ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA ELEKTROTECHNICKÁ

Katedra elektromechaniky a výkonové elektroniky

BAKALÁŘSKÁ PRÁCE

Komerční jednotky pro bezdrátovou komunikaci na krátké vzdálenoti

Tomáš Portášik **2018**

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta elektrotechnická
Akademický rok: 2017/2018

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Tomáš PORTÁŠIK**
Osobní číslo:	**E15B0246P**
Studijní program:	**B2644 Aplikovaná elektrotechnika**
Studijní obor:	**Aplikovaná elektrotechnika**
Název tématu:	**Komerční jednotky pro bezdrátovou komunikaci na krátké vzdálenosti**
Zadávající katedra:	**Katedra elektromechaniky a výkonové elektroniky**

Zásady pro vypracování:

1. Proveďte průzkum trhu a možností v oblasti komerčních řešení bezdrátových komunikací na krátkou vzdálenost cca do 10 m.
2. Vyberte podle prvního bodu zadání vhodné řešení s optimalizací parametrů cena, komunikační rychlost, vzdálenost bezchybové komunikace a spotřeba.
3. Otestujte na funkčním vzorku komunikaci a ověřte teoretické předpoklady předchozích bodů zadání.

Rozsah grafických prací:	**podle doporučení vedoucího**
Rozsah kvalifikační práce:	**30 - 40 stran**
Forma zpracování bakalářské práce:	**tištěná/elektronická**

Seznam odborné literatury:

1. **Faludi, Robert; Building wireless sensor networks.**

Vedoucí bakalářské práce:	**Ing. Josef Justa** Katedra technologií a měření
Datum zadání bakalářské práce:	**10. října 2017**
Termín odevzdání bakalářské práce:	**7. června 2018**

Doc. Ing. Jiří Hammerbauer, Ph.D.
děkan

Prof. Ing. Václav Kůs, CSc.
vedoucí katedry

V Plzni dne 10. října 2017

Abstrakt

Tato bakalářská práce popisuje vybrané bezdrátové technologie používané pro přenos dat na krátké vzdálenosti. Jsou zde rozebrány výhody, nevýhody jednotlivých komerčních jednotek, jejich zabezpečení, typ přenosu a jejich různé standardy. Na konci experimentální části porovnává jednotlivé technologie, pro usnadnění výběru některé z technologií. V praktické části je přiblížen standard Bluetooth 4.0. a naprogramován na desce Arduino UNO R3.

Klíčová slova

Bezdrátová komunikace, technologie, specifikace, standard, WiFi, Bluetooth, ZigBee, modulace, data, zabezpečení, přenos dat, informace, rádiová komunikace, signál, spektrum, frekvence, frekvenční pásmo, spotřeba, uzel, Z-Wave, RFID, NFC, spotřeba energie, BLE, HM-10 modul.

Abstract:

This bachelor thesis describes selected wireless technologies used for short-distance data transmission. There are here dismantled benefits, disadvantages individual commercial units, their security, type transmission and their different standards. At the end of the experimental part, it compares individual technologies to facilitate the selection of some of the technologies. In the practical part is Bluetooth 4.0. and programmed on the Arduino UNO 3 board.

Key words

Wireless communication, technology, specifications, standard, Wifi, Bluetooth, ZigBee, modulation, data, security, data transfer, information, radio communication, signal, spectrum, frequency, frequency band, consumption, node, Z-Wave, RFID, NFC, power consumption, BLE, HM-10 module.

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně, s použitím odborné literatury a pramenů uvedených v seznamu, který je součástí této bakalářské práce.

Dále prohlašuji, že veškerý software, použitý při řešení této bakalářské práce, je legální.

.....

podpis

V Plzni dne 06.06.2018 Tomáš Portášik

Poděkování

Tímto bych rád poděkoval vedoucímu bakalářské práce Ing. Josefu Justovi, za cenné profesionální rady, připomínky a metodické vedení práce.

Obsah

Seznam symbolů a zkratek

BLE ..... - ; Bluetooth Low Energy

BSIG ..... Speciální zájmová skupina Bluetooth; The Bluetooth Special Interest Group

ČTU ..... Český telekomunikační úřad; -

EPC ..... Projekt energetických úspor; Electronic Product Code

GAP ..... Generický přístupový profil; Generic Access Profile

GATT ..... Generický profil atributů; Generic Attribute Profile

GFSK ..... Gausssovo frekvenční posun klíčováním; Gaussian frequency-shift keying

IEEE ..... Institut pro elektrotechnické a elektronické inženýrství; Institute of Electrical and Electronics Engineers

IoT ..... Internet věcí; Internet of Things

LAN ..... Lokální síť; Local Area Network

MAC ..... Fyzická adresa zařízení; Media Access Control

MAN ..... Metropolitní síť; Metropolitan Area Network

NFC ..... - ; Near field communication

OFDM ..... Ortogonální multiplex s frekvenčním dělením; Orthogonal Frequency Division Multiplexing

PAN ..... Osobní síť; Personal Area Network

PSK ..... Klíčování fázovým posuvem; Phase-shift keying

QoS ..... Kvalita služeb; Quality of Service

RFID ..... Identifikace na rádiové frekvenci; Radio Frequency Identification

SSID ..... Identifikátor sítě; Service Set Identifier

UUID ..... Univerzálně jedinečný identifikátor; Universally unique identifier

VoIP ..... Hlas přes internetový protokol; Voice over Internet Protocol

WAN ..... Rozlehlá síť; Wide Area Network

WECA ..... - ; Wireless Ethernet Compatibility Alliance

WEP ..... Soukromí ekvivalentní drátovým sítím; Wired Equivalent Privacy

WLAN ..... Bezdrátová lokální síť; Wireless Local Area Network

WPA ..... Chráněný přístup k Wi-Fi; Wi-Fi Protected Access

Úvod

V dnešní době je již velmi rozšířené používání bezdrátových sítí. Stále se ale, najde větší procento uživatelů používající komunikaci vedenou pomocí metalických a optických kabelů. Tato komunikace se stává v dnešní době velice nepraktickou a je nahrazována bezdrátovými sítěmi, z důvodu možnosti připojení se odkudkoliv k dané síti, a tudíž možnosti volně se pohybovat. Volnost pohybu je u bezdrátových sítí jedna z hlavních výhod. Další výhodou je také ekonomická stránka, jelikož není potřeba kupovat si kabeláž. Mezi další výhody patří také velmi jednoduchá rozšiřitelnost a jednoduchost připojení dalšího zařízení k již vytvořené síti. Z hlediska bezpečnosti a rychlosti je stále ve výhodě síť pomocí kabeláže. Proto spoustu lidí ještě tuto síť používá.

Především díky volnosti pohybu a jednoduché rozšiřitelnosti, dnes zažívají tyto bezdrátové sítě velký rozkvět. Nepoužívají se pouze k připojení k internetu, ale díky pohodlí se začaly rozšiřovat i k ovládání veškeré elektroniky. Začínají se stavět chytré domy, parkoviště a lavičky.

Máme tři nejvýznamnější bezdrátové přenosy dat pomocí sonické komunikace. Tento styl bezdrátové komunikace je ze všech tří nejstarší a známe ji pod pojmem řeč. Tato komunikace, blízká pro všechny, si našla uplatnění i v elektronice, a to především v ponorkách. Dalším typem je optická bezdrátová komunikace, která má, vzhledem k dnešní době, několik velmi důležitých nevýhod. A proto je dnes nejvíce rozšířeným typem bezdrátové komunikace v elektrotechnice rádiová komunikace. V ní dnes vidím největší možnost posunu směrem k budoucnosti. Proto jsem se rozhodl zacílit tuto práci především na rádiovou komunikaci.

Začátkem práce se nejprve věnuji bezdrátové komunikaci jako takové, a tudíž samotným přenosem dat, modulaci a rozdělení sítí. Dále se věnuju ve své bakalářské práci danému rozdělení bezdrátové komunikace podle typu přenosu. Následně se věnuji již samotným technologiím přenosu, u kterých rozebírám zabezpečení, standardizaci, výhody i nevýhody. Konec práce je zaměřen na bezdrátový přenos prostřednictvím Bluetooth 4.0 + LE. Přenos probíhá prostřednictvím desky Arduino UNO 3. V práci se také snažím vysvětlit, jak probíhá samotný přenos prostřednictvím tohoto standardu.

Cílem této bakalářské práce je věnovat se bezdrátové komunikaci a jejímu použití ke komunikaci na krátké vzdálenosti. Z důvodu největšího uplatnění směrem do budoucnosti se především věnuji rádiové komunikaci. Proto bych vás zde velmi rád seznámil s možnostmi, které tato bezdrátová komunikace nabízí, ať se již jedná o Wi-Fi,

Bluetooth, Z-Wave, Insteon, NFC, RFID či ZigBee. Práce má posloužit jako pomocník při výběru bezdrátové technologie, pro komunikaci s jakýmkoliv elektronickým zařízením. Proto se zde věnuji specifikaci technologie, zabezpečení, ale také výhodami a nevýhodami, každé z uvedených typů komunikace radiové komunikace.

