vzniklo několik RFC dokumentů definujících IPv6. Asi největší podíl na jeho vzniku mají pánové S. Deering a R. Hinden. Vydali sadu RFC dokumentů, definujících IPv6. Ten nejpodstatnější je RFC 2460 dokument, který definuje specifikace IPv6. Existuje celá řada dalších dokumentů definujících doprovodné mechanismy a protokoly. Vyznat se v nich však nemusí být vůbec snadné. Jednotlivé dokumenty mají různý stupeň závaznosti pro implementaci. Z toho důvodu vznikl RFC 6434, které shrnuje požadavky na každé zařízení zapojené do IPv6.

U vzniku IPv6 byly definovány následující požadavky:

- Rozsáhlý adresní prostor, který vystačí pokud možno navždy,
- tři druhy adres: individuální (unicast), skupinové (multicast) a výběrové (anycast),

- jednotné adresní schéma pro Internet i vnitřní síť,
- zvýšení zabezpečení pomocí různých mechanismů IPv6 pro šifrování, autentizaci a sledování cesty k odesilateli,
- automatická konfigurace,
- hladký a plynulý přechod z IPv4 na IPv6. (Satraba, 2011, str. 17)

Internet protokol IPv6 používá délku adresy 128 bitů. To je čtyřnásobek délky IPv4. K dispozici je tedy $3,4 \cdot 10^{38}$ adres. Pro představu: na jeden čtvereční milimetr zemského povrchu připadá $667 \cdot 10^{15}$ adres. To představuje neskutečné číslo řádově miliony miliard. S tím by si měl svět dlouhou dobu vystačit.

IPv6 poskytuje tři druhy adres.

- **Individuální (unicast)** – každá z nich identifikuje jedno síťové rozhraní a data mají být doručena právě tomuto rozhraní.
- **Skupinové (multicast)** – slouží pro adresování skupin počítačů či jiných zařízení. Pokud někdo odešle data na takovou adresu, musí být dopravena všem členům skupiny.
- **Výběrové (anycast)** – je to nový způsob adresace a nejzajímavější přírůstek v IPv6. Tyto adresy označují celou skupinu, data se však doručí jedinému členovi, které je nejbližší. (Satraba, 2011, str. 56)

Oproti IPv4 zmizeli všesměrové adresy (broadcast). Broadcast není potřeba, protože jeho funkci nahradily skupinové adresy.

Adresování

IPv6 adresy se zapisují pomocí osmi skupin po čtyřech číslicích šestnáctkové soustavy. Navzájem se oddělují dvojtečkami. Příklad IPv6 adresy je:

2001:0db8:7654:3210:fedc:ba98:7654:3210.

Adresy je možné zkracovat. Je poměrně časté, že adresy obsahují nuly. Zkracování lze provést dvěma způsoby. Místo „0000“ lze zapsat jen „0“. Vyskytují se i adresy, kdy se dokonce vyskytuje několik nulových skupin za sebou. Ty můžeme zkrátit pomocí dvou dvojteček „::“.

1.7 Jiné technologie

1.7.1 LoRa

LoRa Alliance je otevřené neziskové sdružení členů, kteří věří, že začíná éra IoT. Hlavním důvodem vzniku LoRa Alliance je snaha standardizovat nízkoenergetické WAN (LPWAN). Členové aliance jsou rozmístěni po celém světě a spolupracují spolu, aby IoT, machine-to-machine (M2M), inteligentní města a průmyslové aplikace standardizovali pomocí protokolu LoRaWAN. (LoRaWAN™ What is it?, 2015)

LoRaWAN je specifikace pro nízkoenergetické sítě WAN (LPWAN). Specifikace slouží pro provoz bezdrátových bateriových zařízení (věcí), která fungují na regionální, národní nebo globální síti. Řeší klíčové požadavky IoT jako je zabezpečení obousměrné komunikace a mobilita. Tato specifikace poskytuje snadný provoz chytrých věcí bez potřeby budování komplexních sítí, dává uživatelům a vývojářům svobodu, umožňuje firmám vybudování IoT.

Síťová architektura LoRaWAN je obvykle postavena na topologii star-of-stars, v níž brány (gateways) fungují jako most pro předávání zpráv mezi koncovými zařízeními a centrálním síťovým serverem. Brány jsou připojeny k síťovému serveru pomocí standardního IP spojení, zatímco koncová zařízení používají single-hop bezdrátovou komunikaci pro jednu nebo více bran. Všechna koncová zařízení obecně komunikují obousměrně, ale také podporují provoz multicast (umožňuje aktualizaci softwaru nebo distribuci hromadných zpráv). (LoRaWAN™ What is it?, 2015)

Komunikace mezi koncovým zařízením a bránou je rozdělena mezi různé frekvence kanálů a přenosové rychlosti dat. Přenosová rychlost dat je kompromisem mezi komunikačním dosahem a délkou zprávy. Rychlost přenosu dat se pohybuje v rozmezí od 0,3 kbps do 50kbps. Síťový server řídí přenosovou rychlost a RF výstup pro každé koncové zařízení individuálně prostřednictvím systému adaptivní rychlosti přenosu dat (ADR), tím maximalizuje životnost baterií v koncových zařízeních. (LoRaWAN™ What is it?, 2015)

1.7.2 Z-Wave

Z-Wave je proprietární bezdrátový komunikační protokol navržený pro domácí automatizaci, který je mezinárodně standardizován. Specifikuje možnosti pro vzdálené ovládání v domácnostech a v komerčním prostředí. Technologie používá nízko-energetických RF radio embedded v domácí elektronice a systémech, jako je osvětlení, termostaty, čidla, klimatizace, ovládání audio či videotechniky a zabezpečení domácností. Jeho hlavní výhody spočívají v mobilitě a možnosti propojení zařízení různých výrobců. (About Z-Wave, 2015)

Zařízení Z-Wave mají minimální spotřebu energie. Z-Wave používají topologii sítě typu Mesh, kde každé zařízení dokáže přijímat i vysílat řídicí příkazy a je zároveň i opakovač, který dokáže šířit signál dál. Každý prvek sítě je schopný sledovat a řídit práci ostatních modulů a také komunikovat s centrálním prvkem. Tato vlastnost dává možnost zařízením pracovat ve skupině nebo samostatně. Také umožňuje zapojení tzv. plug & play. Přidání nového prvku do systému je pak velmi snadné. V otevřeném prostoru je dosah až 100 metrů. Komunikace probíhá v pásmu 900MHz. Z-Wave je zahrnuta v ITU (International Telecommunications Union) G. 9959 standardu, který obsahuje vrstvy Z-Wave PHY a MAC a definuje sadu pokynů pro úzkopásmová bezdrátová zařízení. Z-Wave dokáže připojit až 232 zařízení, což je ideální pro domácí použití nebo malé firmy. (About Z-Wave, 2015)

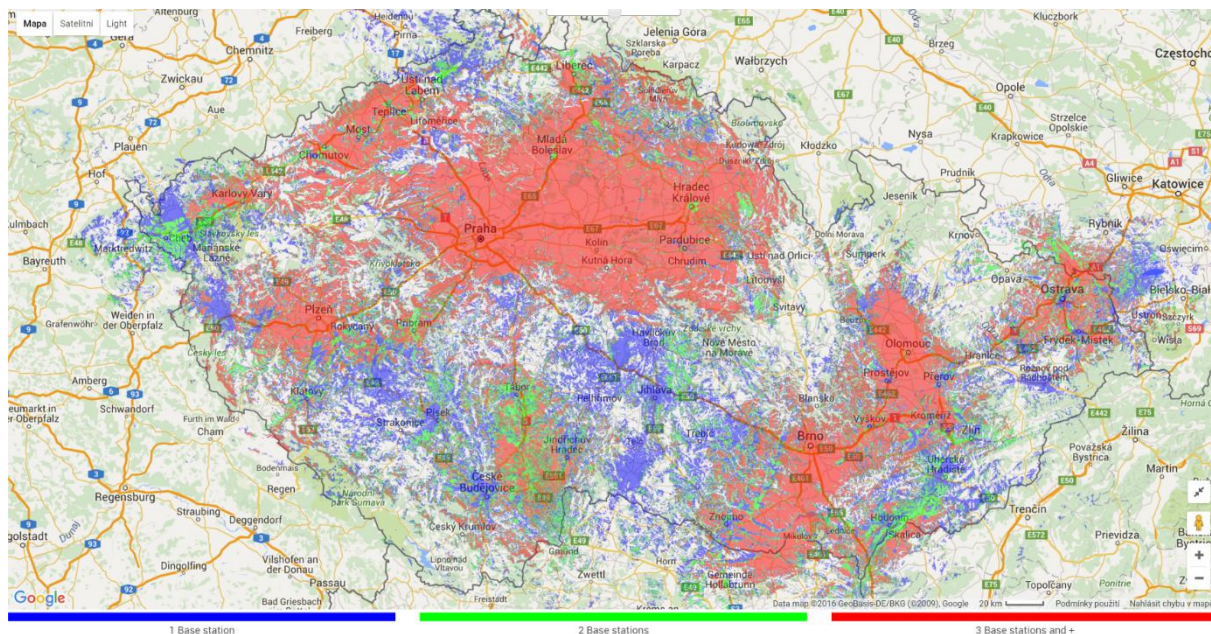
1.7.3 SIGFOX

Technologie SIGFOX je od počátku budována pro IoT. Využívá bezlicenční pásmo 868Mhz, stejně jako ČRa. Umožňuje IoT zařízením komunikovat levně, bezpečně a na velké vzdálenosti při minimální spotřebě energie. SIGFOX se používá pro odečty vody, elektřiny, plynu a také pro parkovací senzory, SmartCity, zabezpečovací zařízení, sledování teploty, měření srážek a průtoků na řekách. (Technologie SIGFOX, 2016)

SIGFOX se snaží koncipovat modemy tak, aby jejich výroba byla co nejlevnější a rozměry co nejmenší. Jedna základnová stanice je schopna přijmout až 9 milionů zpráv denně.

Zařízení se SIGFOX vydrží fungovat na baterii 5 až 15 let, oproti měsíční výdrži zařízení s využitím GSM nebo Wi-Fi. SIGFOX je odolný vůči rušení. Každá zpráva je vysílána třikrát na náhodné frekvenci a přijímána všemi základnovými stanicemi v okolí.

Velikost zprávy může mít velikost 0-12 bajtů, doba přenosu a zpracování trvá 4-6 sekund, denně lze poslat 144 zpráv. Dosah SIGFOX je až 50 km v terénu a 3km v městech. (Technologie SIGFOX, 2016)



Obrázek 14 SIGFOX mapa pokrytí (Technologie SIGFOX, 2016)

2 Analýza bezpečnostních rizik

Nová „éra“ Internetu věcí přináší řadu výhod i nevýhod. K internetu lze připojit stále více věcí a zařízení, ke kterým se dá vzdáleně připojit a ovládat je. Všechny věci od chytrých ledniček, televizorů až po různé senzory jsou připojeny do internetu a vzájemně spolupracují, přičemž všechna tato zařízení mají usnadnit lidem život. Tato zařízení generují ohromnou spoustu dat a informací, mohou mít také přístup k velmi citlivým a osobním informacím jakou jsou například čísla bankovních účtů. I nezabezpečená IP kamera je velmi nebezpečná z pohledu bezpečnosti soukromí.

IoT je rychle se vyvíjející obor, který se rozšiřuje do všech oblastí života. Zařízení pro IoT exponenciálně přibývá. Společnost Gartner odhaduje, že v roce 2016 bude po celém světě kolem 6 miliard zařízení (věcí) pro IoT, což je o 30 % více než v roce 2015. Dokonce odhady mluví až o 20,8 miliard zařízení v roce 2020. (van der Maulen, 2015) Zařízení IoT jsou na nejlepší cestě stát se početnější a všudypřítomnou skupinou zařízení, než mobilní telefony a počítače. Vzhledem k tomuto faktu, vzniká velké bezpečnostní riziko a ohrožení pro tyto zařízení. IoT vytváří úročníkům nové možnosti útoků. Nemusí se jednat přímo o proniknutí do systému a jeho zneužití. Stačí i získání pouhého přístupu ke čtení dat či odposlouchávání. To vše představuje velkou výzvu pro firmy a podniky, které se zabývají bezpečností a IoT, aby vytvořili bezpečný IoT.

Mnoho zařízení sbírá nějakou formou osobní údaje jako je jméno, adresa, datum narození i čísla kreditních karet. To přináší obavy ze zneužití těchto informací. Obavy se zvyšují, když k těmto zařízením přidáme cloudové služby a mobilní aplikace. Mnoho zařízení pracuje s těmito údaji v nešifrované formě na domácích sítích. Pro uživatele stačí jedna špatně nakonfigurovaná síť a doslova poskytuje všechny tyto informace celému světu. (Internet of things research study, 2015)

Firma Hewlett-Packard provedla v roce 2015 zajímavou studii na zranitelnost zařízení v IoT: (Internet of things research study, 2015)

- 90 procent ze všech shromážděných zařízení obsahuje alespoň jeden z osobních údajů,
- 70 procent zařízení používá nešifrované síťové služby,
- 80 procent zařízení s využitím cloudových a mobilních aplikačních komponent nepožadovalo hesla s dostatečnou složitostí a délkou,
- 70 procent zařízení umožnilo útočníkovi identifikovat platný uživatelský účet pomocí výčtu účtu (account enumeration),
- 6 zařízení z 10, která poskytují uživatelské rozhraní, byla zranitelná na velký rozsah chyb, jako je XSS (Cross-site scripting) a slabé ověření.

Útočník může využít zranitelností, jako jsou slabá hesla, nezabezpečená obnova hesla, špatně zabezpečené ověření k přístupu zařízení. Většina zařízení s jejich cloudovými a mobilními komponenty nepožadovala dostatečnou složitost a délku hesel. Na většině těchto zařízení a služeb šla použít hesla jako „1234“ nebo „123456“. Další alarmující výsledek přinesl výzkum HP při aktualizaci softwaru zařízení. Přes 60 % zařízení stahovalo aktualizace bez využití šifrování nebo jiné ochrany, přičemž aktualizací soubory nebyly nijak chráněny. Ve skutečnosti by mohlo dojít k zachycení této komunikace útočníkem. Útočník této slabiny může využít tak, že získá aktualizaci, kterou může zkoumat a upravit. Pak tuto upravenou aktualizaci může podvrhnout jako skutečnou aktualizaci. (Internet of things research study, 2015)

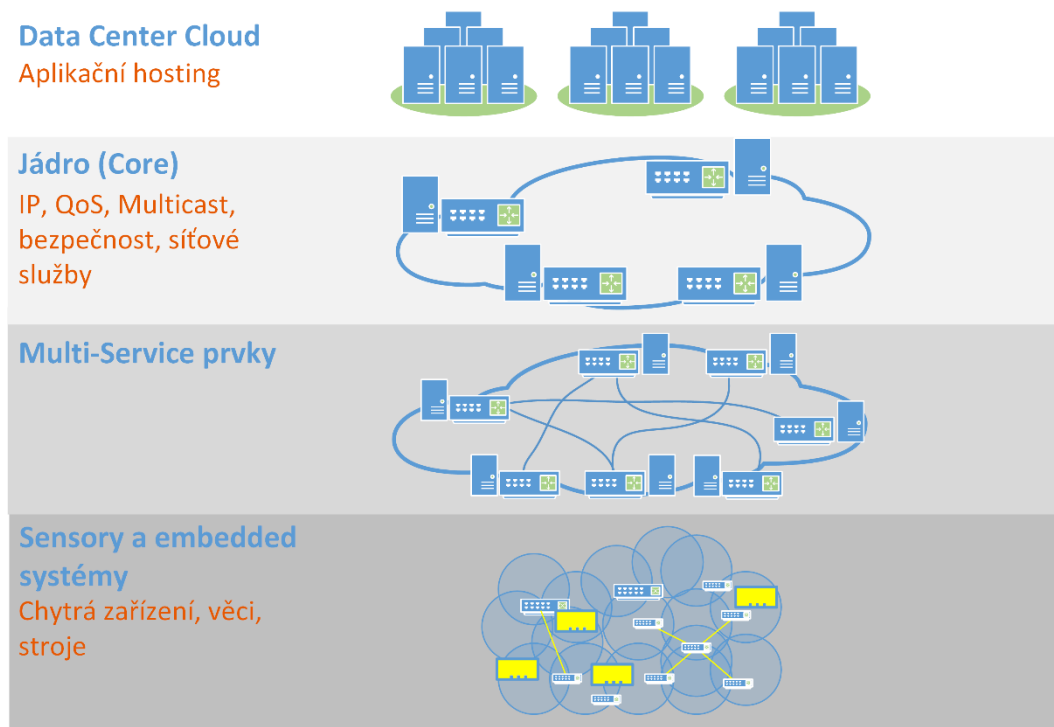
2.1 Bezpečnostní rizika

Bezpečnost je velmi rozsáhlá problematika, která zasahuje do širokého spektra oborů. V případě IoT můžeme uvažovat o bezpečnosti dat koncových zařízení, centrálních prvků, serverů, databází, webových služeb, komunikace, infrastruktury sítě. IoT je velmi různorodý, zejména v použitých technologiích, ale i v samotném použití. Tím se může lišit i samotný pohled na zabezpečení IoT a důsledky provedených útoků. V případě využití IoT v chytrých domácnostech budou nároky na zabezpečení jiné, než při využití IoT ve výrobních fabrikách či zdravotnictví. Pokud útočník napadne chytrou domácnost, s nadsázkou může ovládat osvětlení a topení nebo se může zmocnit citlivých údajů. To je velmi závažné bezpečnostní riziko. Ve firemním prostředí mohou být bezpečnostní rizika mnohem závažnější. Situaci také komplikuje heterogennost zařízení a technologií.

Bezpečnost představuje velmi důležitý stavební kámen pro IoT. Proto je nezbytné, aby výrobci a projekty zaměřené na IoT řešili bezpečnost a ochranu soukromí prioritně. Základem pro zabezpečení by mohli být identifikační mechanismy a funkce, které by zaručily bezpečnost uživatelských dat, soukromí a integritu, autentizaci uživatele a důvěryhodnost systému.

Zabezpečení dat můžeme rozdělit na dvě kategorie. Jednou je ochrana dat na samotném úložišti a další je ochrana dat na komunikační úrovni. Ochrana dat na komunikační úrovni je jedním z hlavních oblastí výzkumu v IoT. (Vermesan a Friess, 2013) Mnoho komunikačních protokolů poskytuje zabezpečení na vysoké úrovni. Hlavním problémem je však jejich nasazení z pohledu požadovaného hardwaru a softwaru, který by umožňoval spuštění bezpečnostních algoritmů efektivním a bezpečným způsobem.

IoT architekturu můžeme rozložit na vrstvy. Každá vrstva je definována její funkcí a také zařízeními, které jsou v této vrstvě používány. Existuje však spousta různých názorů o počtu vrstev IoT. Nicméně podle výzkumů IoT se nejvíce uvádí tři nebo čtyři vrstvy. Cisco uvádí 4vrstvou architekturu. (Securing the Internet of Things, 2015)



Obrázek 15 IoT síťová architektura (Securing the Internet of Things, 2015)

Vrstva senzorů

Skládá se z vestavených systémů, čidel, senzorů a akčních členů. Většinou se jedná o malé jednoúčelové přístroje s různými operačními systémy, typy CPU a paměťmi. U těchto zařízení se očekává co nejnižší cena. Může se jednat o snímače teploty či tlaku. Mohou být umístěny na odlehlých či nepřístupných místech, kde je lidský zásah téměř nemožný. (Securing the Internet of Things, 2015)

Vrstva Multi-services hran

Variabilita koncových zařízení v senzorové vrstvě a jejich potenciálně obrovské množství má vliv na multi-services vrstvu. Vrstva podporuje bezdrátové i pevné připojení. Dokonce i uvnitř této vrstvy musí být podpora několika různých protokolů, jako jsou například ZigBee, IEEE 802.11, 3G a 4G. (Securing the Internet of Things, 2015)

Páteřní vrstva (Core)

Tato vrstva je velmi podobná architektuře v klasických sítích. Funkcí této vrstvy je poskytování cesty pro výměnu dat a síťových informací mezi více podsítěmi. Hlavní rozdíl mezi IoT vrstvou a klasickou vrstvou je její provoz. Samotný provoz vrstvy a data mohou být různá. Například unikátní protokol a variabilní velikost paketů. Bezpečnostní služby na páteřní síti IoT musí být robustní, aby dokázaly chránit síť před hrozbami, jako jsou: MITM (Man-in-the-middle), spoofing. (Securing the Internet of Things, 2015)

Data Cloud vrstva

Architektura této vrstvy je také podobná architektuře, která se používá u běžných sítí. Funkcí této vrstvy je hostování aplikací, které jsou kritické při zajišťování služeb a správě end-to-end architektury IoT. Opět platí, že je velmi důležité tuto vrstvu dostatečně zabezpečit před možnými útoky typu: DOS/DDOS, Buffer overflow, zneužití koncového prvku. (Securing the Internet of Things, 2015)

Základem pro IoT je IPv6 z důvodů, které byly popsány v předešlých kapitolách. IPv6 podléhá stejným hrozbám, jako známe na IPv4. Příkladem mohou být útoky jako smurfing, spoofing, odposlouchávání, útoky typu MITM a další. Z toho důvodu je potřeba zabezpečit pátevní vrstvu architektury před možnými útoky, které existují dnes pro IPv4.

IoT však otevírá zcela novou dimenzi bezpečnosti. Je to místo, kde se setkává internet (digitální svět) s fyzickým světem. To má vážné dopady na bezpečnost. Hrozby útoků se mohou přenést do reálného života (jinými slovy z digitálního světa do fyzického světa). Důsledkem toho se mohou dramaticky rozšířit známé útoky na nové. Mnoho uzavřených operačních systémů (např. SCADA, Modbus, CIP) se orientuje do systémů založených na IP, což také značně zvyšuje bezpečnostní rizika. (Securing the Internet of Things, 2015)

IoT může být zneužit různými kategoriemi bezpečnostních hrozeb včetně:

- běžných červů a virů přeskakujících z ICT do IoT, zejména pro věci běžících na operačních systémech Windows, Linux, iOS, Android,
- „Script kiddies“ nebo jiní útočníci: nezabezpečené webové kamery, krádeže dat, vniknutí do centrálního systému domu,
- Cyber terosismus: útoky na jaderné elektrárny (virus Stuxnet), elektrické rozvodné sítě, monitoring kritické infrastruktury (železnice, doprava).

IoT začíná ovlivňovat naše každodenní životy, ať už v průmyslu, dopravě, chytrých sítí nebo ve zdravotnictví. Proto je nutné zajistit jeho bezpečnost. S rychlým vývojem IoT a jeho rozšiřováním rostou také hrozby útoků, které budou i nadále růst v počtu a budou stále sofistikovanější a propracovanější. Rozsah a možnosti IoT vytváří cíle pro ty, kteří by chtěli poškodit nebo ublížit společnostem, organizacím, národům nebo lidem. Potencionální následky těchto útoků mohou způsobit malé škody v podobě nefunkční chytré žárovky nebo také obrovské škody na elektrické infrastruktuře. V krajním případě může dojít k ohrožení lidských životů, například při výbuchu jaderné elektrárny. (Securing the Internet of Things, 2015)

Ačkoliv mohou být hrozby v IoT podobné hrozbám v tradičním prostředí internetu, celkový dopad by mohl být výrazně odlišný. To je hlavním důvodem, proč se komunity pracující na IoT zaměřují na analýzu hrozeb a jejich řešení.

Jedním ze základních prvků pro zajištění bezpečnosti IoT je identita a mechanismus, který ji dokáže ověřit. Jak již bylo zmíněno, mnoho zařízení v IoT nemá potřebný výpočetní výkon a paměť, aby mohla podporovat aktuální autentizační protokoly. Dnes se používá silné šifrování

a autentizační mechanismy založené na kryptografickém aparátu jako AES (Advanced Encryption Suite) sloužící pro důvěryhodný přenos dat, RSA (Rivest-Shamir-Adleman) digitální klíče a jejich přenos. Z tohoto důvodu musí být autentizace a autorizace přizpůsobena i pro tato zařízení a věci.

Za další prvky v oblasti bezpečnosti můžeme považovat umístění a stupeň ochrany dat, silnou identifikaci, zlepšení ostatních síťových služeb jako je DNS, DNSEC a DHCP a přijetí protokolů, které jsou tolerantní ke zpoždění. (Securing the Internet of Things, 2015)

Mnohé z bezpečnostních úvah o IoT spoléhají na protokoly, které využívají šifrování. Pro senzory a zařízení v IoT může vzniknout otázka, v jakém časovém horizontu dokáží pracovat zařízení v IoT spolu s tímto řešením. Například zařízení pro měření spotřeby energie v domácnosti může fungovat 20 let, ale jak dlouho vydrží šifrovací protokol, aby byl bezpečný?

Obava o ochranu soukromí byla i u vzniku Internetu. S příchodem IoT se tento problém stává ještě komplikovanější, protože mnoho zařízení dokáže shromažďovat informace o poloze a chování jednotlivců. Otázka ochrany soukromí je zejména důležitá v oblasti zdravotnictví, kde se IoT může hodně rozšířit. Jedná se o sledování lékařského vybavení v nemocnici, monitorování vitálních hodnot pacienta doma. V tomto případě je nezbytné ověřit vlastnictví zařízení a vlastníka identity, když dojde ke změně vlastníka. (Securing the Internet of Things, 2015)

Správa identity může nabídnout v IoT nové možnosti ke zvýšení bezpečnosti tím, že kombinuje různé metody ověření pro člověka i zařízení. Příkladem by mohla být biometrická identifikace v rámci domácí sítě pro otevření dveří. (Securing the Internet of Things, 2015)

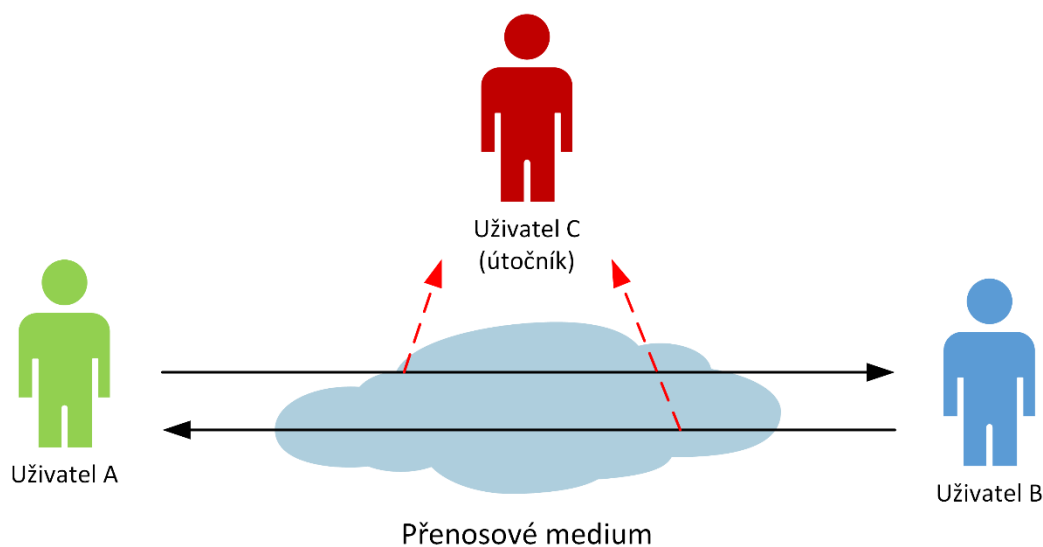
Ochrana soukromí a jeho dodržování jsou vzájemně propojeny. Jeho rozsah regulují jednotlivé země. I když se technologie rychle vyvíjejí, uživatel si musí být vědom, jak se tyto věci vztahují na jeho každodenní život.

2.2 Typy útoků

V další kapitole budou popsány základní typy útoků na bezdrátové počítačové sítě, které lze využít i v IoT, Princip útoků bude ve většině případů stejný, jen jeho důsledky mohou být rozdílné. Byly vybrány takové útoky, které představují největší riziko pro IoT. Existuje však celá řada dalších útoků a hrozeb. Útoky můžeme rozdělit do dvou kategorií a to pasivní útoky a aktivní útoky.

2.2.1 Pasivní útoky

Tyto útoky jsou orientovány především na získávání citlivých informací, které lze zneužít nebo případně použít pro další útoky. Při pasivním útoku útočník pouze monitoruje a analyzuje komunikační médium. Pasivní útoky lze špatně detekovat a ve většině případů je nejlepší ochrana prevence pomocí šifrování. K tomuto typu útoků se používají softwary na analýzu a zachytávání síťového provozu, mezi nejznámější patří program Wireshark. Na obrázku 16 je zobrazené schéma útoku, kdy mezi uživatelem A a B probíhá komunikace a uživatel C komunikaci odposlouchává.