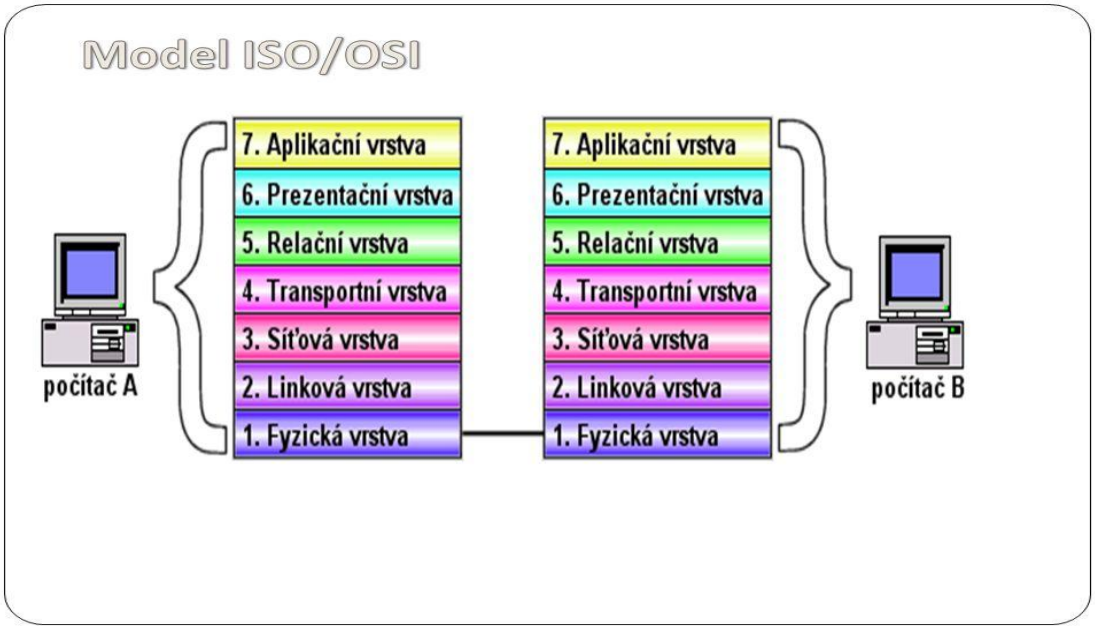
.

1 Bezdrátová komunikace

1.1 Obecně

Bezdrátová komunikace je propojení dvou subjektů (zařízení, uživatelů), které spolu komunikují jinak než prostřednictvím kabeláže (metalických kabelů, optických kabelů…). Mediem pro šíření jejich signálů se stává především vzduch, voda a jiné materiály. Bezdrátové sítě nabízejí v principu podobné služby, ale s mnohem větší flexibilitou. Je možné do nich zapojit, stejně jako u drátového připojení, servery koncového uživatele, ale také je možné vytvořit připojení peer-to-peer. [3][8][10]

U bezdrátové komunikace se pro přenos dat používá ISO/OSI model. Jedná se o referenční komunikační model, či TCP/IP model, či jejich upravená verze. ISO/OSI model se skládá ze 7 vrstev. TCP/IP model se skládá pouze ze 4 vrstev. K přenosu používají různé technologie pocházející většinou jen některé z těchto vrstev. Vrstvy se starají o zapouzdření dat, vyhledání příjemce a další softwarové rozpracování dat. [3][8]



Obr. 2.1 Model ISO/OSI [3]

Fyzická vrstva s linkovou má za úkol danou zprávu komunikace upravit na signál, který se dá přenášet. Dnes se jedná především o digitální formu signálu, proto je zde nutný A/D a D/A převodník. Zpracování digitálního signálu se děje tak, že signál je nejprve pomocí vzorkování rozkouskován podle vzorkovací frekvence, následně dochází ke kvantování a signál se stává diskrétním. Již i v amplitudě, nejen v čase, je nakonec podle kvantizačních hodnot zakódován (přiřazení vhodné kombinace kvantizačním hladinám) a

následně může být signál přenesen. Linková vrstva se stará především o adresaci pomocí MAC adres. K tomuto procesu slouží také hardwarová část, zdroj, kodér, modulátor, A/D a D/A převodník, anténa, demodulátor, dekodér. Síťová vrstva má za úkol především směrování, hledání nejlepší cesty, ale také zapouzdření segmentu do paketu. Segment přichází z transportní vrstvy, která se stará o spolehlivost neboli o potvrzení komunikace, o komunikaci mezi aplikacemi, a dokonce o vkládání dat do segmentu. Vrstva pět, relaxační, se stará o udržení ukončení komunikace, zabezpečení komunikace, šifrování. Prezenční a aplikační vrstva se starají již o komunikaci mezi samotnými uživateli, kompresi a dekompresi dat a jejich šifrování. Bezdrátová komunikace se dělí podle typu přenosu signálu: [7][8]

- Sonická komunikace
- Optická bezdrátová komunikace
- Rádiová komunikace

1.1.1 Modulace

Modulace je nelineární proces, kterým se dá změnit charakter nosného signálu za pomoci modulujícího signálu. Základem je směšovač, který k modulačnímu signálu přidává nosný signál. Modulovaný signál vzniká prostřednictvím změn jednotlivých harmonických signálů, na které se dají nanést určitá data, a dále je přenášet. Základní typy modulace jsou:

- Amplitudová modulace - při níž jsou určité logické hodnoty zakódovány určitými hodnotami.
- Fázová modulace – jednotlivé hodnoty jsou vyjádřeny pomocí změny fáze.
- Frekvenční modulace – jednotlivé logické hodnoty jsou vyjádřeny různou frekvencí.

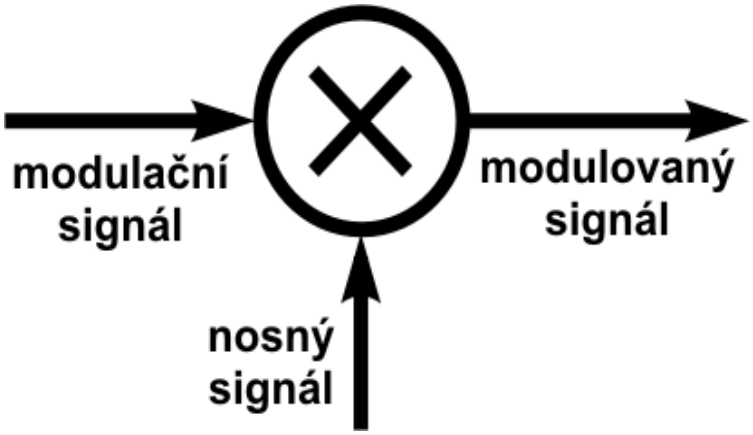
Dalším důležitým rozdělením je podle typu nosného signálu:

- Spojité analogové modulace – nosným signálem je signál s harmonickým průběhem, modulačním signálem je analogový signál.
- Spojité digitální modulace - nosným signálem je signál s harmonickým průběhem, modulačním signálem je digitální (diskrétní) signál.
- Diskrétní modulace – nosným signálem je signál s nespojitým průběhem (taktovací signál.

[42]

Podle dané modulace dojde ke klíčování signálu, rozložení a jeho zakódování.

Některou z těchto forem modulace, klíčování fázovým posuvem, lze po rozložení signálu dále přenášet.



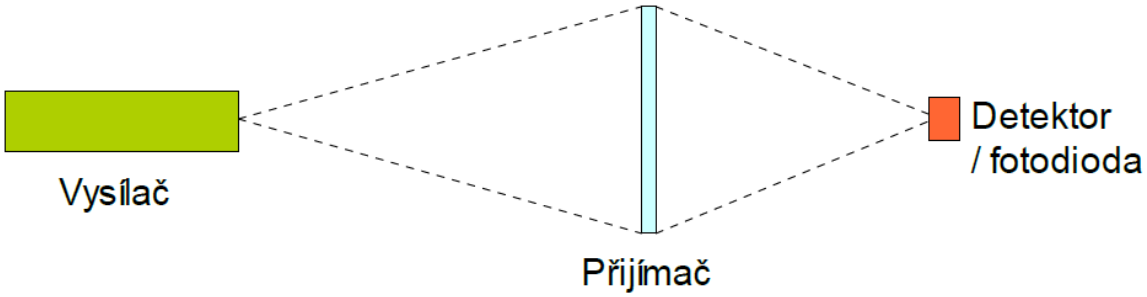
Obr. 2.2 Schematická značka modulátoru [42]

1.1.2 Sonická bezdrátová komunikace

Jedná se o bezdrátovou komunikaci, formou zvuku. Princip je podobný jako orientace při letu u netopýrů. Do bezdrátové komunikace lze zařadit i naši běžnou mluvu. Tento druh komunikace se používá v elektrotechnice u ponorek formou ultrazvukových pojítek. Jde o komunikaci krátkého dosahu, která zahrnuje přenos a příjem zvuku. [10]

1.1.3 Optická bezdrátová komunikace

Principem této bezdrátové technologie je vysílání optického, světelného signálu (nejmenší částice foton) z vysílacího zařízení k přijímači volným prostorem, většinou vzduchem. Pro přenos se používají optické signály, pulzně modulované o frekvenci 100-1000 THz. Každý spoj se skládá z jednoho přijímače a jednoho vysílače. Vysílač má za úkol vyslat světla o největším možném výkonu tak, aby dopadlo na plochu přijímače. Plocha přijímače následný signál přijme a usměrní je do detektoru a dále zpracovává. Přijímač se konstruuje tak, aby měl největší plochu a dokázal usměrnit velké množství signálů do fotodiody. Jelikož detektor je velmi malý, kladou se velké nároky na správné upevnění přijímače, aby nedocházelo k vychýlení, a také na používaní samonaváděcí systémy. Jako světelný zdroj se používá LED dioda či laser. Každý ze světelných zdrojů se hodí více pro jinou situaci, například výhodou laseru je jeho výkon, naopak nevýhodou se stává potřeba chlazení, cena a složitost obvodů.