Obrázek 16 Schéma pasivního útoku

Odposlouchávání

Síťová komunikace bývá obvykle nezabezpečena. To znamená, že po síti proudí data v otevřené textové podobě. Pokud bude útočník naslouchat na přenosové cestě v síti, dokáže snadno přenášena data číst. Možnost odposlechu síťového provozu je celkem velký bezpečnostní problém. Není problém na veřejné bezdrátové síti získat desítky přihlašovacích údajů během pár minut. Jediná možnost, jak se před podobnými útoky bránit, je použití šifrovacích služeb založených na kryptografických principech. Například u webové služby využívat HTTPS místo HTTP. (Doseděl, 2004)

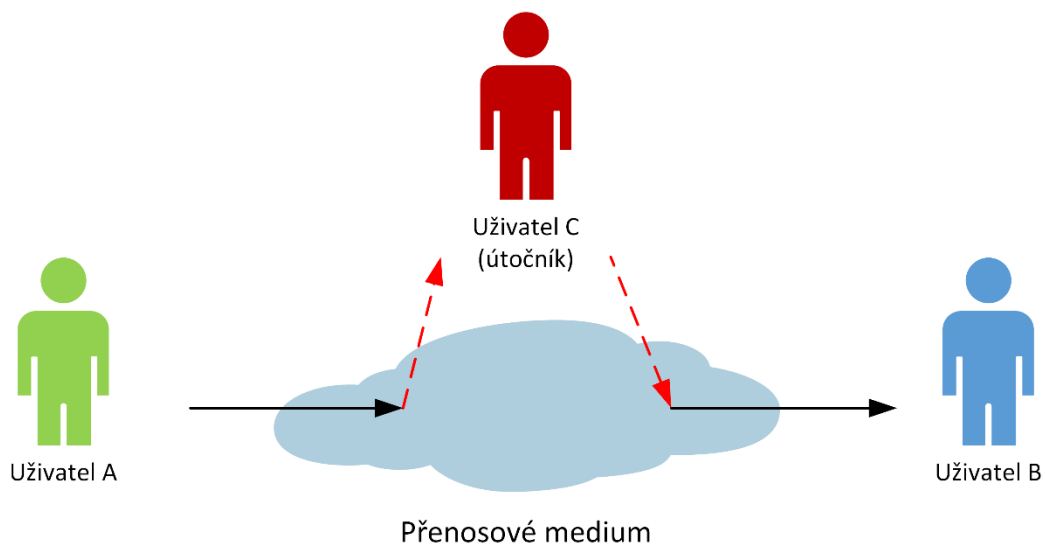
Analýza provozu

Tento typ útoku se snaží zachytávat a zkoumat přenášené zprávy. Hlavním účelem je ze zachycených zpráv odvodit určité informace. Obecně lze u tohoto typu útoku říci, že čím více zpráv bude takto sledováno či zachyceno, tím více lze získat potřebných poznatků. Do této

skupiny útoků například spadá prolamování zabezpečení bezdrátových sítí a to WEP a WAP, kde lze ze zachycených paketů prolomit heslo. (Jirovský, 2007)

2.2.2 Aktivní útoky

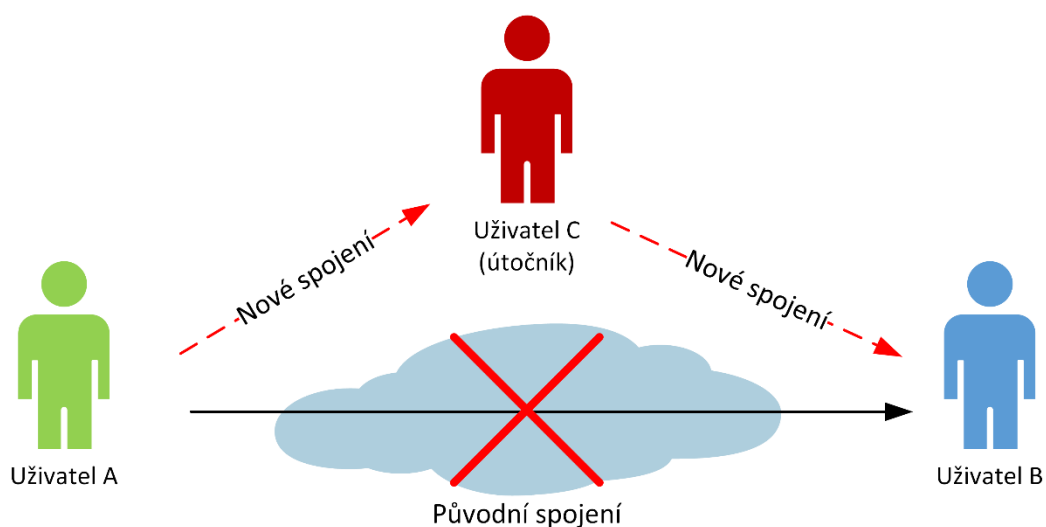
Aktivní útoky se od pasivních liší zejména v tom, že se snaží měnit systémové prostředky nebo ovlivnit jejich funkčnost a chování. Při tomto útoku se útočník snaží data přenášená přes přenosové medium přidat, odstranit nebo jinak měnit. Tím je ohrožena integrita dat, autentizace a důvěryhodnost. Aktivní útoky bývají snadněji detekovatelné než pasivní útoky díky projevům útoků, ale mohou způsobit mnohem vyšší škody než pasivní útoky. Ukázka aktivního útoku je znázorněna na obrázku 17, kdy uživatel (A) komunikuje s uživatelem (B). Veškerá komunikace prochází přes uživatele (C - útočníka), který komunikaci může měnit. Jedná se o klasický útok typu MITM.



Obrázek 17 Schéma aktivního útoku

MITM

Man-in-the-middle (MITM) je aktivní forma útoku, která zahrnuje řadu útoků a technik, kdy dochází k narušení integrity dat. Podstatou těchto útoků je snaha útočníka odposlouchávat komunikaci mezi uživateli tak, že se stane aktivním prostředníkem. Útočník může modifikovat data, která mu mohou posloužit pro řízení chodu systému způsobem, kterým útočník chce. Existuje celá řada nástrojů pro provedení těchto útoků. Například nástroj pro SSL MITM – dsniff nebo pro LAN MITM – PacketCreator. Na obrázku 18 je ukázka takového útoku. (Doseděl 2004, Jirovský 2007)



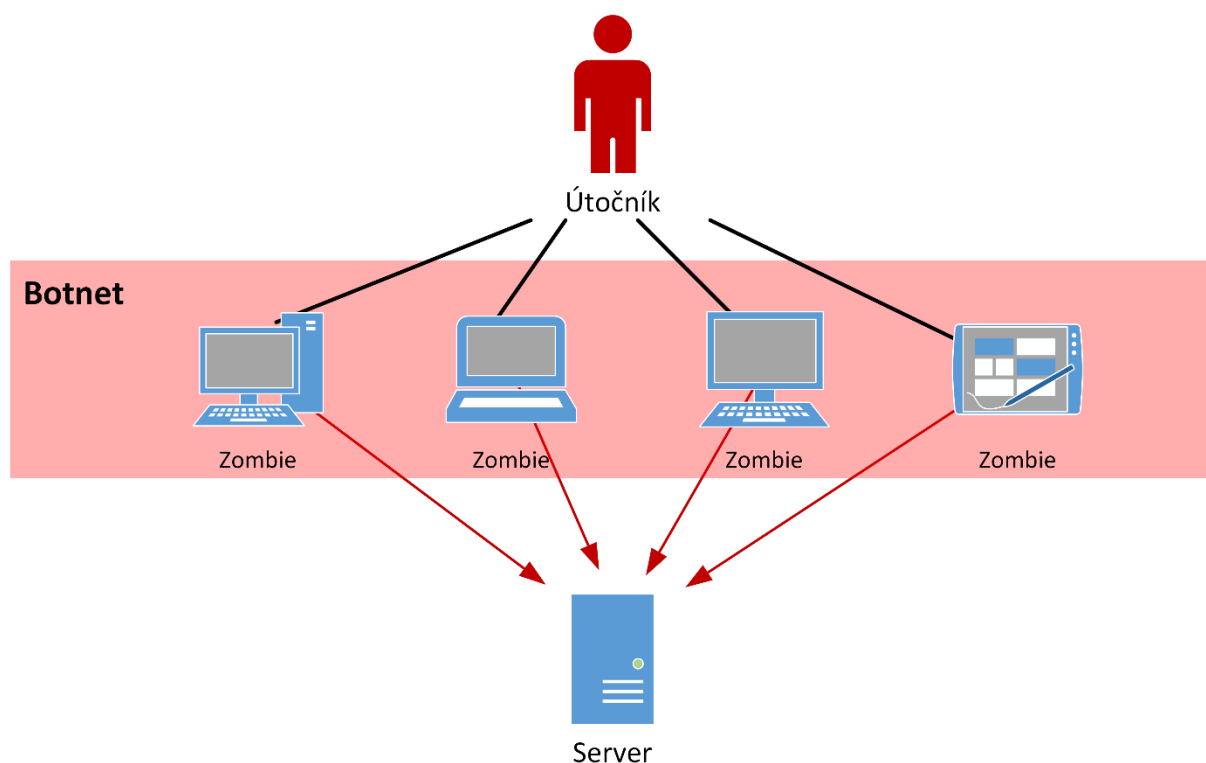
Obrázek 18 Ukázka MITM útoku

Uživatel A komunikuje s uživatelem B. Je zde však ještě jeden uživatel C, o kterém uživatel A a B nevědí. Útočník přeruší původní spojení a vytvoří nové spojení. Útočník se pak uživateli A jeví jako uživatel B a uživateli B jako uživatel A. Tímto způsobem má kontrolu nad veškerou komunikací, kdy může komunikaci modifikovat, přidávat, či odstraňovat. Možnosti obrany proti těmto útokům jsou kontrolní součty a digitální podpisy.

K tomuto typu útoku patří i změna identity ve prospěch útočníka. Ne pokaždé je cílem modifikovat samotná data, někdy je výhodnější, když se útočník postaví do role odesílatele dat. Útočník se snaží o podvrhnutí autentizační informace nebo se pokouší převzít již autentizovanou komunikační relaci (session stealing). (Jirovský, 2007)

DoS/DDoS

Pokud útočník nechce komunikaci odposlouchávat ani modifikovat, má další možnosti útoku, jak komunikujícím stranám škodit. Jedná se DoS (Denial of Service) – odepření služby a DDoS (Distributed DoS) – distribuované odepření služby. Rozdíl mezi těmito útoky je hlavně v počtu útočících zařízeních. V literatuře se o těchto útocích píše jako o útoku na znepřístupnění služby či infrastruktury. Tuto definici splňují oba, jen první varianta nemusí být účinná ve velkém měřítku, díky výkonným a moderním serverům, kapacitě jejich internetového připojení. (Doseděl, 2004, Jirovský, 2007)



Obrázek 19 Ukázka DDoS útoku

Mnohem účinnější je distribuovaná verze DDoS, kdy útočník nejprve získá kontrolu nad velkým množstvím počítačů a ve stejný okamžik jim dá povel k útoku na jeden vybraný počítač nebo server. Napadeným počítačům se říká „zombie“, který tvoří tzv. „botnet“. Jedná se o velkou síť napadených počítačů, která může obsahovat desetitisíce takových zombií. Existují tři možnosti útoků, které vedou k nedostupnosti serveru či infrastruktury. První je útok na šířku pásma, kdy útoky spočívají v zahlcení kapacity sítě serveru. Útok na zdroje spočívá v zaplnění systémových zdrojů serveru, což zabraňuje jeho reakcím na normální dotazy. Poslední typ útoku využívá chyby softwaru tzv „exploit“, zaměřuje se na konkrétní chybu softwaru pro znepřístupnění služby. (Doseděl 2004, Jirovský 2007)

V IoT mohou být útoky typu DDoS velký problém. S přihlédnutím na různé výzkumy o počtech zařízení v IoT, kdy v roce 2020 má být více zařízení pro IoT než počítačů a mobilních telefonů dohromady. U dnešních DDoS útoků známe jejich sílu. Co pak taková představa milionů infikovaných zařízení v IoT, která tvoří gigantické armády zombií?

2.3 Doporučení

Zabezpečení IoT je velmi aktuální a důležitá otázka pro samotný chod a fungování IoT. IoT vytváří velkou výzvu jak pro vývojáře, tak i pro útočníky. V další kapitole budou zmíněny základní požadavky na zabezpečení IoT. Například je nutné u embedded zařízení zajistit bezpečný firmware takovým způsobem, aby s ním nebylo možno manipulovat a dále ho měnit. Také je velmi důležité zabezpečit data uložená na zařízeních, zajistit bezpečnou komunikaci a chránit přístroje před počítačovými útoky. Toho všeho lze dosáhnout pouze tím, že počáteční fáze vývoje zahrnují i bezpečnost.

Zatím neexistuje nikdo, kdo by dokázal vyřešit všechny bezpečnostní otázky pro IoT. Bezpečnostní požadavky musejí být brány s ohledem na následky bezpečnostního selhání, rizik útoků, dostupnou množinu útoků a na náklady na implementaci bezpečnostního řešení. Existují základní funkce, které je potřeba zvážit: (The Internet of Secure Things, 2016)

- Bezpečné spouštění – Toho lze dosáhnout pomocí kryptograficky podepsaného kódu od výrobce spolu s hardwarovou podporou pro ověření kódu, zda je validní. Tím lze zajistit to, že firmware nebyl změněn a je bezpečný
- Bezpečné aktualizace – jsou důležitou součástí bezpečnosti. Slouží pro opravy kritických chyb a bezpečnostních záplat. Bezpečné aktualizace lze dosáhnout podobně jako u bezpečného spouštění pomocí podepsaného kódu, který zajistí, že se do zařízení nedostane škodlivý kód.
- Zabezpečení dat – Lze dosáhnout zabráněním neoprávněného přístupu k zařízení, šifrováním úložiště dat nebo šifrováním komunikace.
- Ověření – K neoprávněnému přístupu k zařízení by měly zabránit metody pro ověření identity a to použitím minimálně silných hesel nebo použití ověřovacích protokolů jako je X.509 nebo 802.11.X.

- Ochrana proti útokům – Kritická vrstva ochrany proti útokům může být firewall. Brána firewall může omezit komunikace pouze na známé a důvěryhodné hostitele, blokuje útočníka dříve, než může spustit samotný útok. Je nezbytné zajistit nějakou vrstvu ochrany, která ochrání zařízení proti běžným útokům, jako jsou paketové záplavové útoky (packet flood attacks), buffer overflow a využívání chyb v protokolech tzv. „exploits“.
- Detekce a monitorování – Stávající embedded zařízení mohou být napadena útočníkem a nikdo se o tom nikdy nedozví. Útočník může poslat tisíce až miliony přihlašovacích pokusů, aniž by byl tento útok nějak zaznamenán. S ohledem na výzkum HP (Internet of things research study, 2015), kdy většina zařízení nevyžadovala silná přihlašovací hesla, by tato hrozba znamenala kritické ohrožení bezpečnosti. Embedded zařízení musí být schopná detekovat a hlásit neplatné pokusy o přihlášení a jiné potenciální hrozby.
- Integrovaná zpráva zabezpečení – Důležitá je také integrace systému pro řízení bezpečnosti, která umožňuje nastavovat bezpečnostní politiky, které lze snadno aktualizovat a tím zmírnit bezpečnostní hrozby.

Klíčovou a nutnou součástí zabezpečení IoT je bezesporu autentizace a autorizace, neboli AAA architektura, kam patří i accounting (účtování). Tyto metody slouží pro identifikaci zařízení v IoT a jejich následná oprávnění a monitorování.