Obr. 2.3 Optický přenos

Mezi výhody optického spoje patří velmi snadná instalace (spočívající v pouhém zaměření a namontování), bezpečnost a vysoká rychlost.

Nevýhodou však těchto sítí je vzdálenost použití, která je limitována několika kilometry a rušení při horším počasí, snížené viditelnosti, i přes odolání silnému dešti, sněžení či husté mlze, je doporučováno mít záložní zdroj.

V komunikaci na krátké vzdálenosti je jejich největší nevýhodou nutnost volného prostoru mezi vysílačem a přijímačem, což je v dnešní době nechtěné, proto se od této komunikace upouští a nahrazuje jí rádiová komunikace. Mezi komerční jednotky této komunikace patří IR spotřebitelská zařízení (dálková ovládání) a IrDA síť, která slouží jako alternativa k Bluetooth přenosu mezi dvěmi zařízeními (počítači, telefony, digitálními kamerami).

1.2 Rádiová komunikace:

Rádiová komunikace má dnes, díky IoT, největší bujnost. Jedná se o nejlepší možnost bezdrátové komunikace na krátké vzdálenosti. Signál je mezi dvěma body posílán pomocí rádiových vln. Největší předností této komunikace je nepotřeba přímé viditelnosti mezi dvěma komunikujícími uzly. Tato komunikace je realizována pomocí rádiového kanálu pro přenos rádiových vln:

- Přímá rádiová vlna – potřeba přímé viditelnosti.
- Povrchová rádiová vlna – šíří se na rozhraní země a vzduch. Je doprovázena ztrátamy při průchodu různými prostory. Při průchodu vzduch země se vlna utlumí, citlivá na atmosférické, elektrizační a průmyslové poruchy.
- Prostorová rádiová vlna – složena z přímé a odražené vlny, na přijímači součet či rozdíl těchto vln.
- Šíření rádiové vlny troposférickým rozptylem – šíření v troposféře

(nehomogenní prostředí) vlna má zakřivenou trajektorii, dochází k odrazu a útlumu na hydrometeorech (mlha, sníh apod.).

- Šíření rádiové vlny odrazem od ionosféry – šíření je tvořeno rozptylem, odrazem vln od nehomogenit a difuzním rozptylem. Ionosféra má schopnost odrážet rádiové vlny zpět k povrchu. Je závislá na ročním období, používá se k šíření rádiových vln na dlouhé vzdálenosti. Ionosféra se nachází 60 – 600 km nad povrchem země.

[11] [12] [45]

Rádiové vlny jsou elektromagnetické vlnění v kmitočtovém pásmu od 10kHz až do 3000GHz. Tento rozsah je od několika desítek kilometrů až 0,1mm. Mediem pro rádiové vlny se stává především vzduch. Rádiové vlny dělíme podle různé vlnové frekvence na různé typy vln: [11] [12]

Tab. 2.1 Základní rozdělení rádiových vln [11]

Číslo pásma	Symboly	Rozsah kmitočtů	Názvy pásem	Metrické zkratky
4	VLF	3 – 30 kHz	Myriametrové	Mam
5	LF	30 – 300 kHz	Kilometrové	km
6	MF	300 – 3000 kHz	Hektometrové	Hm
7	HF	3 – 30 MHz	Dekametrové	Dm
8	VHF	30 – 300 MHz	Metrové	m
9	UHF	300 – 3000 MHz	Decimetrové	dm
10	SHF	3 – 30 GHz	Centimetrové	cm
11	EHF	30 – 300 GHz	Milimetrové	mm

Důležitými, základními pojmy pro měření a výpočet přenosu jsou:

- Frekvence – Udává se v jednotce Hertz. Jedná se o počet opakování periodického děje za určitou časovou jednotku.
- Šířka pásma – Značí se písmenem B, jednotkou je Hertz. Jde o určitou šířku intervalu frekvence, rozdíl mezi nejnižší a nejvyšší frekvencí. Mimo toto pásmo je signál velmi utlumen, a má velké zkreslení. Kanály dělíme do tří kategorii: [11]
    - Širokopásmové – 25 kHz obsazení rádiového spektra.
    - Úzkopásmové – 12,5 kHz osazení rádiového spektra.
    - Ultra úzkopásmové – 6,5 kHz obsazení rádiového spektra.
- Modulace – viz str. 11.

- Modulační rychlost – vyjadřuje rychlost změn v přenášeném signálu, jednotky jsou Baudy.
- Přenosová rychlost – jde o údaj, který je závislý na šířce pásma a na kvalitě signálu. Kvalita signálu je udávaná pomocí odstupu signálu od šumu. Udává objem informace, jež byl přenesen za určitou časovou jednotku, tedy bity za sekundu.
- Spektrum signálu – jde o zobrazení signálu pomocí jeho frekvencí. Data můžem přenášet pomocí různých frekvencí. Zobrazením všech frekvencí v grafu pomocí amplitudy každé frekvence, získáme spektrum signálu.

1.2.1 Rozdělení rádiové komunikace

Rádiové komunikace se dají dělit podle několika možností, například podle rozsahu sítě:

- PAN (Personal Area Network) – jedná se o malou většinou osobní síť, s malou spotřebou, menší rychlost přenosu, rozsah v řádech metrů.
- LAN (Local Area Network) – jedná se o místní síť rozprostřenou několik desítek až stovek metrů, je v soukromé správě. Propojuje menší množství koncových uzlů mezi sebou. Rychlost přenosu se pohybuje v Mb/s, Gb/s.
- MAN (Metropolitan Area Network) – podobná jako LAN, ale na větším prostranství, například propojení města, rozsah až několik kilometrů.
- WAN (Wide Area Network) – rozsáhlá síť použitá především jako přenosová páteř, například pro poskytovatele internetu.

Dále podle vzdáleností komunikace na krátkou vzdálenost (Short-range) a dlouhou vzdálenost (Long-range). Dalším velmi podstatným dělením je podle licence pásma:

- Licencovaná pásma – jde o placenou část pásma, kterou může používat provozovatel až po přidělení, odsouhlasení a zaplacení pronájmu Českým telekomunikačním úřadem (ČTÚ). Tento úřad na základě splnění různých kritérii může povolit toto používání. Cena se odráží, závisí na pásmu, na vysílacím výkonu, šířce pásma a dalších důležitých parametrech. Licencovaná pásma používají, například pro letectvo, námořnictvo, rozhlas. Jsou však i společnosti, jež na něm využívají technologii WiFi, či WiMax.
- Bezlicenční pásma – jinak také ISM, na těchto pásmech může kdokoliv vysílat, a to naprosto volně, bez omezení, což je velká výhoda, avšak i nevýhoda. Může docházet k vzájemnému rušení, jelikož není garantována jedinečnost použití. Nejvíce vytíženým pásmem je 2400 – 2500 MHz. Na tomto pásmu vysílají svůj signál především jednotky pro krátkou rádiovou komunikaci, jako je WiFi,

Bluetooth, tak i jednotky na dlouhou komunikaci, například WiMax. I bezlicenční pásma jsou spravována ČTÚ.