2.3.1 Autentizace

Autentizace slouží k jednoznačnému určení a identifikaci subjektů v IoT jako jsou embedded zařízení, senzory, akční členy nebo koncové body. Po připojení zařízení k IoT potřebuje mít každý prvek přístup k infrastruktuře IoT. Ověření důvěryhodnosti zařízení je provedeno na základě ověření identity (autentizace). Způsob jak uchovávat a prezentovat informace o identitě může být odlišný pro zařízení v IoT. V klasických sítích mohou být koncové body identifikovány pomocí přihlašovacího jména a hesla, tokenů nebo biometrických dat. Koncová zařízení IoT ve většině případů nepotřebují lidskou interakci. Naopak je žádané, aby se zařízení dokázala identifikovat sama. K tomu může posloužit radiofrekvenční identifikace (RFID), sdílené tajemství, protokol X.509, certifikáty, identifikace pomocí MAC adresy zařízení nebo jiný druh autentizace na hardwarové bázi. (Securing the Internet of Things, 2015)

2.3.2 Autorizace

Autorizace je proces ověření přístupových oprávnění zařízení IoT do infrastruktury IoT. Tento proces ve většině případů navazuje na proces autentizace, kdy na základě identity přidělí zařízení nějaká oprávnění. Hlavní podstatou autorizace je tedy ověřit, zda daný prvek má oprávnění provést příslušnou akci, například vložení nového záznamu do databáze. Velkou výzvou v této oblasti je vytvořit architekturu, která dokáže zvládnout miliardy zařízení s různou úrovní důvěryhodnosti. (Securing the Internet of Things, 2015)

2.3.3 Accounting

Tato část AAA architektury neřeší přímo zabezpečení ale účtování (protokolování). Slouží pro sledování využitých síťových služeb a zdrojů. Tyto informace mohou být důležité pro správu a plánování. Také lze z těchto informací předcházet případným plánovaným útokům. Lze například sledovat jaké zařízení a kdy se se snažilo ověřit, zda bylo ověření úspěšné.

Pro účely AAA architektury lze u klasických počítačových sítí využít protokoly TACACS+ nebo protokol 802.1x a RADIUS, které jsou podrobněji popsány v bakalářské práci. (Jelínek, 2014)

3 Návrh a implementace

Navrhované řešení cílí na využití především v domácím prostředí. Hlavním důvodem této volby jsou možnosti dostupných technologií a také fakt, že návrh a implementace ve firemním prostředí je mnohem komplikovanější. Zejména kvůli neznalosti firemních postupů, procesů a bezpečnostní politiky.

Samotný návrh řeší autentizaci a ověření zařízení. Řešení je postaveno na jednom centrálním prvku, který bude autentizaci a ověření zařízení provádět. Také bude obsahovat webový server, databázi a bude filtrovat komunikaci.

Navrhované řešení využívá technologie, které se běžně používají a jsou dostupné. Jako komunikační síť byla zvolena Wi-Fi. Wi-Fi používá každá domácí bezdrátová síť a tak není třeba kupovat nové bezdrátové rozhraní pro připojení k síti. Další důvod proč nebyla zvolena jiná technologie, je poměrně vysoká cena za moduly Zigbee nebo řešení Lora, kde se ceny pohybují v řádu stovek dolarů. K adresaci jsou použity IPv4 adresy, může to vypadat jako krok zpět. Záleží však na způsobu využití a dle toho zvážit a vybrat vhodné technologie. IPv4 je dostačující v domácím prostředí, kde není kladen důraz na dostupnost zařízení z internetu.

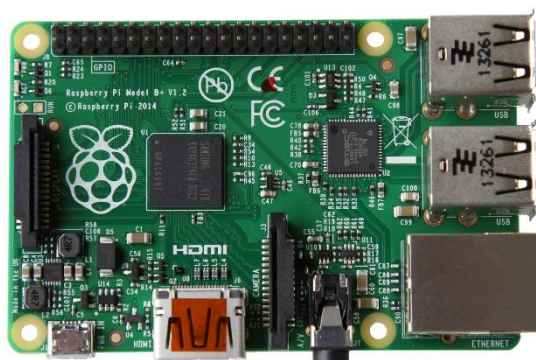
K samotné autentizaci zařízení je použit integrovaný obvod DS2401, který poskytuje unikátní 48bitové číslo. Na základě tohoto unikátního čísla bude probíhat autentifikace. Dalo by se říci, že replikuje MAC adresu zařízení, která je snadno zjistitelná a lze lehce podvrhnout. Samotný průběh autentizace bude popsán v kapitole 3.4..

3.1 Použité technologie a hardware

Jako hardware pro praktickou část byla zvolena platforma Raspberry Pi, přesněji novější model 2 pro řídicí prvek, který řídí autentizaci, poskytuje webové rozhraní pro uživatele a obsahuje databázi. Pro testovací zařízení, které bude žádat o autentizaci, byl použit starší model B. Počítač Raspberry Pi byl zvolen na základě jeho minimálních rozměrů, nízké spotřeby a velké komunity, která Raspberry Pi používá.

3.1.1 Raspberry Pi

Raspberry Pi je dílo britské nadace Raspberry Pi Foundation. Hlavním cílem této nadace je vyvíjet levný hardware pro podporu vzdělávání dospělých i dětí v oblastech výpočetní techniky, informatiky a dalších oborů. Jedná se o velmi kompaktní a levnou desku, která dokáže sloužit jako klasický počítač či multimediální centrum. V dnešní době je čím dál častěji využíván jako vývojový kit a to díky GPIO (General Purpose Input/Output) pinům, I2C, SPI a UART sběrnice. Díky tomu lze k Raspberry Pi připojit mnoho periférií jako jsou například rozšiřující kity, čidla nebo senzory. (New product launch! Introducing Raspberry Pi Model B+, 2014)



Obrázek 20 Raspberry Pi model B+ (Upton, 2014)

Existuje několik verzí Raspberry Pi, které se liší výbavou a výkonem. Nejnovější a nejvýkonnější je Raspberry Pi 3, který jako první disponuje 64bitovým procesorem se čtyřmi jádry Cortex-A53 s frekvencí 1,2 Ghz, 1GB operační paměti, grafickým čipem VideoCore IV s taktem 300MHz. Jako první nativně obsahuje rozhraní pro bezdrátové sítě WiFi 802.11n a Bluetooth 4.1.

V této práci je použito Raspberry Pi 2 a model B. Jde o téměř shodná zařízení, u kterých v praxi nepoznáte větší výkonnostní rozdíl. Hlavní rozdíly jsou v operační paměti, použitém procesoru a počtu výstupních/vstupních pinů. Starší Raspberry Pi disponuje pouze 26 piny, zatímco novější 40 piny.

Existuje několik operačních systémů pro Raspberry Pi. Oficiální podporovaný systém je Raspbian. Jedná se o operační systém založený na linuxové distribuci Debian, který je optimalizovaný pro používání na Raspberry Pi. Tento systém je také použit v této práci. Další podporované operační systémy jsou Ubuntu Mate, Snappy Ubuntu Core, OSMC, RISC OS. Také Windows vydal operační systém pro vývojové kity a to Windows 10 IoT Core, který je podporován na Raspberry Pi od verze 2 a je zaměřen na IoT.

3.1.2 MySQL

Jde o multiplatformní databázový systém, který vytvořila švédská firma MySQL AB. Je k dispozici jak pod bezplatnou licenci GPL, tak pod komerční placenou licenci. Jedná se o nejoblíbenější open source databázi na světě. Jak už název napovídá, používá jazyk SQL (Structured Query Language). Velmi oblíbená kombinace pro webový server je MySQL, Apache a PHP. V práci je použita verze MySQL 5.7.

3.1.3 Apache

Apache je webový server s open-source kódem dostupný pro moderní operační systémy, včetně UNIX a Windows. Cílem tohoto serveru je zajistit bezpečný, efektivní a rozšiřitelný server pomocí modulů. Apache podporuje velké množství funkcí, mnoho z nich je implementováno jako moduly rozšiřující jádro. Pro implementování modulů lze využít jazyků Perl, Python nebo PHP. Apache je jedním z nejpoužívanějších webových serverů. 30. května bylo jeho zastoupení 52,8% druhý Nginx měl 29,9% (Historical trends in the usage of web servers for websites, 2016). V této práci je použita poslední stabilní verze 2.4.10..

3.1.4 OpenSSL

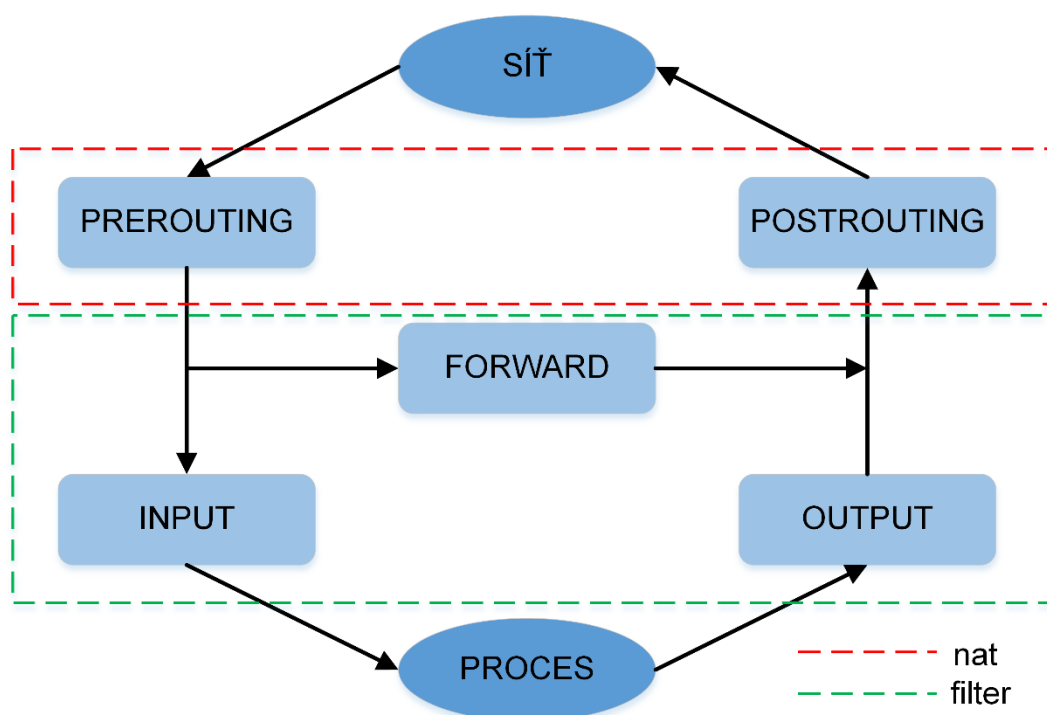
OpenSSL je open-source implementace protokolů SSL (Secure Sockets Layer) a TLS (Transport Layer Security). TLS je nástupce protokolu SSL. Oba dva jsou kryptografické protokoly, poskytující možnost zabezpečené komunikace na síti pro různé služby.

3.1.5 Další využití technologie

Dále budou představeny technologie a služby, které byly využity v praktické části.

IPTABLES

Firwall v Linuxu je tvořen subsystémem Netfilter, který pracuje na úrovni jádra a filtruje síťový provoz na základě mnoha kritérií. Dokáže pracovat se stavovými a nestavovými pravidly. Základním nástrojem pro filtrování paketů je Iptables. Je součástí linuxového jádra od verze 2.4. Pro filtrování provozu lze použít i jiné nástroje jako jsou UFW nebo Guarddog. Iptables jsou rozděleny do čtyř nezávislých tabulek: filter, nat, mangle a raw. Je nutné specifikovat tabulku, se kterou chceme pracovat pomocí přepínače -t, -table. Pokud tabulka není specifikována, použije se výchozí tabulka filter.



Obrázek 21 Průchod paketu

Tabulka **filter** je výchozí tabulkou, která je vhodná pro základní filtrování, logování síťového provozu. Obsahuje tři vestavěná pravidla (chainy):

- INPUT – vstupní řetězec pro pakety, které vstupují do počítače,
- OUTPUT – výstupní řetězec pro pakety, který odchází z počítače,
- FORWARD – pro přeposílání paketů. Rozhoduje, co se stane s paketem, který není určený pro daný počítač.

Tabulka **nat** se používá pro překlad adres (NAT), maškarádu nebo port forwarding. Používá se jen pro první paket spojení. Také obsahuje tři vestavěné řetězce pravidel.

- **PREROUTING** – příchozí pakety,
- **POSTROUTING** – odchozí pakety,
- **OUTPUT** – pro lokálně generované pakety.

Tabulky **mangle** a **raw** . Používají se například pro rozšíření pravidel pro přeposílané pakety nebo pro nastavování výjimek. Mangle také zpracovává hlavičky paketů a využívá se pro QoS. Tyto tabulky nebyly použity v praktické části, a proto nebudou dále popisovány.

Základní syntaxe může vypadat takto:

```
$iptables [tabulka] [příkaz] [řetězec] [pravidla] [cíl]
```

Je nutné specifikovat tabulku, kterou chceme použít. Pokud nebude tabulka specifikována, použije se tabulka filter.

Příkaz určuje, zda budeme pravidlo vkládat, upravovat nebo mazat. Od přepínačů se liší tím, že je to velké písmeno.

Základní přehled příkazů je:

- **-A, --append** – připojí pravidlo na konec vybraného řetězce,
- **-D, --delete** – z vybraného řetězce odebere pravidlo. Buď podle čísla pravidla, nebo podle specifického příkazu, který se použil při vkládání pravidla,
- **-I, --insert** – vloží pravidlo do zvoleného řetězce. Podle čísla lze určit pořadí pravidla. Pokud není pořadí určeno, zařadí se pravidlo na začátek řetězce,
- **-P, --policy** – nastavuje výchozí politiku pro řetězec.

Příkazů je samozřejmě vícero, více informací lze dočíst v dokumentaci.

Základní přehled parametrů:

- **-p, --protocol** – protokol pravidla nebo paketu, který má být kontrolován. Může se jednat o jeden z protokolů tcp, udp nebo icmp. Nebo může být zadán číselně specifický port.
- **-s, --source** – zdrojová IP adresa paketu, případně rozsah IP adres,
- **-d, --destination** – cílová IP adresa paketu,
- **-i** – vstupní interface, který paket přijme,
- **-o** – výstupní interface, kterým paket odejde,
- **-j, --jump** – určuje cíl pravidla. Tedy to, co se s paketem má stát.

Cíle pravidel:

- **ACCEPT** – povolí paket, nechá paket projít filtrem,
- **REJECT** – paket bude zahozen a na zdrojovou adresu bude poslán chybový paket. Jinými slovy paket slušně odmítne.
- **DROP** – paket bude zahozen.