Další rozdělení je na základě dostupnosti provedení a jeho standardizované řešení.
K tomuto řešení jsou vydávány standarty, podle nichž se řídíme. Tyto standarty jsou již otestované a volně dostupné. Naopak proprietární řešení je v rámci jedné firmy, či malého spolku firem, výhodné kvůli zabezpečení sítě. Toto řešení využívá i firma Telmo a.s.. [13]

Tab. 2.2 Rozdělení některých bezdrátových technologií.[13]

Technologie	Licence	Frekvence	Rozsah	Řešení
ZigBee	Bezlicenční	868 MHz, 2,4 GHz	PAN	Standard
WiFi	Bezlicenční	2,4 GHz, 5 GHz	LAN	Standard
GSM	Licenční	900 MHz, 1800 MHz	WAN	Standard
LTE	Licenční	800, 900, 1800, 2600 MHz	WAN	Standard
SigFox	Bezlicenční	868 MHz	WAN	Proprietární
Wimax	Licenční	3,5 GHz, 10,5 GHz	WAN	Standard
LoRaWAN	Bezlicenční	868 MHz	WAN	Open-standard
Bluetooth	Bezlicenční	2,4 GHz	PAN	Standard
Z-Wave	Bezlicenční	868 MHz, 915 MHz	PAN	Open source
Insteon	Bezlicenční	902 - 924 MHz	PAN	-

2 WiFi

WiFi je standard pro lokální bezdrátové sítě (WLAN). Je na něj vydána specifikace IEEE 802.11, z níž vycházejí různé specifikace pro WiFi. Původně šlo o licencovanou technologii, jež vlastnila a vytvořila aliance WECA (dnes Wi-Fi Alliance). Tato organizace přišla s názvem Wi-Fi, mělo jít o hříčku slov ze slova „Hi-Fi“. Zkratka WiFi je dnes chápána jako spojení dvou anglických slov „wireless“ a „fidelity“, do češtiny přeloženo jako bezdrátová věrnost. Později ve snaze rozšířit tuto technologii na sítě WLAN, byl standart popsán jako IEEE 802.11. Původním cílem sítí WiFi bylo zajišťování bezdrátového spojení, přenosným zařízením, a ty následně propojovat, připojovat na některou lokální sít LAN, MAN. Dnes lze skrz WiFi propojit snad veškerou spotřební elektroniku, poskytovat internet, či VoIP připojení. Díky různým standardům se technologie WiFi rozšířila i mezi IoT a přispívá také ke zvýšení bezpečnosti inteligentního dopravního systému. I když ústup od licencovaného pásma přinesl velký rozkvět, přinesl s

sebou i jednu nevýhodu, a to ve formě silného zahuštění frekvenčního pásma 2,4 GHz a 5GHz, které používá tato technologie. [5] [6][9][15]

V každé síti je typicky minimálně jeden Access Point a s ním i minimálně jeden klient. Access Point má funkci vysílání ve velmi malých časových intervalech SSID signál, čímž identifikuje síť. Tyto signály jsou tak malé, jak jen to umožňuje přenos přes WiFi (1Mbit/s). Díky tomu nijak nezpomalují ani nesnižují výkon sítě. SSID slouží jako jméno dané sítě (nejde přímo o jméno sítě ale jen o ID). Po seznámení uživatele se zařízením, se uživatel rozhodne, zda se pokusí k dané síti přes tento Access Point připojit. Standard WiFi má v tomto velkou výhodu. Jelikož nechává kritéria daného spojení na klientovy, či na připojeném zařízení, znamená to potřebu správného nastavení, aby byl využit celý potenciál připojení. WiFi používá k určení správnst potvrzovací pakety, které jsou poslány na začátku a na konci přenosu. [5][6][15]

WiFi využívá především 2,4GHz pásmo, které je bezlicenční. Toto pásmo však používá mnoho dalších technologií jako je Bluetooth. Z tohoto důvodu začala WiFi přecházet i na další pásmo, chárakterizováno 5GHz. WiFi na pásmu 2,4 GHz využívá u nás 13 různých kanálů, ty mají za úkol rozdělit více WiFi sítí mezi sebe, aby nedocházelo k vzájemnému rušení. [5] [6][14][15]

Obr. 3.1 Logo Wi-Fi aliance [4]

Důležité pojmy:

- Access Point – přístupový bod k síti, řídí komunikaci mezi všemi zařízeními v infrastrukturním režimu.
- Brána – vykonává funkci routeru. Jedná se o bod, který spojuje komunikaci dvou či více sítí.
- Firewall – jedná se o ochranu lokální sítě a dokáže omezovat přístup. Jsou různé možnosti této ochrany blokování portů, nastavení seznamu, zabránění přenosu při neznámém původu a mnoho dalších. Firewall lze nakonfigurovat a zvýšit tím zabezpečení sítě.
- QoS – řízení kvality služeb, pomocí protokolů QoS je možné zajistit, a rozdělit

dostupnou přenosovou kapacitu, tím nedochází k zahlcení sítě, naopak síť má vyšší kvalitu svých služeb.

2.1 Zabezpečení

U zabezpečení veškerých bezdrátových sítí, nejen sítí WiFi, se setkáváme s problémem snazšího nabourávání, než je tomu u drátových spojů. Důvodem problému je vzduchové medium, tedy volný prostor. Proto stačí útočníkovi všesměrová anténa, kterou se může připojit k některé z bezdrátových sítí. Útočník dokonce nemusí být přímo v této síti, která je pokrytá daným vysílačem, pokud má dostatečně výkonnou anténu. Proto je zabezpečení velmi důležité pro správné fungování sítě. Je tedy nesmírně důležité vždy změnit nastavení zabezpečení u nově koupeného produktu, jelikož přednastavené nastavení má většinou snadný klíč, heslo, či je úplně bez zabezpečení. [5][14]

Zabezpečení primárně dělíme do dvou skupin:

- Zabezpečení pomocí šifrování – především chrání proti odposlechům.
- Zabezpečení pomocí autorizace – zabraňuje přístupu do sítě nezvaným, nechtěným uživatelům

2.1.1 Typy zabezpečení

- Kontrola fyzické adresy - na Access Pointu je nastaven seznam adres zařízení (MAC adres), které mají odepřený přístup k síti či naopak povolen. Bohužel se dá tato adresa v zařízení změnit. Je to snadno prolomitelná ochrana. Stačí chvíli odposlouchávat a zachytit povolenou adresu.
- Skrytí SSID – tímto zabezpečením porušujeme standard, avšak jde o nejjednodušší typ zabezpečení bezdrátového připojení, pomocí jeho skrytí. To lze nevědomostí uživatele snažícího se nalézt síť. Tato síť se mu totiž neukáže, protože nezná broacasty a SSID. I toto zabezpečení je snadno prolomitelné, jelikož při přihlášení uživatele do sítě se SSID přenáší viditelně, a tak je snadné jej zachytit. Tímto se i může pošlat vir, který donutí zařízení k novému přihlášení.
- WEP – Jde o šifrovací způsob zabezpečení,WEP. Vznikl v roce 1999 jako původní zabezpečení normy 802.11. Zabezpečení se provádí pomocí WEP klíčů, symetrické šifry. Tyto klíče jsou ručně zadány na všech uzlech připojení, klíč má různé délky 64bitů, 128 bitů i více bitů. Kvůli nedostatkům v protokolu, lze zachytit unikátní rámec dat, z kterého se dá klíč formou speciálních programů snadno zjistit. Navíc k zabezpečení dochází pouze v komunikaci mezi uživatelem a přístupovým bodem.

- WPA – Vzniklo s cílem napravit slabá místa WEP a však použít hardware podporující WEP. WPA funguje podobně jako dřívější zabezpečení WEP, ale k šifrování využívá protokol TKIP, ten má standardně 128 bitový klíč, ale výhodou je jeho schopnost měnit klíč po 10 000 přenesených paketech. Tento klíč se tak stává plovoucím a dynamickým. K přihlášení do sítě skrz tuto ochranu se používá buď PSK (klíčování fázovým posuvem), nebo pomocí přihlašovacího serveru RADIUS.
- WPA2 – Vylepšení WPA, které je možné jen na kvalitnějším hardwaru, má důmyslnější šifrování.

[5][14]

2.2 Standardizace

WiFi používá standard IEEE 802.11. x. X je používáno jako označení několika doplňků, pro něž je tato specifikace použitelná. Tento standard zahrnuje několik druhů modulace pro přenos dat pomocí rádiového signálu, ale protokol je pro všechny stejný. Mezi nejpoužívanější modulace patří specifikace s písmeny a,b,g, a s písmenem n, ten však přináší jinou techniku modulace. Existuje i standard pro zlepšení zabezpečení, který má písmeno i. Ostatní specifikace pouze rozšiřují předchozí a již zmíněné specifikace. Různé standardy pracují také v jiném frekvenčním pásmu, například 802.11g přenáší na pásmu 2,4 GHz a je schopen komunikovat s bluetooth zařízením či mikrovlnou troubou. Tuto specifikaci nemůže provádět standard pracující na 5 GHz frekvenci.

Seznam specifikací najdeme na uvedeném zdroji [1] [4].

2.2.1 Důležité standardy

U nás jsou nejčastěji používané jen některé z výše uvedených standardů:

- IEEE 802.11a – používá 5 GHz pásmo, modulaci OFDM (ortogonální multiplex s frekvenčním dělením), modulace pracuje s rozprostřeným spektrem, kdy je vysílaný signál vysílán na větším množství vzájemně ortogonálních frekvencích, subnosných. Jeho povolený vyzařovací výkon je vyšší, a tím pádem lze používat na větší vzdálenost. Zároveň je stabilnější než například specifikace IEEE 802.11b či g.
- IEEE 802.11b – přenosové pásmo je 2,4GHz, rozšiřuje původní standard, zvyšuje rychlost na 11 Mbit/s.
- IEEE 802.11c – tato specifikace rozšiřuje standard d, věnuje se především

přemosťování v zařízeních pro bezdrátový přenos. Přidává požadavky na přemosťování fyzických adres.

- IEEE 802.11d – definuje požadavky na první vrstvu ISO/OSI modelu, fyzickou vrstvu. Říká se mu také globální harmonizační standard, jelikož posílá v paketu zároveň s ID sítě také kód země. Rozdíl od základního standardu je v povolených frekvencích, propustnosti a vyzařovacím výkonu. Vhodný pro poskytování globálního roamingu.
- IEEE 802.11e – Vylepšuje kromě linkové vrstvy (podvrstva MAC), také kvalitu služeb (QoS). A velmi dobře odstraňuje problém se zpožděním, proto je vhodný například pro VoIP.
- IEEE 802.11g – rozšiřuje IEEE 802.11b, zvyšuje jeho přenosovou rychlost až na 25 Mbit/s, navíc je zpětně kompatibilní.
- IEEE 802.11h – Evropský standard jež upravuje IEEE 802.11a pro použití i mimo budovy. Pracuje tedy na 5GHz pásmu, na kterém řeší rušení například od radarů, satelitů. Má za úkol deklarovat rušení a následně omezit výkon či pomocí dynamického výběru kanálů pro lepší pokrytí, přeskočit na volnější kanál. Upravuje fyzickou a linkovou vrstvu ISO/OSI modelu.
- IEEE 802.11n – upravuje fyzickou vrstvu a linkovou vrstvu tak aby bylo možné docílit mnohem větší rychlosti přenosu a to až 540 Mbit/s, dále zvyšuje dosah sítě, to vše díky technologii multiple input multiple output (více vstupů, více výstupů), jde o abstraktní matematický model, který používá multi-anténní systémy. Specifikace používá modulaci OFDM.

[1] [4]

2.3 Výhody, nevýhody

Výhody:

- Používá bezlicenční rádiové pásmo.
- Dosah až na několik stovek metrů, při použití všesměrové antény, možnost vybudovat LAA sítě.
- Velmi dobrá dostupnost na trhu
- Možnost použití 5 GHz frekvenčního pásma.
- Možnost použití vícero přístupových bodů (Access Pointů).
- Celosvětová komptabilita.

- Snadné vybudování infrastruktury.
- Možnost přenosu internetu i intranetu

Nevýhody:

- Bezpečnost, starší kryptovací standardy WEP či WPA, jsou celkem snadno přemožitelný, novější WPA2 je bezpečnější.
- Velké množství technologii na frekvenčním pásmu 2,4 GHz, které používají i některé standardy WiFi.
- Přidělená pásma a operační omezení nejsou na celém světě stejné, například USA, Japonsko a další mají jiné množství povolených kanálů.
- Vysoká spotřeba, což má negativní vliv na životnost baterie, porovnáme-li ji s technologií Bluetooth. Technologie Wi-Fi nebyla navržena na spotřebu energie, nýbrž na nejrychlejší přenos největšího množství dat. Zajímavostí však je, že standard 802.11g, který má vyšší vysílací výkon než standard 802.11b, je jeho spotřeba baterie nižší. U 802.11g je tento jev zapříčiněn především lepším využitím baterie a v případě nečinnosti, a kratšímu času pro vysílání, příjem dat. Spotřeba je dnes velmi zásadní z hlediska používání mobilních telefonů, notebooku a dalších podobných zařízeních.
- Ve frekvenčním pásmu 2,4 GHz má lepší dosah než na pásmu 5 GHz, ale toto pásmo je mnohem více používané.
- Při vzájemném působení uzavřených přístupových bodů na stejném či sousedním kanále, může zabránit přístupu klientů v oblasti s nezaheslovaným přístupovým uzlem, to může způsobit přetížení.
- Problémy v kompatibilitě různých výrobců, lehké odchylky, mohou snížit přenosovou rychlost. například při použití zařízení od výrobce Cisco Systems, a některého z méně kvalitních výrobců, nemají certifikaci například Cisco4.

[13] [14] [15]

3 Bluetooth

Jedním ze standardů pro připojení různých zařízení pro bezdrátovou komunikaci je Bluetooth. Jedná se o standart pracující na krátké vzdálenosti. Bluetooth používá ke komunikaci rádiové vlny. Bluetooth vzniklo roku 1994, kdy vzniká studie výrobce mobilních telefonů Ericsson, která měla snahu nahradit kabelové propojení ve spojení mobilních telefonů s jejich periferiemi. O 4 roky později vzniká skupina Bluetooth Special

Interes Group (*BSIG)*. BSIG tvoří společenství několika předních firem zabývajících se přenosem dat (Nokia, Intel, Microsoft a další). Hlavní myšlenkou bylo minimalizovat nekompatibilitu rozhraní různých typů zařízení, na krátké vzdálenosti, s co nejmenší energetickou zátěží pro bezdrátový přenos. Název Bluetooth má přitom odkazovat na vikingského krále Heralda II. (940-981), jež si vysloužil přezdívku, která se překládá do angličtiny jako Bluetooth. Během roku 2000 přichází na trh první výrobky se specifikací Bluetooth verze 1.0. V následujících letech se Bluetooth velmi rychle šíří, především prostřednictvím mobilních telefonů, handsfree, bezdrátových tiskáren, klávesnic a myší. Postupně se vyvíjí další verze 1.1, která opravovala chyby v předchozí verzi. Dále verze 1.2, která především zvětšila rychlost připojení. Následující verze 2.1, vyšla v roce 2007, velmi zvýšila bezpečnost technologie. Avšak změna přišla o dva roky později, kdy Bluetooth v3.0 +HS přináší rychlost přenosu až 24Mbit/s. I když se zde nejedná přímo o připojení pomocí Bluetooth, provádí se totiž přes souběžné připojení 802.11. Dále přichází v4.0, která však se nesnaží nahradit předešlou verzi, ale zaměřuje se především na ještě menší energetickou náročnost. Dnes se bluetooth používá například i ke komunikaci s chytrými žárovkami. Bluetooth spadá do kategorie WPAN a má standardizaci 802.15.1. [16][17][19]

3.1 Funkčnost

Jak již bylo uvedeno. Bluetooth se používá na krátké vzdálenosti a jeho dosah je v rozsahu desítek až stovek metrů, v závislosti na okolních faktorech jako viditelnost. Dosah až několik set metrů lze docílit díky anténě s vysokým ziskem. Při použití této antény je však zapotřebí dbát na pravidla ČTÚ, o vymezení maximálního výkonu antény, a co nejmenšímu ovlivnění již dostupných sítí, jinak se uvádí dosah až 200 m u Bluetooth 5 LE [43]. Technologie Bluetooth pracuje stejně jako WiFi v nelicencovaném pásmu 2,4GHz. Jelikož je toto pásmo využíváno právě i technologii WiFi a dalšími bezdrátovými technologiemi přenosu, je nutné zajistit to, aby se dané technologie na tomto frekvenčním pásmu nerušili. Proto se u Bluetooth využívá frekvenční skládání nosné v rozprostřeném spektru, a také velmi nízké vysílací výkony, pohybující se od 1mW až do 100mW. Podle dané výkonové třídy, ta také určuje maximální dosah. V České republice se používá šířka frekvenčního pásma 2,4-2,4835GHz vztah pro nosnou je

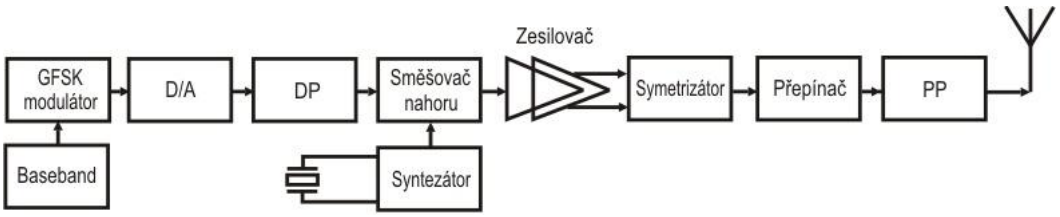
$$f_0 = 2402 + k\ [MHz], kde\ k \in < 0; 78 >$$

4.1

Jak lze podle vzorce vidět, jsou zde nevyužité kanály. Tyto se používají jako tzv. dolní ochranné pásmo, jehož šířka je 2MHz a horní postranní pásmo 7,5MHz. Jelikož šířka jednoho rádiového kanálu je 1 MHz máme možnost využití 79 kanálů.[16] [20]