Jako příklad je přidání a odebrání pravidla na povolení SSH ze zdrojové IP adresy 1.1.1.1 na interface eth0.

```
$iptables -A INPUT -i eth0 -s 1.1.1.1 -p tcp --dport 22 -j ACCEPT #pridani  
$iptables -D INPUT -i eth0 -s 1.1.1.1 -p tcp --dport 22 -j ACCEPT #smazani
```

ISC-DHCP-SERVER

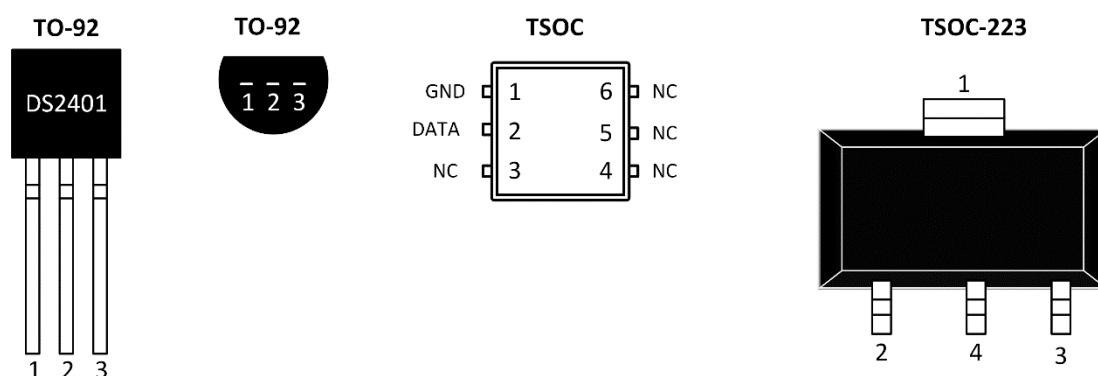
Balíček ISC-DHCP-SERVER slouží jako DHCP server (Dynamic Host Configuration Protocol). Protokol DHCP vyvinula a spravuje ISC (Internet Software Consortium). Dodává také příslušný balíček, který je šířen jako open source. Typicky se pomocí DHCP nastavuje IP adresa, maska sítě, výchozí brána a DNS server. Všechna IP zařízení potřebují svou adresu a je nutné adresy přidělovat každému zařízení a to buď manuálně, nebo dynamicky. Tento balíček usnadňuje a mnohem zefektivňuje přidělování IP adres. Adresy jsou přidělovány automaticky na základě rozsahu IP adres nebo staticky na základě MAC adresy zařízení. Balíček podporuje adresaci IPv4 a IPv6 adres. (ISC DHCP, 2016)

HOSTAPD

Hostapd je software, který slouží k vytvoření AP (Access Point) IEEE 802.11 a také jako autentizační server pro IEEE 802.1X/WPA/WPA2/EAP/, RADIUS client, EAP server a RADIUS autentizační server. Pro správné fungování musí WiFi karta podporovat ovladač nl80211. Hostapd je vytvořen jako daemon běžící na pozadí systému a slouží jako backend pro kontrolu autentizace.

3.2 DS2401

Pro identifikaci zařízení byl zvolen integrovaný obvod DS2401 Silicon Serial Number. Mezi hlavní výhody patří nízká cena a jednoduché použití. DS2401 obsahuje unikátní 64-Bit ROM ID čip pro identifikaci. Další výhodou je použití 1-Wire sběrnice, která umožňuje využití více integrovaných obvodů DS2401 na jedné datové lince. Také redukuje ovládání, adresaci, data a napájení do jednoho pinu. Komunikuje rychlostí do 16,3 kbps. DS2401 je vyráběn v několika provedeních a to v TO-92, SOT-223 nebo TSOC, které jsou ukázány na obrázku 22 i s jejich piny. (DS2401 Silicon Serial Number, 2015)



Obrázek 22 DS2401 přehled

DS2401 obsahuje 64 bitové identifikační číslo, které poskytuje naprosto jedinečnou identitu. Na obrázku 23 je zobrazena ROM paměť DS2401, která obsahuje unikátní 48 bitové sériové číslo, 8 bitový CRC kontrolní součet a 8 bitový Family kód. Family kód určuje typ integrovaného obvodu a jeho funkci. Například teplotní čidlo DS18B20 má Family kód (28) a DS2401 (01). (DS2401 Silicon Serial Number, 2015)

8-Bit CRC kód		48-Bit Sériové číslo		8-Bit Family kód (01h)	
MSB	LSB	MSB	LSB	MSB	LSB

Obrázek 23 DS2401 paměťová mapa

Data jsou přenášena pomocí 1-Wire sběrnice. Napájení pro čtení a zápis lze získat z datového pinu a není potřeba žádného externího zdroje energie.

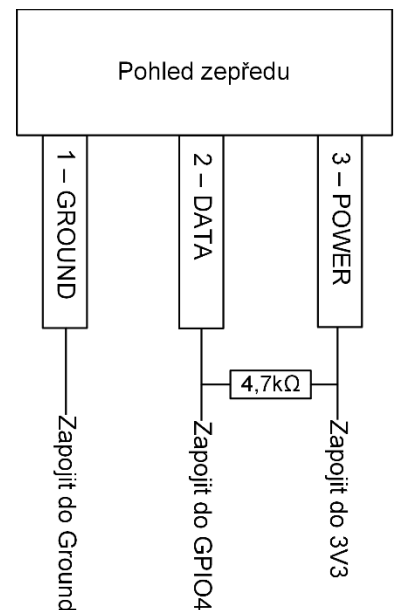
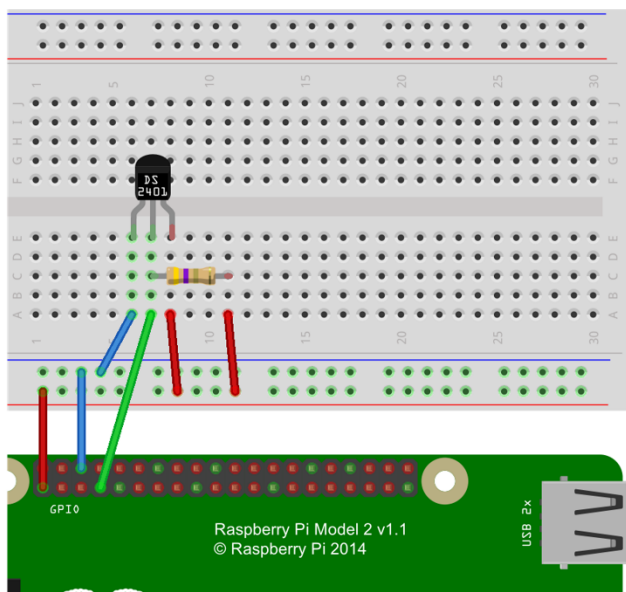
3.2.1 1-Wire sběrnice

1-Wire sběrnice byla navržena v devadesátých letech firmou Dallas Semiconductor, kterou v roce 2001 koupila firma Maxim Integrated Products, Inc.. Jedná se o sběrnici, která dokáže využít pouze jeden vodič pro datový signál i napájení, druhý vodič sloučí jako zem. Tedy umožňuje připojit více zařízení k řídicí jednotce prostřednictvím dvou vodičů.

Komunikace na sběrnici je asynchronní a poloduplexní. Striktně dodržuje schéma jednoho master zařízení a jednoho nebo více slave zařízení. Master inicializuje a řídí komunikaci s jedním nebo více slave zařízeními 1-Wire na sběrnici 1-Wire. DS2401 je vždy typu slave. Každé slave zařízení má unikátní 64-bit identifikační číslo ID. 1-Wire slave zařízení typicky pracují v rozsahu 2,8V až 5,25V. Více obvodů je připojeno na společnou zem a paralelně na společný datový vodič. 1-Wire podporuje dva typy zapojení a to parazitní režim, který byl zmíněn na začátku, kde lze využít pouze jednoho vodiče pro datový signál a napájení a druhý vodič pro zem. Druhý režim se třemi vodiči využívá jeden vodič pro napájení, druhý vodič pro datový signál a třetí vodič pro zem. (DS2401 Silicon Serial Number, 2015, Overview of 1-Wire Technology and Its Use, 2008)

3.2.2 Schéma zapojení DS2401

Samotné zapojení DS2401 k Raspberry Pi je poměrně jednoduché. Stačí nám pouze RPi, DS2401 a rezistor 4K7 ohmů. Při práci s GPIO porty si musíme dát pozor, abychom RPi nezničili. RPi pracuje s napětím 3,3V. To znamená, že komponenty počítače Pi vyžadují zdroj napájení 3,3V. Port 2 GPIO však poskytuje zdroj napájení 5V. Pokud bychom omylem připojili zdroj napájení 5V k libovolnému pinu portu GPIO mohlo by dojít k poškození počítače Pi. Proto je třeba dbát opatrnosti a raději dvakrát kontrolovat. Zapojení je identické pro RPi 2 i RPi B.



Obrázek 24 Schéma zapojení DS2401

Na obrázku 24 je schéma zapojení. Důležité jsou 3 piny na RPi. A to první pin v dolní řadě, který poskytuje napájení 3,3V, třetí pin v horní řadě představuje zem a čtvrtý pin v druhé řadě je datový pin GPIO4. Pro shrnutí červený vodič je napájení 3,3V, modrý vodič představuje zem a zelený vodič je datový.

RPi je vybaven řadou ovladačů pro různá rozhraní. Tyto ovladače jsou uloženy jako moduly jádra a jsou dostupné přes příkaz *modprobe*. Tímto příkazem se jednotlivé moduly zavedou do linuxového jádra, když jsou potřeba. Proto není nutné programovat čtení z obvodu DS2401, ale využijeme hotových modulů.

Pro nastavení GPIO nejprve upravíme konfigurační soubor */boot/config.txt* a na konec souboru přidáme:

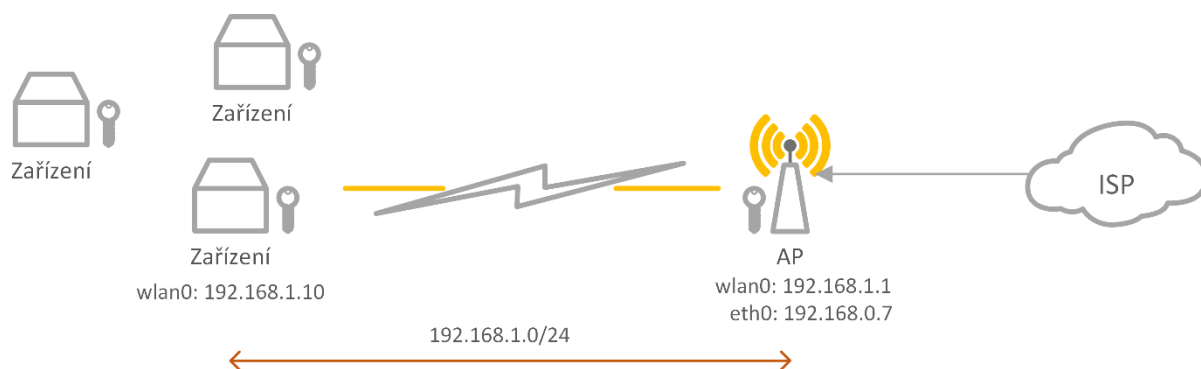
```
#GPIO
dtoverlay=w1-gpio,gpiopin=4
```

Zavedeme jednotlivé moduly:

```
$ sudo modprobe wire
$ sudo modprobe w1-gpio
$ sudo modprobe w1-smem
```

Ted' stačí systém restartovat. Název a zároveň unikátní ID připojeného DS2401 najdeme v souboru */sys/bus/devices/*. Pokud je nějaký obvod zapojený, vytvoří se zde složka s unikátním ID ve tvaru 01-xxxxxxxxxxx. První dvě čísla označují family kód, pro DS2401 je family kód 01. Za pomlčkou pak následuje unikátní 48bitový kód. Načítání unikátního kódu má na starosti hlavičkový soubor *get_id.h*.

3.3 Navrhovaný systém



Obrázek 25 Schéma sítě

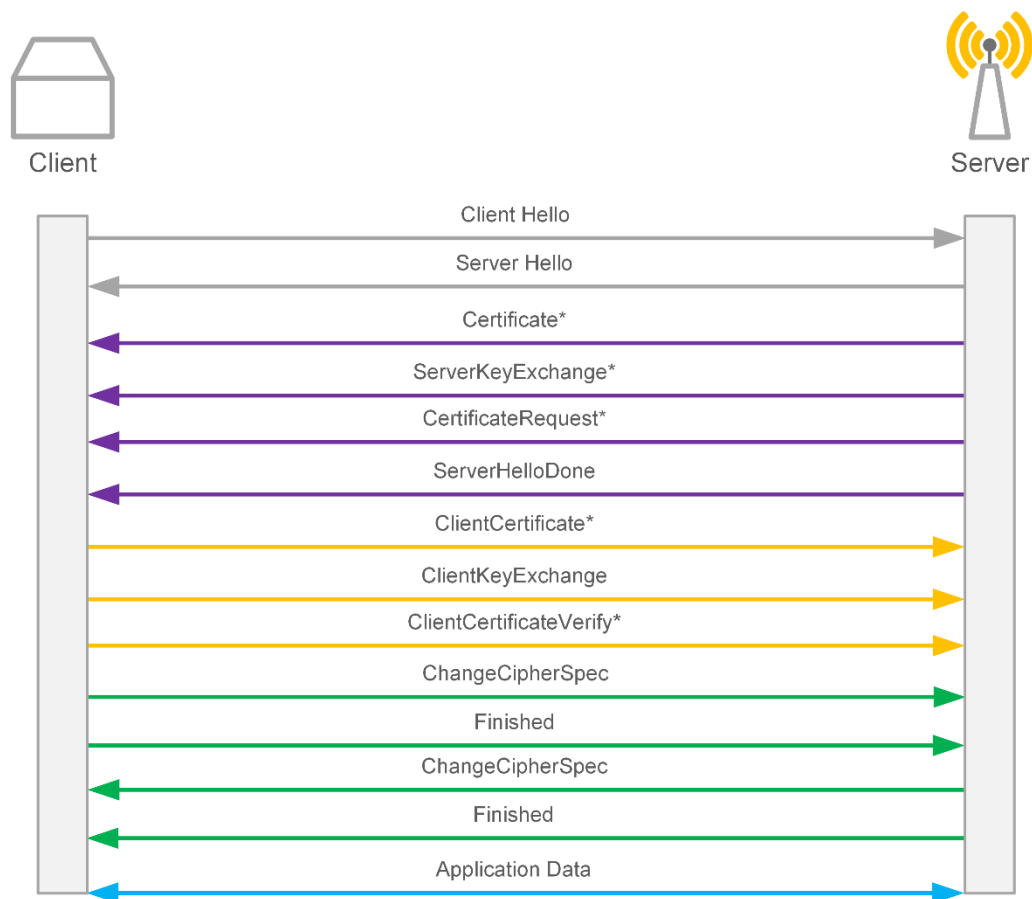
Myšlenka je taková, že každý prvek sítě (zařízení) bude mít své unikátní identifikační číslo, kterým se bude ověřovat, identifikovat. Otázka zní, kde takové unikátní identifikační číslo získat. Další otázka je, jakým způsobem zařízení ověřit? Bude šifrovaná celá komunikace, nebo se bude šifrovat jen část? Jaké šifrování se použije?