Kvůli potlačení interference s dalšími signály se používá metoda kmitočtových skoků, s rychlostí 1600 skoků/s. Data se v paketech přenášejí ve velmi krátkých časových intervalech a frekvence se po každém přenosu mění, tím se zajistí lepší kvalita spojení. Bluetooth používá k modulaci Gaussovu modulaci s frekvenčním klíčováním (GFSK), pro zvýšení rychlosti se od verze 2.0 používá modulace 8-PSK. [16] [17]

3.2 Vysílač bluetooth



Obr. 4.1 Blokové schéma vysílače Bluetooth[16]

Vysílač bezdrátového signálu pomocí technologie Bluetooth má několik bloků. Prvním z nich je zdroj (Baseband), zde se provádí formátování dat do paketů. Jedná se o první, základní zpracování signálu, korekci chyb, šifrování či kanálové kódování. Jde o přidání různých bitů k signálu, které jsou nezbytné pro přenos či se přidávají z důvodu odstranění chyb vzniklých při přenosu. Následuje GFSK modulátor, zde se provádí klíčování frekvenčním posuvem. Předtím však prochází Gaussovským filtrem, aby se snížila spektrální šířka. Cílem je vyhladit přechody mezi změnou frekvence, aby docházelo k co nejplynulejšímu uklidnění přechodu. Výhodou je snižování výkonu vedlejšího pásma, tím snižuje rušení sousedních kanálů. D/A převodník a dolní propust, jejichž účelem je převod signálu na analogový a následné omezení spektra signálu vysílaného D/A převodníkem. Signál pokračuje do směšovače, respektive dvou paralelních směšovačů, a dva jsou používané z důvodu omezení rušení zrcadlovými kmitočty mezi 30-40dB. Signály směšovačů jsou spojeny pomocí sčítání, odčítání a jsou řízeny pomocí signálů v kvadratuře (45°), jež produkuje kmitočtový syntezátor se smyčkou fázového závěsu. Syntezátor je napěťově řízen, referenční kmitočet zajišťuje oscilátor. Jelikož je syntezátor velmi rychle přeladitelný může Bluetooth využívat vysílání malých paketů a následně se přeladit na

jinou frekvenci k pokračování přenosu. Signál má na výstupu směšovače frekvenci pohybující se v mezích 2402-2480 MHz, což odpovídá 79 použitelným rádiovým kanálům. Následně je pomocí symetrického zesilovače zesílen. Zesilovač je výkonový a symetrický a dokáže potlačit rušivá napětí, především však zesiluje na určitý výkon podle dané třídy a dosahu. [16]

Tyto třídy se vztahují k anténnímu konektoru zařízení. Výkon je možné zvyšovat, snižovat po krocích. Jejich minimální velikost kroku je 2dB a maximální 8dB. Výkon je nastavován pomocí informace zakódované v paketu.[16]

Tab. 3.1 Třídy systému Bluetooth[16][20]

Třídy:	**Maximální výstupní výkon**		**Rozsah (m)**
	mW	**dBm**	
1	100	20	100
2	2,5	4	10
3	1	0	1
4	0,5	-3	0,5

Symetrizátor, neboli symetrický člen, je použit z důvodu konektoru antény. Z důvodu možnosti použití jedné antény pro příjem i vysílání „multiplex“ je zbytek blokového schéma stejný i pro přijímač. K rozdělení vysílaného signálu od přijímaného se provádí přepínačem, který je řízen číslováním, time slotů. Nakonec je signál již jen pomocí pásmové propusti frekvenčně omezen, většinou se používá dialektický filtr. Bluetooth vysílá, přijímá na frekvenci 2,4GHz.[16][18]

3.3 Zabezpečení

K zabezpečení technologie Bluetooth se používá několik mechanismů. Bluetooth zajišťuje bezpečnost, a odvození klíčů pomocí vlastních algoritmů ty jsou založené na šifře SAFER +. Mezi tyto klíče patří i takzvaný PIN bluetooth, který se musí zadávat do obou zařízení, které chtějí komunikovat. Poté jsou zařízení spárována. Tento postup se dá obejít, pokud je u zařízení nastaven pevný PIN kód. Spárování se však objevilo až od specifikace Bluetooth v2.1. Dále jsou na spojové vrstvě další bezpečnostní kódy Veřejná adresa (48bitů, jedinečná pro každé zařízení), dva tajné klíče (128bitů) a náhodné číslo (128bitů, různé pro každou operaci). K bezpečnosti přispívají i velmi rychlé frekvenční skoky a také malý dosah signálu, který velmi ztěžuje případný odposlech. [17][19][20]

Bluetooth, i přes veškeré zabezpečení, není zrovna nejbezpečnější. Velký problém nastal, když se objevil tzv. Bluejacking. Ten byl poprvé proveden roku 2001. Původně šlo o neškodný software, kterým bylo možno odesílat textové zprávy, později obrázky či zvuk, aniž by o tom napadený věděl. Čehož se hackeři snaží využít, kteří se snaží díky tomu převzít kontrolu nad zařízením. Dalším škodlivým softwarem pro Bluetooth je Bluesnarfing, což je neoprávněný přístup k zařízení přes bluetooth. [19][20]

3.4 Specifikace

Specifikace jsou normalizovány společností BSIG, veškeré verze Bluetooth jsou kompatibilní s nižšími verzemi. Celá kapitola citována [16] [17] [18].

3.4.1 Bluetooth v1.0

Tato verze měla mnoho problémů, ať již bezpečnostních tak i ve schopnosti různé systémy společně spolupracovat a poskytovat si služby. Tato verze obsahovala také povinné hardwarové adresy Bluetooth zařízení v procesu připojení, jelikož nebyla možnost anonymity v protokolu, to bylo největší překážkou pro širší rozšíření Bluetooth.

3.4.2 Bluetooth v1.1

Zavedeno jako norma IEEE Standard 802.15.1 roku 2002, opraveno několik chyb z předchozí verze a stanoveny nové specifikace. Dále byla přidaná podpora pro nešifrované kanály a indikátor signálu (RSSI), ten se udává v decibelech a udává sílu přijímaného signálu.

3.4.3 Bluetooth v1.2

Schváleno roku 2005, k hlavním vylepšením patří zlepšení rychlosti, a to ať již u vyhledávání, tak vyšší přenosová rychlost až 721kbit/s. Dále bylo zavedeno posílání menších paketů a následné přeskakování mezi kanály, tím se nejen, že zlepšila bezpečnost, ale také se zabraňuje použití přeplněných frekvencí. Byla také přidána standardizace rozhraní mezi hostitelem a příjemcem (HCI).

3.4.4 Bluetooth 2.0 + EDR a 2.1 + EDR

Došlo k dalšímu navýšení rychlost pomocí EDR až 3Mbit/s. EDR používá již kombinaci dvou modulací GFSK a PSK a to se dvěma variantami π / 4- DQPSK a 8 DPSK. EDR také poskytuje nižší spotřebu energie díky snížení provozního cyklu.

Funkce EDR byla volitelná, a tak se tato verze objevuje i bez EDR.

Verze Bluetooth 2.1 + EDR byla přijata roku 2007. Hlavním vylepšením je párování, které je velmi jednoduché a provádí se pomocí PIN kódu. Dále díky rozšířené možnost dotazovací procedury poskytuje více informací, a tím možnost lépe filtrovat zařízení. Tím vším se zlepšuje zabezpečení a zvyšuje používání Bluetooth.

3.4.5 Bluetooth 3.0 + HS

Specifikace vyšla roku 2009. Hlavní předností této verze bylo další zvýšení rychlosti již na 24Mbit/s. To se však již neprovádí přes spojení Bluetooth, ale přes 802.11 používající technologii WiFi, což zajišťoval protokol Alternativní MAC/PHY. To znamená, že v době nečinnosti se používají osvědčené modely s nízkou spotřebou energie a ve chvíli odesílání velkého množství dat se zapne alternativa MAC PHY 802.11 a ta přenáší data. Bluetooth bez přípony + HS se téměř nevyužívalo.

3.4.6 Bluetooth verze 4

Podrobnější informace jsou uvedeny v kapitole 9.1, která obsahuje implementaci komunikace zařízení v této technologii

Bluetooth 4.1 je vylepšením pouze softwarovým, aktualizace obsahuje Bluetooth Core Specification, čímž umožňuje vykonávání více funkcí najednou, aktualizaci zvukové architektury pro širokopásmovou řeč, přenos na 802.11n PAL, a rozšíření topologie sítě.

Bluetooth 4.2 je představeno 2014 a přináší velkou renovaci a možnost rozšíření pro Bluetooth, a to díky protokolu IPSP verze 6, čímž je Bluetooth připraveno pro přechod na chytré domácnosti. Použití nachází například u chytrých žárovek. Dále rozšiřuje délku datového paketu a zlepšuje ochranu soukromí.

3.4.7 Bluetooth 5

Z důvodu marketingu se již nepoužívá označení 5.0, ale dochází ke zkrácení. Tato verze vychází 2016 a je zaměřená hlavně na IoT, což má za úkol možnost komunikace jakéhokoliv spotřebiče s čímkoliv, tím je potřeba mnoha uzlu připojení. Proto Bluetooth 5 přichází se zvětšením výkonu z důvodu výběru použití, bud je zde možno zdvojnásobit rychlost za cenu dosahu či naopak zněkolikanásobit rozsah, ale tím snížit rychlost. Dále dochází k dalšímu zvětšení paketu. Jsou přidány funkce pro bezdrátové služby, například pro navigaci. Přesto že se zvýšil výhon, je stále vyžadován LE režim.

3.5 Výhody, nevýhody

Výhody:

- Kompatibilita rozhraní různých druhů zařízení (hlavní myšlenka Bluetooth).
- Díky použití rádiové komunikace není potřeba přímá viditelnost mezi zařízeními.
- Vzájemná komunikace různých typů zařízení (PC, mobil, PDA, notebook, handsfree, tiskárna, modem,…).
- Snadné navazování spojení.
- Relativně velký dosah i přes malé vysílací výkony (šetrnost k baterii zařízení).
- Odolnost vůči rušení (systém s rozprostřeným spektrem).
- Malé rozměry rádiového čipu a tím také celého Bluetooth modulu.
- Technologii lze implementovat do libovolného zařízení (snaha o chytré lavičky, domy, byty,…).
- Špatně odposlouchatelné

Nevýhody:

- Stále velmi malá přenosová rychlost mezi zařízeními.
- Cena.
- Potřeba kvalifikace a typového schválení každého zařízení Bluetooth

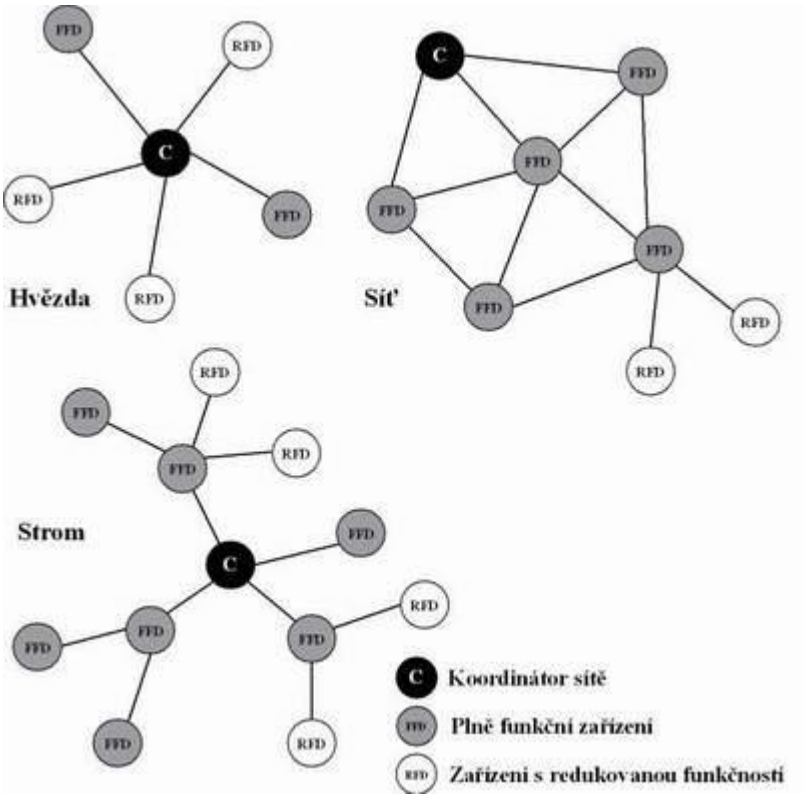
[8]

4 ZigBee

Protokol ZigBee byl vytvořen jako WPAN technologie stejně jako Bluetooth, ale na rozdíl od něj je ZigBee vytvořeno pro bezdrátové připojení elektronických zařízení s velmi nízkou spotřebou neboli pro možnost napájení AA bateriemi, a zároveň však pro široký rozsah aplikací. Jedná se o celosvětově otevřenou technologii. Její standart je IEEE 802.15.4, platný pro tuto technologii od roku 2004, kdy jej vydala skupina ZigBee Aliance. ZigBee má za úkol vytvořit bezdrátové pokrytí pomocí malého a snadno naprogramovatelného zařízení. Dosah se pohybuje v řádu stovek metrů. ZigBee je však především kvůli velmi nízké rychlosti přenosu 250kb/s technologii jež se nesnaží vytlačit, konkurovat technologii Bluetooth, IrDA, ale snaží se velmi nízkou energetickou závislost. Zároveň se jedná o velmi nenáročný protokol, co se týká hardwarových požadavků, což přináší velmi pozitivní vliv na cenu tohoto zařízení. Uplatnění tedy získá především u senzorové sítě a u automatizace.[15] [21] [22] [23]

4.1.1 Topologie logická

U logické technologie ZigBee si můžeme vybrat ze tří možností zapojení, topologie sítě: strom (tree), síť (mesh) a hvězda (star). Jedná se o rozložení uzlů a jejich následného připojení k síti, také se dá připojit pomocí peer-to-peer. Zde se jedná o jednoduchou komunikaci pouze dvou zařízení. V každé ze sítí se nachází ZigBee koordinátor, ten zajišťuje veškeré služby a kompletní protokolový rámec. Koordinátor tedy síť spravuje pro větší dosah sítě, tedy i koordinátora přispívá směšovač (router), ten připojuje k jednomu uzlu více koncových zařízení a rozesílá jim potřebná data. Ten se používá především v topologii strom, a mesh. [21] [22] [23]



Obr. 5.1 Možnosti topologie sítí ZigBee [21]

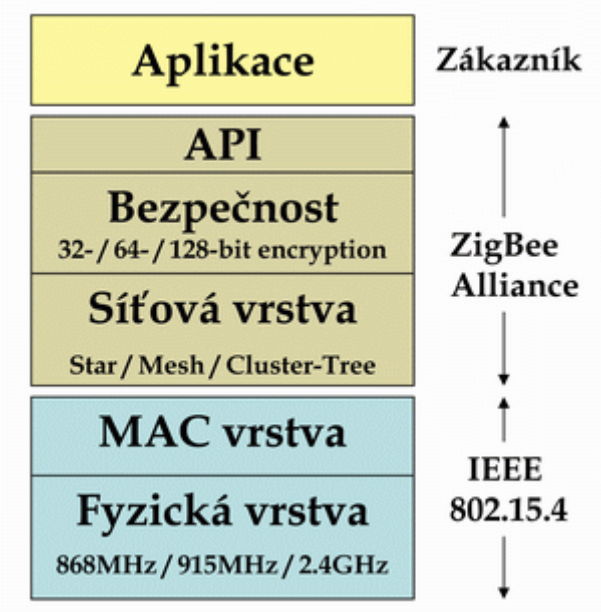
Při užití topologie hvězda komunikuje každé koncové zařízení s jiným přes koordinátora, což síť zpomaluje a zároveň je přímo závislá na koordinátoru. Jakmile vypadne cesta mezi zařízením a koordinátorem je toto zařízení odstřihnuto, stejně tak u topologie Strom, což je vlastně jen rozšíření hvězdy. Naproti tomu topologie Síť má výhodu, že při výpadku některého koncového zařízení je stále možnost komunikovat s tímto zařízením přes jiné. Zároveň je tato topologie nejsložitější. [21] [22] [23]

4.1.2 Softwarová architektura přenosu

ZigBee stejně jako každý komunikační standard lze popsat pomocí ISO/OSI modelu. Tato struktura zahrnuje tři základní úrovně (od nejnižší):

- Fyzická s linkovou vrstvou,
- Síťová vrstva,
- Aplikační vrstva.