Aby se zabránilo odposlouchávání a útokům typu MITM bude šifrovaná celá komunikace. To znamená, že se nejdříve vytvoří zabezpečená komunikace, poté proběhne ověření a až následně proběhne samotná komunikace. Pro šifrování komunikace je využita knihovna OpenSSL a kryptografický protokol TLS ve verzi 1.2..

3.4 Autentizace

3.4.1 Zabezpečená komunikace

Jak již bylo zmíněno, nejdříve se vytvoří zabezpečená komunikace. Zabezpečenou komunikaci lze vytvořit pomocí SSL/TLS. V tomto případě se využije dvou párů klíčů. Server i klient má



Obrázek 26 TLS Handshake

vlastní pár soukromých a veřejných klíčů. Pro šifrovanou komunikaci není nutné, aby měl klient také svůj pár klíčů. Postačí, když klíči disponuje server.

TLS protokol je založen na vzájemné výměně zpráv mezi klientem a serverem tzv. handshake. Zprávy označené hvězdičkou jsou dobrovolné. Handshake probíhá následovně:

- Typicky TLS handshake začíná zprávou *ClientHello*, kterou posílá klient. Tato zpráva nese informace o nejvyšší verzi TLS. Také posílá náhodné číslo, seznam doporučených šifrovacích sad, kompresních metod a seznam rozšíření.
- Server odpovídá zprávou *ServerHello* obsahující zvolenou verzi protokolu, náhodné číslo, šifrovací a kompresní metodu vybranou ze seznamu klienta.

- Server pošle zprávu *Certificate*. Certifikát serveru obsahuje veřejný klíč, který klient použije k ověření serveru a zašifrování premaster secret.
- Server může poslat zprávu *ServerKeyExchange*. Toto je volitelný krok, kdy server vytvoří a odešle dočasný klíč klientovi. Tento klíč může být použit k zašifrování zprávy *ClientKeyExchange*.
- Další zpráva *CertificateRequest* je také volitelná. Je poslána, pokud server vyžaduje ověření i od klienta.
- Zprávou *ServerHelloDone* server oznamuje, že první fáze je dokončena a čeká na odpověď klienta.
- Klient odpoví zprávou *ClientCertificate*, pokud server poslal požadavek na certifikát klienta zprávou *CertificateRequest*.
- Klient pošle zprávu *ClientKeyExchange*. Tou posílá serveru zprávu o vypočteném premaster secret. Premaster secret je zašifrováno pomocí veřejného klíče serveru.
- Další volitelnou zprávou je *ClientCertificateVerify*. Tuto zprávu klient odesílá jen tehdy, odeslal-li zprávu *ClientCertificate*. Klient je ověřen pomocí svého soukromého klíče. Příjemce ověřuje podpis pomocí veřejného klíče odesílatele, čímž je zajištěno, že byla zpráva podepsána soukromým klíčem klienta.
- Předposledním typem zprávy je *ChangeCipherSpec*. Touto zprávou klient oznamuje serveru, že veškeré zprávy budou šifrovány s využitím jeho klíče s dohodnutým algoritmem.
- Na závěr klient pošle již první šifrovanou zprávu *Finished* obsahující hash a MAC předchozích iniciačních zpráv.
- Server se pokusí dešifrovat klientovu zprávu *Finished* a ověřit její hash a MAC. Pokud dešifrování nebo ověření selže, inicializace je považována za neúspěšnou. Spojení by v takovém případě mělo být ukončeno.
- Server odešle svou zprávu *ChangeCipherSpec* a zašifrovanou zprávu *Finished*. Klient provede analogické dešifrování a ověření.

Pokud vše proběhlo v pořádku, komunikace je šifrovaná. Poté dochází k ověření pomocí unikátního identifikátoru.

3.4.2 Generování certifikátů

Základem pro použití SSL/TLS je asymetrická kryptografie. Asymetrická kryptografie pracuje s dvojicí klíčů – veřejný a soukromý. Data zašifrovaná veřejným klíčem dešifruje pouze soukromý klíč.

Jako první je nutné vygenerovat certifikační autoritu:

```
$ openssl genrsa -des3 -out ca.key 4096
$ openssl req -new -x509 -days 365 -key ca.key -out ca.crt
```

Příkazy vygenerují klíč ca.key o síle 4096 b a certifikát ca.crt s platností 365 dní.

Dalším nutným krokem je vygenerování dvojice pro server a klienty.

```
# generovani server cert a klic
$ openssl genrsa -des3 -out ssl_server.key 4096
$ openssl req -new -key ssl_server.key -out ssl_server.csr
```

```
# generovani klient cert a klic
$ openssl genrsa -des3 -out ssl_client.key 4096
$ openssl req -new -key ssl_client.key -out ssl_client.csr
```

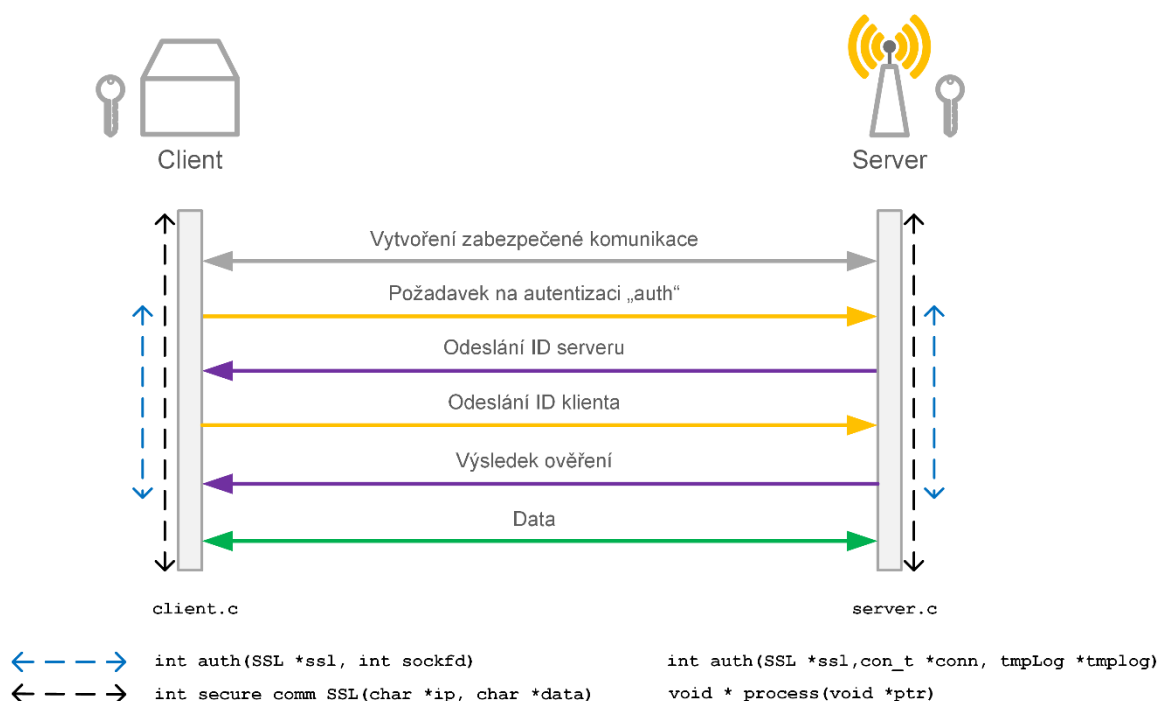
Posledním krokem je podepsání vygenerovaných certifikátů certifikační autoritou.

```
# podepsani cert server CA
$ openssl x509 -req -days 365 -in ssl_server.csr -CA ca.crt -CAkey ca.key -
set_serial 01 -out ssl_server.crt

# podepsani cert klient CA
$ openssl x509 -req -days 365 -in ssl_client.csr -CA ca.crt -CAkey ca.key -
set_serial 01 -out ssl_client.crt
```

Více informací o jednotlivých parametrech je uvedeno v manuálové stránce OpenSSL.

3.4.3 Ověření



Obrázek 27 Schéma autentizace

Autentizace zařízení na základě unikátního identifikačního čísla probíhá v pěti krocích.

- Před zahájením samotné autentizace proběhne vytvoření zabezpečené komunikace, která je popsána na straně 67-68. Samotné vytvoření zabezpečené komunikace pomocí certifikátů by stačilo k autentizaci zařízení. Každé zařízení by však muselo mít vlastní unikátní certifikát. Navrhované řešení funguje tak, že každé zařízení v síti má stejný pár certifikátů, kterým říká, že patří do naší sítě.
- Autentizaci začíná klient, který posílá požadavek na autentizaci „auth“.
- Server požadavek zpracuje a odpovídá klientovi svým ID.
- Klient ID přijme a ověří, zda se jedná o daný server. Pokud ověření proběhne v pořádku, klient pošle serveru své ID.
- Server ověří vůči databázi, zda zařízení s daným ID existuje. Pokud existuje, zkoumá, jestli má dané ID právo komunikovat. Pokud je zařízení ověřeno a může komunikovat, posílá server zprávu „0x123“ v jiném případě „0x987“.
- Po ověření může klient komunikovat šifrovaně se serverem na portu 1111.

Veškeré zdrojové kódy, které řeší autentizaci, jsou přiloženy a okomentovány. Z tohoto důvodu nebudou dále popisovány.

3.4.4 Spuštění

Na straně klienta je použit soubor *client.c* pro ověření a komunikaci se serverem. Klient vyčítá unikátní identifikační kód z DS2401 pomocí hlavičkového souboru *get_id.h*. pokaždé, když se snaží ověřit. Pro kompilaci se použije následující příkaz:

```
$ gcc client.c -o client -lssl -lcrypto -W
```

Při spouštění zkompilevaného kódu je nutné zadat IP adresu serveru:

```
$ ./client 192.168.1.1
```

Server využívá soubor *server.c*, který slouží pro komunikaci a ověření zařízení. Pro každé nové připojení je vytvořeno vlákno starající se o dané spojení. Server také používá hlavičkový soubor *get_id.h* pro získání unikátního identifikačního kódu. Server dále používá hlavičkový soubor *connmysql.h* pro připojení k databázi a *arpmac.h* pro získání MAC adresy ověřovaného zařízení. Kompilace se provede pomocí příkazu:

```
$ gcc server.c -o server -I/usr/include/mysql -lmysqlclient -lpthread -lssl  
-lcrypto -W
```

Zkompilevaný soubor se spustí příkazem: `$./server`

Pro automatické spouštění skriptů po restartu systému lze použít nástroj `crontab`:

```
$ crontab -e  
@reboot /cesta/k/souboru/nazev-skriptu # pridame na konec
```

Další možnost je přidat spouštěcí skript do `/etc/init`.

```
$ nano /etc/init/mujskript.conf  
# do souboru pridame  
description      "nas skript"  
start on startup  
task  
exec /cesta/k/souboru/nazev-skriptu
```


3.5 Návrh Databáze

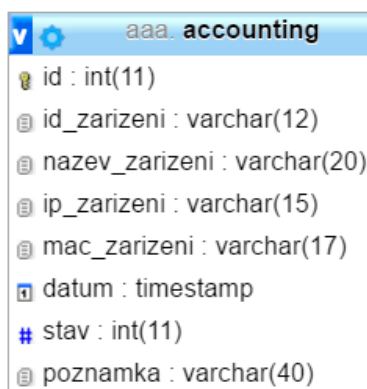
Pro testovací účely postačí jednoduchá databáze, která bude složena ze třech tabulek. Jedna tabulka bude obsahovat informace o jednotlivých zařízeních, druhá tabulka bude sloužit pro základní logování a třetí tabulka pro ukládání přihlašovacích údajů k webovému rozhraní.



aaa. zarizeni	
id	int(11)
id_zarizeni	varchar(12)
mac_zarizeni	varchar(17)
nazev_zarizeni	varchar(20)
stav	int(11)

Obrázek 28 Tabulka zařízení

Tabulka zařízení obsahuje informace o jednotlivých zařízeních: unikátní identifikační číslo, MAC adresu zařízení, název zařízení a stav (povoleno/nepovoleno).

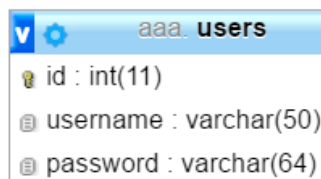


aaa. accounting	
id	int(11)
id_zarizeni	varchar(12)
nazev_zarizeni	varchar(20)
ip_zarizeni	varchar(15)
mac_zarizeni	varchar(17)
datum	timestamp
stav	int(11)
poznámka	varchar(40)

Obrázek 29 Tabulka účtování

Tabulka accounting slouží k účtování. Uchovává informace o průběhu ověření (zda zařízení bylo, či nebylo povoleno), o nově připojeném zařízení, které čeká na autentizaci a také loguje posílané zprávy. Obsahuje unikátní identifikační číslo, MAC adresu, IP adresu, datum a čas, stav a poznámku. Tabulek pro logování by mohlo být mnohem víc. Například logování filtrované komunikace.

Poslední velmi jednoduchou tabulkou je tabulka users. Obsahuje přihlašovací údaje k webovému rozhraní. Uživatelské jméno je uchovááno v textové podobě a uživatelské heslo je uloženo bezpečně v SHA256.



aaa. users	
id	int(11)
username	varchar(50)
password	varchar(64)

Obrázek 30 Tabulka uživatelů

SQL skripty pro vygenerování tabulek jsou přiloženy na CD.

3.6 Konfigurace serveru

Pro autentizační server bylo zvoleno zařízení Raspberry Pi, které je popsáno v kapitole 3.1.1.. Také bude zastávat funkci webserveru, DHCP serveru, databáze a přístupového bodu. Za normálních podmínek by všechny tyto služby byly odděleny. Pro testovací účely však postačí jedno zařízení. Než se dostaneme k samotné konfiguraci jednotlivých služeb, je doporučeno provést aktualizaci systému.

```
$ sudo apt-get update && sudo apt-get upgrade
```

V dalším kroku je nutné nainstalovat všechny potřebné balíčky. Jedná se o:

- apache2, php5
- isc-dhcp-server,
- hostapd,
- mysql-server, libmysqlclient-dev, phpmyadmin.

Instalaci provedeme pomocí příkazu *apt-get install*, kde *pkg1* označuje název balíčku:

```
$ sudo apt-get install pkg1 [pkg2 ...]
```

Konfigurace rozhraní

Jako první nastavíme jednotlivá rozhraní. Rozhraní eth0 bude sloužit pro připojení mimo síť (wan), rozhraní wlan0 pak jako AP pro lokální síť. Konfigurace jednotlivých rozhraní je uložena v souboru /etc/network/interfaces. Pro editaci souboru lze použít jakýkoliv textový editor. Samotný soubor otevřeme například pomocí editoru nano.

```
$ sudo nano /etc/network/interfaces
```

Eth0 bude získávat adresu automaticky pomocí DHCP serveru, wlan0 bude mít statickou IP adresu 192.168.1.1 s maskou 255.255.255.0. Příkaz *pre-up iptables-restore < cesta* zajistí automatické nastavení pravidel firewallu.

```
auto eth0
iface eth0 inet dhcp
    pre-up /sbin/iptables-restore < /home/pi/diplom/firewall/fwrules

allow-hotplug wlan0
iface wlan0 inet static
    address 192.168.1.1
    netmask 255.255.255.0
    pre-up /sbin/iptables-restore < /home/pi/diplom/firewall/fwrules
```

Aby se projevíly změny konfigurace, je nutné jednotlivé interface restartovat. To můžeme provést příkazy:

```
$ sudo ifdown eth0
$ sudo ifup eth0
$ sudo ifdown wlan0
$ sudo ifup wlan0
```

Konfigurace DHCP serveru

Konfiguraci DHCP serveru isc-dhcp-server najdeme v souboru */etc/dhcp/dhcpd.conf*. DHCP poběží na interface wlan0. Bude automaticky přidělovat IP adresy a DNS. Otevření konfiguračního souboru:

```
$ sudo nano /etc/dhcp/dhcpd.conf
```

V konfiguračním souboru najdeme následující řádky a vložíme před ně #. Tím zajistíme, že se nepoužijí. Stane se z nich komentář.

```
#option domain-name "example.org";
#option domain-name-servers ns1.example.org, ns2.example.org;
```

Dále najdeme řádek *#authoritative*, a odstraníme #. Tím nastavíme, že je DHCP server oficiální DHCP server pro lokální síť.

Nakonec souboru přidáme subnet s adresou sítě 192.168.1.0 maskou sítě 255.255.255.0. Tak bude DHCP server znát topologii sítě a IP adresy, které má použít pro adresaci a DNS. Rozsah přidělovaných adres bude 192.168.1.20 – 192.168.1.50. Výchozí brána bude mít IP adresu 192.168.1.1 a DNS 8.8.8.8 a 8.8.4.4.

```
subnet 192.168.1.0 netmask 255.255.255.0 {  
    range 192.168.1.20 192.168.1.50;  
    option broadcast-address 192.168.1.255;  
    option routers 192.168.1.1;  
    default-lease-time 600;  
    max-lease-time 7200;  
    option domain-name "local";  
    option domain-name-servers 8.8.8.8, 8.8.4.4;  
}
```

Také můžeme specifikovat IP adresu pro daného hosta dle MAC adresy. Tím docílíme, že zařízení s danou MAC adresou bude mít vždy stejnou IP adresu.

```
host client{  
    hardware ethernet 00:1f:1f:42:98:cf;  
    fixed-address 192.168.1.10;  
}
```

Poslední věc, která je potřeba nastavit je interface na kterém DHCP server poběží. To lze nastavit v souboru */etc/default/isc-dhcp-server* přidáním wlan0.

```
INTERFACES="wlan0"
```

Konfigurace AP

Funkci AP obstarává daemon hostapd. Pro jeho správnou funkci hostapd je potřeba, aby byl bezdrátový interface podporován ovladačem nl80211. Konfigurační soubor hostapd se nachází v `/etc/hostapd/hostapd.conf`. Zde nastavíme ssid, ověřovací heslo, typ ověření, číslo kanálu. Do souboru přidáme následující konfiguraci:

```
interface=wlan0
driver=nl80211
ssid=rpi
hw_mode=g
channel=1
macaddr_acl=0
auth_algs=1
ignore_broadcast_ssid=0
wpa=2
wpa_passphrase=raspberry
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP
rsn_pairwise=CCMP
```

Tím docílíme, že AP bude na interface wlan0, Wi-Fi síť se bude jmenovat „rpi“ s ověřovacím heslem „raspberry“, způsob ověření bude wpa2, kanál 1.

Posledním krokem je úprava konfigurace `/etc/default/hostapd`, kde najdeme řádek `#DEAMON_CONF=""` a upravíme ho na `DEAMON_CONF="/etc/hostapd/hostapd.conf"`.

Konfigurace firewallu

Pro konfiguraci firewallu lze použít nástroj iptables, který je popsán v kapitole 3.4.1. Jako první specifikujeme výchozí politiku ve všech třech základních řetězech. Pro nastavení firewallu se hodí vše zakázat a povolit to nejnutnější, respektive, co je potřeba. Proto všechny pakety, co přichází, nebo mají být směrovány, zahodíme a povolíme jen odchozí pakety. Je třeba dát pozor, pokud zakážeme veškerou komunikaci a k serveru přistupujeme vzdáleně, abychom nezakázali komunikaci sami sobě. Pak je nutné server restartovat.

```
$ sudo iptables -P INPUT DROP
$ sudo iptables -P OUTPUT ACCEPT
$ sudo iptables -P FORWARD DROP
```

Všechna příchozí komunikace je zakázána. Pro lepší přehled lze vytvořit soubor s pravidly, který pak spustíme, a všechna pravidla se aplikují najednou. Dále povolíme jen to, co je potřeba.

```
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
iptables -A INPUT -i wlan0 -p tcp --dport 1111-j ACCEPT
```

První řádek povoluje komunikaci pro loopback. Ten je nutný povolit, protože některé služby ho využívají a nemusely by fungovat korektně. Druhý řádek propouští všechny pakety, které náleží již vytvořeným spojením (ESTABLISHED) nebo novým spojením, která k nim patří (RELATED). Třetí a čtvrtý řádek povolují nová TCP spojení směřující na porty 22 (SSH) a 80 (HTTP). Předposlední řádek povoluje ICMP, typ specifikuje echo-request. Poslední řádek povoluje komunikaci na portu 1111 pro ověření zařízení. Tento řádek je důležitý pro autentizaci nových zařízení, v opačném případě by se pro každé zařízení muselo ručně zadávat nové pravidlo pro povolení komunikace na portu 1111.

Poslední konfigurace firewallu se týká nastavení NAT. Ta je důležitá, pokud je potřeba, aby zařízení v síti mohla komunikovat mimo síť. Je nutné nastavit překlad privátních adres na veřejné. Nejprve je potřeb povolit samotné směrování paketů. To se povolí v souboru */etc/sysctl.conf*, kde se odstraní # před řádkem *net.ipv4.ip_forward=1*. Nastavení se aktivuje automaticky při startu počítače. Můžeme ho však aktivovat ihned příkazem:

```
$ sysctl -p
```

nebo ručně zápisem jedničky do speciálního souboru:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Dalším krokem je povolení překladu adres mezi eth0 a wlan0 ve firewallu. Pro zopakování interface wlan0 představuje lokální síť a eth0 veřejnou síť (wan).

```
$ sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
$ sudo iptables -A FORWARD -i eth0 -o wlan0 -m state --state
RELATED,ESTABLISHED -j ACCEPT
$ sudo iptables -A FORWARD -i wlan0 -o eth0 -j ACCEPT
```

První řádek způsobí, že pokud z lokální sítě přijde paket, který chce opustit síť přes interface eth0, dojde k nahrazení jeho původní adresy adresou eth0. Druhý a třetí řádek stanovuje, že spojení mohou být navázána pouze směrem z vnitřní sítě a ne opačně, přičemž pakety již otevřených spojení mohou putovat oběma směry.

Posledním krokem je uložení pravidel a nastavení automatického načítání pravidel po restartování nebo odpojení a připojení rozhraní. Načtení pravidel již bylo popsáno při konfiguraci jednotlivých rozhraní. Uložit pravidla lze následovně:

```
$ sudo iptables-save > /cesta/k/souboru
```

Spuštění

Po konfiguraci `isc-dhcp-server` a `hostapd` je nutné tyto služby restartovat, aby se projevíly změny. Také je nutné zajistit, aby se spouštěly při každém startu systému automaticky. To lze provést příkazy:

```
$ sudo service isc-dhcp-server restart|start
$ sudo service hostapd restart|start
$ sudo update-rc.d hostapd enable
$ sudo update-rc.d udhcpd enable
```

Aby uživatelské webové rozhraní mohlo konfigurovat pravidla v `iptables` je nutné v souboru `/etc/sudoers` povolit práva pro skupinu `www-data`. Příkazem `sudo visudo` otevřeme konfiguraci souboru. Na konec řádku je nutné přidat:

```
www-data ALL=NOPASSWD: /sbin/iptables
www-data ALL=NOPASSWD: /sbin/iptables-save
```

3.7 Konfigurace klienta

Konfigurace klienta je výrazně snazší. Stačí nastavit rozhraní `wlan0`, aby získávalo IP adresu automaticky z DHCP serveru a `wpa_supplicant` pro připojení k Wi-Fi síti. Jak již bylo zmíněno, rozhraní se nastavuje v souboru `/etc/network/interfaces`. Zde smažeme konfiguraci k rozhraní `wlan0` a přidáme:

```
allow-hotplug wlan0
iface wlan0 inet dhcp
    wpa-conf /etc/wpa_supplicant/wpa_supplicant.conf
```

V souboru `/etc/wpa_supplicant/wpa_supplicant.conf` nastavíme název bezdrátové sítě (SSID) a ověřovací heslo.

```
network={
    ssid="rpi"
    psk="raspberry"
}
```

Nakonec stačí restartovat rozhraní `wlan0`, aby se projevíly změny.

```
$ sudo ifdown wlan0
$ sudo ifup wlan0
```

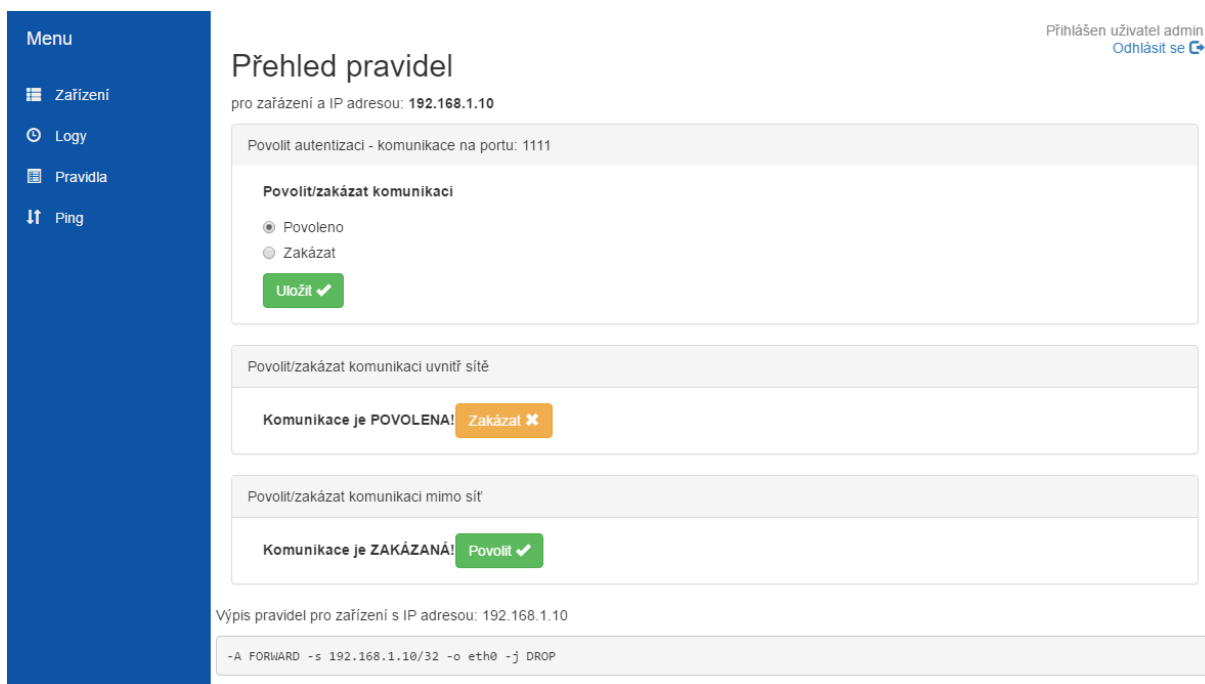
3.8 Uživatelská aplikace

Uživatelské webové rozhraní je jednoduché a intuitivní. Díky responsivnímu vzhledu lze webové rozhraní pohodlně ovládat na počítači i na mobilu. Skládá se z postranního menu a hlavního obsahu stránky. Webové rozhraní využívá framework Bootstrap. Je to velmi populární HTML, CSS a JavaScript framework pro vývoj responsivních webových stránek. Menu je členěno do 4 záložek.

ID	ID zařízení	MAC adresa	Název	Autentizace	IP/Ping	Akce
1	000018a7d545	00:1F:1F:42:98:CF	Raspbery Pi	POVOLENO		
20	B827EB190000	B8:27:EB:19:4C:00	TestovacíZarizeni	ZAKÁZÁNO		
36	000018a6f611	00:1F:1F:42:98:CF	Zarizeni	ČEKÁ NA SCHVÁLENÍ		

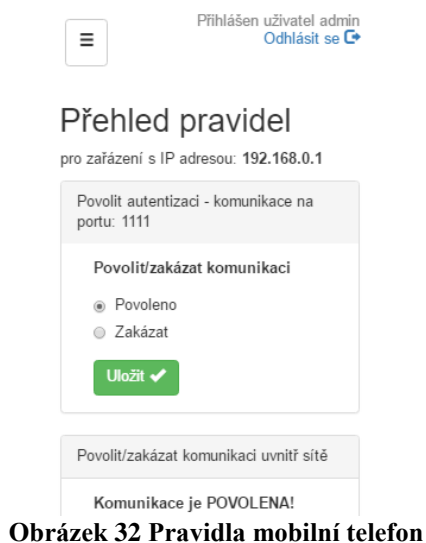
Obrázek 31 Přehled zařízení

Nejdůležitější část webového rozhraní je záložka Zařízení, která zobrazuje všechna uložená zařízení v systému a čekající zařízení na povolení k ověření. Každé zařízení má ID, unikátní ID (dle kterého se identifikuje), MAC adresu, název a stav autentizace (povoleno/zakázáno/čeká na schválení). Každé zařízení lze editovat, povolit, zakázat a odebrat. Zařízení můžeme filtrovat podle stavu. Dále je tu tlačítko pro ping, kterým můžeme ověřit, která zařízení jsou skutečně připojena v síti. Ping je prováděn na základě MAC adresy zařízení, z které se zjistí IP adresa daného zařízení. Po kliknutí na vybrané zařízení dojde k přesměrování do záložky pravidla, která umožňuje nastavovat pravidla v iptables.



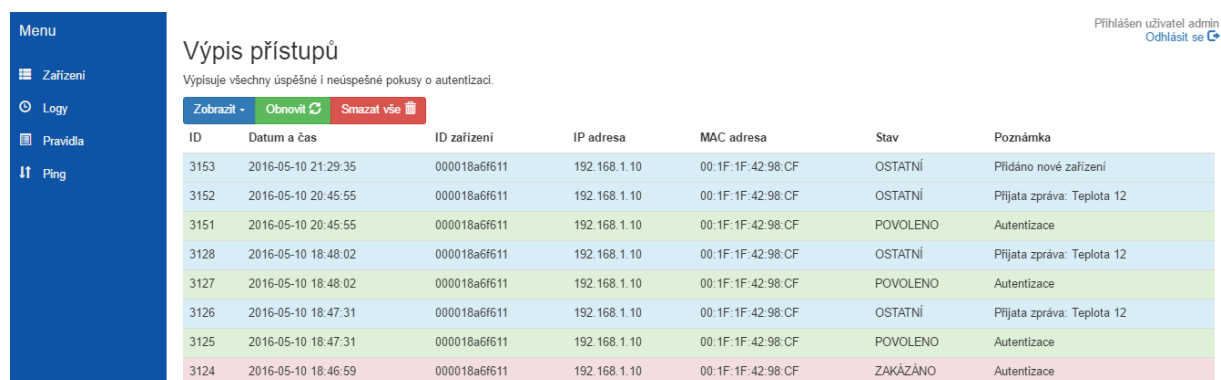
Obrázek 33 Pravidla

V záložce pravidla lze editovat jednotlivá pravidla síťového provozu. Lze povolit/zakázat komunikaci na portu 1111, na kterém funguje autentizační server. Dále je možné zakázat/povolit komunikaci uvnitř sítě. Tato možnost je vhodná, pokud zjistíme, že se zařízením není něco v pořádku nebo je podezření, že bylo napadeno. Poslední možností je povolení/zakázání komunikace mimo síť. To je další možnost, jak předcházet případným problémům. Pokud je dané zařízení určeno pouze ke komunikaci se serverem na lokální síti, je nežádoucí, aby mohlo komunikovat mimo síť. Ve spodní části je výpis všech pravidel pro dané zařízení a IP adresu.



Obrázek 32 Pravidla mobilní telefon

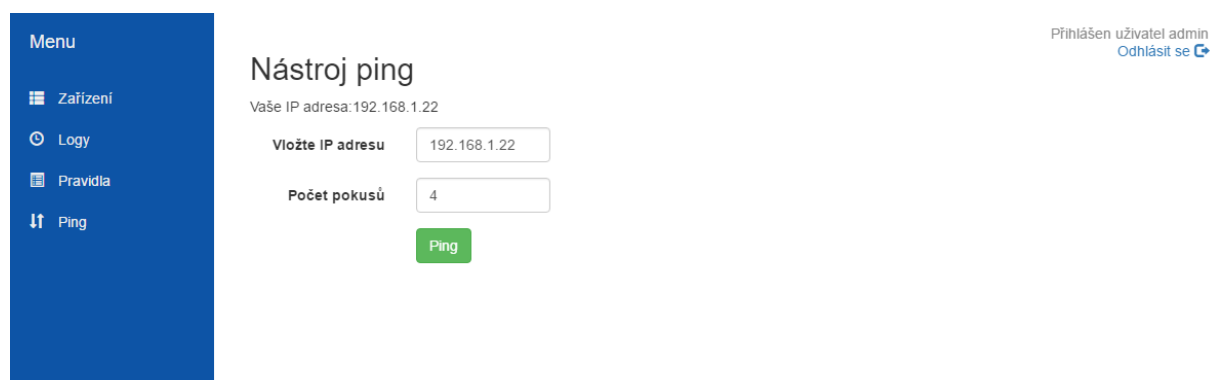
Záložka Logy zobrazuje logování autentizace. Je možné vidět úspěšné a neúspěšné pokusy o ověření. Také se zde logují nová zařízení, která se poprvé připojila do sítě (zařízení s novým unikátním kódem).



ID	Datum a čas	ID zařízení	IP adresa	MAC adresa	Stav	Poznámka
3153	2016-05-10 21:29:35	000018a6f611	192.168.1.10	00:1F:1F:42:98:CF	OSTATNÍ	Přidáno nové zařízení
3152	2016-05-10 20:45:55	000018a6f611	192.168.1.10	00:1F:1F:42:98:CF	OSTATNÍ	Přijata zpráva: Teplota 12
3151	2016-05-10 20:45:55	000018a6f611	192.168.1.10	00:1F:1F:42:98:CF	POVOLENO	Autentizace
3128	2016-05-10 18:48:02	000018a6f611	192.168.1.10	00:1F:1F:42:98:CF	OSTATNÍ	Přijata zpráva: Teplota 12
3127	2016-05-10 18:48:02	000018a6f611	192.168.1.10	00:1F:1F:42:98:CF	POVOLENO	Autentizace
3126	2016-05-10 18:47:31	000018a6f611	192.168.1.10	00:1F:1F:42:98:CF	OSTATNÍ	Přijata zpráva: Teplota 12
3125	2016-05-10 18:47:31	000018a6f611	192.168.1.10	00:1F:1F:42:98:CF	POVOLENO	Autentizace
3124	2016-05-10 18:46:59	000018a6f611	192.168.1.10	00:1F:1F:42:98:CF	ZAKÁZANO	Autentizace

Obrázek 34 Logování

Poslední záložka Ping je nástroj pro příkaz ping, který uživatel může využít k testování dostupnosti zařízení.



Nástroj ping

Vaše IP adresa: 192.168.1.22

Vložte IP adresu: 192.168.1.22

Počet pokusů: 4

Ping

Obrázek 35 Záložka Ping

4 Závěr

Cílem teoretické části bylo seznámení s Internetem věcí a jeho možnostmi využití. Část teoretické části popisuje situaci v České republice. Momentálně jsou u nás dva velcí hráči. Jsou to České Radiokomunikace, které používají otevřený standard LoRa a T-Mobile, který využívá komerční řešení SIGFOX. Dále byla popsána přenosová média, která se dělí na drátová a bezdrátová. Největší důraz byl kladen na média bezdrátová. Hlavním důvodem je lepší využitelnost pro Internet věcí, zejména kvůli mobilitě a škálovatelnosti.

Jedna kapitola byla také vyhrazena pro analýzu bezpečnostních rizik. Ta popisuje možná úskalí Internetu věcí, které je potřeba vyřešit. Dále byly představeny možné typy útoků, které známe již dnes. Útoky jsou rozděleny na pasivní a aktivní. Poslední část obsahuje možná doporučení pro zlepšení bezpečnosti. Je velmi obtížné polemizovat o dalších, či dokonce nových typech útoků na zařízení a komunikaci v Internetu věcí, především kvůli neustálému vývoji. Bude velmi zajímavé sledovat dění kolem Internetu věcí a bezpečnosti. Určitě se najdou sofistikované a nové typy útoků zaměřené právě na Internet věcí. Otázkou je, jak se vývojáři a vědci poučili z minulých let, a zda to pomůže k vytvoření bezpečného Internetu věcí.

Praktická část je věnována samotnému návrhu a implementaci řešení. Existuje jedno optimální řešení? Ne. Internet věcí je velmi různorodý, jak v jeho využití, tak v použitých technologiích. Jiné nároky na bezpečnost bude mít chytrá domácnost a jiné nároky zase budou například v průmyslu a výrobě. Pokud útočník napadne chytrou domácnost, může s nadsázkou přitápnout nebo zhasínat světlo. Nemá to však takový dopad jako v průmyslu, kde by následky útoku mohly být mnohonásobně větší. Dalším příkladem může být čidlo monitorující teplotu na severním pólu, které odesílá zprávu jednou denně nebo chytrá rozvodná skříň energetické sítě, která vyžaduje vyšší stupeň zabezpečení.

Navrhované řešení je zaměřeno na domácí prostředí. K ověření zařízení je využito integrovaného obvodu DS2401, který poskytuje unikátní 48bitové číslo. Dle unikátního čísla dochází k ověření zařízení. Lze říci, že unikátní číslo představuje druhou MAC adresu zařízení, která je však skryta. Samotná komunikace zařízení je řešena pomocí socketové komunikace. Ověřovací server umožňuje ověřit více klientů zároveň pomocí vláken. Pro každé nové připojení se vytváří nové vlákno, které se stará o ověření a komunikaci s daným zařízením. Průběh ověření je logován a ukládán do databáze. Také bylo vytvořeno uživatelské webové rozhraní, které je responzivní a umožňuje pohodlné ovládání na počítači i mobilním telefonu.

Webové rozhraní obsahuje přehled zařízení a jejich editaci, výpis logů, nastavování síťových pravidel a nástroj pro ping.

Literatura

About Z-Wave. *Sigma Designs* [online]. 2015 [cit. 2016-03-01]. Dostupné z: <http://www.z-wave.com/about>

A Guide to the Internet of Things Infographic. *Intel* [online]. 2015 [cit. 2016-03-01]. Dostupné z: <http://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html>

ASHTON, Kevin. That 'Internet of Things' Thing. In: *RFID Journal* [online]. 2009 [cit. 2016-02-16]. Dostupné z: <http://www.rfidjournal.com/articles/view?4986>

Bluetooth core specification. 2015 *Bluetooth* [online]. [cit. 2016-03-05]. Dostupné z: <https://www.bluetooth.com/specifications/bluetooth-core-specification>

Budujeme síť pro internet věcí na technologii Lora. *České radiokomunikace* [online]. 2016 [cit. 2016-03-01]. Dostupné z: <https://www.radiokomunikace.cz/budujeme-sit-pro-internet-veci>

DS2401 Silicon Serial Number. 2015. *Maxim Integrated* [online]. [cit. 2016-04-17]. Dostupné z: <https://datasheets.maximintegrated.com/en/ds/DS2401.pdf>

Historical trends in the usage of web servers for websites. 2016. *World Wide Web Technology Surveys* [online]. [cit. 2016-04-16]. Dostupné z: http://w3techs.com/technologies/history_overview/web_server

HUI, Jonathan, David CULLER a Samita CHAKRABARTI. *6LoWPAN: Incorporating IEEE 802.15.4 into the IP architecture*. Internet Protocol for Smart Objects (IPSO) Alliance [online]. 2009 [cit. 2016-03-10]. Dostupné z: <http://www.ipso-alliance.org/wp-content/media/6lowpan.pdf>

HUI, J. a P. THUBERT. *Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks* [online]. In: . IETF, 2011 [cit. 2016-03-10]. ISSN 2070-1721. Dostupné z: <https://tools.ietf.org/html/rfc6282>

IEEE COMPUTER SOCIETY. 2011. *IEEE standard for local and metropolitan area networks: Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)* [online]. New York: Institute of Electrical and Electronics Engineers [cit. 2016-02-20]. ISBN 978-073-8166-841. Dostupné z: <http://standards.ieee.org/getieee802/download/802.15.4-2011.pdf>

Internet of things research study: 2015 report [online]. 2015. Hewlett Packard Enterprise [cit. 2016-05-04]. Dostupné z: <http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf>

Internet věcí- zahájení pilotního provozu. *České radiokomunikace* [online]. 2015 [cit. 2016-03-01]. Dostupné z: <https://www.radiokomunikace.cz/internet-veci-zahajeni-pilotniho-provozu>

ISC DHCP: Enterprise Grade Solution for Configuration Needs. 2016. *Internet Systems Consortium* [online]. [cit. 2016-04-16]. Dostupné z: <https://www.isc.org/downloads/dhcp/>

JELÍNEK, Václav. *Využití protokolu 802.1x pro ISP*. Pardubice, 2014. Bakalářská práce. UPCE, Fakulta elektrotechniky a informatiky.

JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. ISBN 978-80-247-1561-2.

LoRaWAN™ What is it?: A technical overview of LoRa® and LoRaWAN™. *LoRa Alliance* [online]. 2015 [cit. 2016-03-05]. Dostupné z: <https://www.lora-alliance.org/portals/0/documents/whitepapers/LoRaWAN101.pdf>

MILLER, Michael. *The Internet of things: how smart TVs, smart cars, smart homes, and smart cities are changing the world*. 2015. Indianapolis, Indiana: Que, 2015. ISBN 0789754002.

New product launch! Introducing Raspberry Pi Model B+. *Raspberry Pi* [online]. 2014 [cit. 2016-04-18]. Dostupné z: <https://www.raspberrypi.org/blog/introducing-raspberry-pi-model-b-plus/>

OSEDEĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, 2004. ISBN 80-251-0106-1.

SATRAPA, Pavel. *IPv6: internetový protokol verze 6*. 3., aktualiz. a dopl. vyd. Praha: CZ.NIC, c2011. CZ.NIC. ISBN 978-80-904248-4-5.

Securing the Internet of Things: A Proposed Framework. *Cisco* [online]. 2015 [cit. 2016-03-04]. Dostupné z: <http://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html>

SHELBY, Zach. a Carsten. BORMANN. *6LoWPAN: the wireless embedded internet*. Chichester, U.K.: J. Wiley, c2009. ISBN 04-707-4799-4.

SIGFOX: Nová Bezdrátová síť pro "Internet věcí" v České republice. *T-Mobile* [online]. 2015 [cit. 2016-03-01]. Dostupné z: <http://www.t-mobile.cz/cs/tiskove-materialy/tiskove-zpravy-t-mobile/sigfox-nova-bezdratova-sit-pro-internet-veci-v-ceske-republice.html>

STACHOWICZ, Arthur. ZigBee Wireless Networks. In: *PBworks*[online]. Cleveland State University, 2010 [cit. 2016-03-06]. Dostupné z: <http://zigbee.pbworks.com/w/page/25465049/ZigBee#LayerStack>

Technologie SIGFOX. 2016. *SimpleCell* [online]. Praha [cit. 2016-05-08]. Dostupné z: http://www.simplecell.eu/pages/technologie_sigfox/

The Internet of Secure Things: What is Really Needed to Secure the Internet of Things? 2016. *Icon Labs* [online].[cit. 2016-05-04]. Dostupné z: <http://www.iconlabs.com/prod/internet-secure-things-%E2%80%93-what-really-needed-secure-internet-things>

Things [online]. 2016 [cit. 2016-03-01]. Dostupné z: <https://things.cz/free/>

VAN DER MEULEN, Rob. Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015. In: *Gartner* [online]. Stamford, 2015 [cit. 2016-03-01]. Dostupné z: <http://www.gartner.com/newsroom/id/3165317>

VAŠINA, Milan, Milan HÁBA a Jan JOHN. T-MOBILE: BUDOUCNOST PATŘÍ INTERNETU VĚCÍ. In: *T-Mobile*[online]. 2015 [cit. 2016-03-01]. Dostupné z: <http://t-mobile.cz/cs/files/get?file=150910-inovace-strategicka-fin.pdf>

VERMESAN, Dr. Ovidiu a Dr. Peter FRIESS. Internet of things: converging technologies for smart environments and integrated ecosystems [online]. 2013 [cit. 2016-02-20]. ISBN 9788792982964. Dostupné z: http://www.internet-of-things-research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf

Vstupujeme do internetu věcí. *České radiokomunikace* [online]. 2015 [cit. 2016-03-01]. Dostupné z: <https://www.radiokomunikace.cz/vstupujeme-do-internetu-veci>

ZigBee Specification. *ZigBee Alliance* [online]. ZigBee Alliance, 2012 [cit. 2016-03-06]. Dostupné z: <http://www.zigbee.org/download/standards-zigbee-specification/>