[21] [23]



Obr. 5.3 Struktura ZigBee OSI modelu [21]

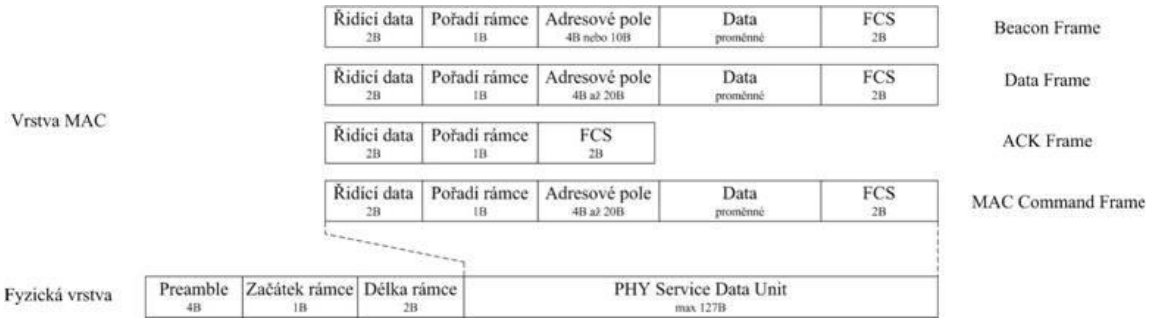
Fyzická a linková vrstva je definována standardem přenosu IEEE 802.15.4. Fyzická část má za úkol zajišťovat rádiový přenos dat fyzicky. K tomu používá jedno ze tří frekvenčních pásem: [23]

- 868 [MHz] – lepší přenos není zde tolik odražených vln, méně uživatelů (Evropa).
- 915 [MHz] - lepší přenos není zde tolik odražených vln, méně uživatelů (Amerika).
- 2400 [MHz] – nejrozšířenější na trhu, nižší spotřeba, vyšší rychlost přenosu, více kanálů (celosvětově). [23]

ZigBee je schopno samo vybrat nejlepší kanál pro přenos a následně pokud dochází k jeho rušení z různého důvodu, je schopno tento kanál změnit. Signál se moduluje pomocí ofsetové kvadraturní fázové komunikace (O-QPSK). Tato modulace se liší od QPSK pouze tím, že nedochází ke změnám z 10 na 01 a z 11 na 00, což v diagramu vyvolá změnu fáze o 180° a tím se omezují chyby vyvolané nežádoucí postranní frekvencí spektra. K samotnému přenosu vzduchem se využívá DSSS protokol, který

nepřenáší jednotlivé bity, ale nahrazuje je nějakou sekvencí a tím dochází k omezení rušení a chyb při přenosu. [15] [22] [23]

Linková vrstva odpovídá za adresování a samotnou komunikaci. Jejím hlavním cílem je připravit pakety ze síťové vrstvy pro přenos médiem k tomu využívá přidání záhlaví a zápatí k paketu, což se následně zapouzdří do rámce. K paketu jsou přidány informace jako posloupnost pro začátek a konec vysílání (CRC), typ datové jednotky protokolu, kvalita a řízení přenosu. [15] [22] [23]



Obr. 5.3 Datový rámec ZigBee [22]

Sítová vrstva zajišťuje pomocí detekce síly signálu vhodný výběr kanálu pro přenos (získá informace od fyzické vrstvy ohledně kvality a síly signálu), Dále také obsahuje knihovny, které vytvářejí rozhraní mezi aplikacemi a standardem IEEE 802.15.4, řeší také zabezpečení a směrování paketů. A vyhledává ostatní zařízení s technologii ZigBee.[15] [21] [22] [23]

Aplikační vrstva, se skládá ze dvou podvrstev ZigBee objektů, tato podvrstva určuje typ zařízení v síti, a spravuje poskytované služby. A z podvrstvy uživatelských aplikačních objektů, ta udržuje tabulky připojení, pro snazší navázání komunikace, a pro snazší výběr zařízení.[15][22][23]

4.1.3 Adresování

U technologie ZigBee má každý uzel svou vlastní a pro sít unikátní identifikaci, to se řeší stejně jako u WiFi pomocí dvou adres:

- Fyzická (MAC) adresa, jde o 64 bitovou adresu. Tuto adresu přiděluje každému zařízení IEEE již při výrobě, a tak žádná dvě existující zařízení nesmí mít stejnou Fyzickou adresu.
- Sítová adresa, zde se jedná o 16bitovou hodnotu. Používá se pouze pro adresování v místní síti, tudíž není nutnost unikátnosti na světě, stačí v síti. Síťové adresy jsou přidělovány uzlům pomocí koordinátora (podobně jako DHCP protokol)

Dále je každá sít určena PAN ID identifikátorem, jde o 16bitovou hodnotu určující danou síť. Díky tomuto PAN ID je možno mít připojeno jedno zařízení k více sítím. PAN ID je přidělováno koordinátorovy.[22] [23]

4.2 Zabezpečení

Sítě ZigBee se dají zabezpečit velmi dobře a jsou díky tomu velmi bezpečné. Velmi silné zabezpečení je použito nejen kvůli kolizím s jinými sousedními sítěmi ZigBee, ale také z důvodu nepřátelským útokům, díky nimž jsou schopni zloději nastavit neustálé otevírání vrat garáže, otevíratelných technologii ZigBee. K zabezpečení se používají následující metody: [21] [22]

- Access Control Lists (ACL) – jde o sekvenční seznam pravidel permit (povolit) a deny (zakázat). V tomto seznamu je předem dáno s jakými uzly je možno komunikovat a s jakými nikoliv. V seznamu jsou zároveň uloženy informace o adrese každého uzlu v síti. Při začátku komunikace je tady nejprve uzel, který si požádá o komunikaci, porovnán se seznamem a výsledek je předán vyšší vrstvě, která rozhodne, zda povolit či odmítnout komunikaci.
- Message Timeout – Tato funkce umožní odmítnutí starých zpráv či zpráv, jež jsou odesílány opakovaně, například opakované útoky na zabezpečení. Pracuje na porovnávání kontrolního součtu, pokud je kontrolní součet stejný jako součet poslední, přijaté zprávy tuto zprávu zahodí.
- AES-based Encryption – Jde o možnost zašifrování dat pomocí 128bitového klíče. Takto zašifrovaná data se odešlou a jen příjemce, jež zná šifrovací sekvenci a klíč, je schopen rozšifrovat obsah dat. Toto je velmi výhodné proti odposlouchávání dat.

[21] [22] [23]

4.3 Specifikace

Specifikací je velké množství jedná se vždy o rozdělení podle daného použití, a tak tady máme například:

- Inteligentní energie 1.2 – jež je určena pro například chytré žárovky
- Domácí automatizace 1.2
- Telekomunikační služby 1.0
- Zdravotní péče 1.0
- RF4CE – Dálkové ovládání 1.0
- ZigBee Smart Energy 2.0 – pro monitorování, řízení, automatizaci dodávek vody,

energie.

[23]

4.4 Výhody, nevýhody

ZigBee našlo uplatnění ve spoustě odvětví, ať už se jedná o průmysl (pohybové senzory, kontrolní linky), zdravotnictví (monitorování pacientů, ultrazvukové sondy), automatizace budov (klimatizace, vytápění, osvětlení) tak se dá použít jako uložiště dat pro různé záznamy, nebo například jako dálkové ovládání pro hračky. ZigBee se zaměřuje především na monitorování a řízení.[22]

Výhody:

- Velmi nízká cena.
- Vysoká spolehlivost.
- Jednoduchá instalace, implementace.
- Malý výkon při multitaskingu.
- Otevřený standard.
- Vysoké zabezpečení.
- Velmi nízká spotřeba.
- Podpora pro pásma pod 1GHz.

Nevýhody:

- Velmi malá šířka přenosového pásma 250kb/s.
- Menší množství spotřebních produktů.

5 Z-Wave

5.1 Úvod

Z-Wave je velmi energeticky nenáročný protokol, používaný pro bezdrátovou komunikaci na krátké vzdálenosti. Určen především pro automatizaci domácností pomocí IoT. Protokol byl vyvinut firmou Zensys, v Dánsku roku 2001. Protokol byl představen jako spotřebitelský systém pro automatizaci domácností, provozovaný na bezlicenčním kmitočtovém pásmu 900 MHz, řízen pomocí čipu SoC. Tento čip nabízí velkou výhodu v nízké spotřebně elektrické energie.Od roku 2008 vlastní technologii firma Sigma Desings. Roku 2005 se technologie Z-Wave začala rozšiřovat a vznikla skupina snažící se podporovat a využívat tuto bezdrátovou technologii, s názvem Z-Wave Alliance, postupem času se do této skupiny začali přidávat i velké společnosti jako jsou například Panasonic,

Intel, či Cisco Systems. V letošním roce však byla technologie Z-Wave prodána, firma Silicon Labs koupila technologii od firmy Sigma Desings. [33] [34]

5.2 Technické parametry

Z-Wave využívá pro přenos modulaci FSK, kdy je signál modulován, přenášen a následně demodulován pomocí frekvenčního posuvu, tím se značí změna logické hodnoty, používá se kódování Manchester. Komunikace se provádí jen na krátké vzdálenosti, maximální dosah se uvádí 100 metrů venku, vnitřní dosah je uváděn kolem 50 metrů, technologie je schopna přenášet pouze malý objem dat, proto je vhodná především pro ovládání domácích spotřebičů, garážových vrat, dokáže však provádět i řízení vzduchotechniky, osvětlení, přístupu nebo se často používá pro detekci požárů, v požárových hlásičích. [32] [33] [34] [36]

Jako většina bezdrátových technologií používaných v průmyslové, zdravotnické či vědecké oblasti používá pásmo ISM, na kmitočtu 868 MHz a 915 MHz, s rychlostí až 200 kbit/s. V jiných částech světa jsou používány jiné frekvence pro tuto technologii. Napájení je řešeno zdrojem, který má 2,2-3,6 V a ve vysílacím režimu spotřebuje proud o velikosti 23 mA. [32] [33] [34] [36]

Protokol používá jako logickou topologii typu síť (mesh), kde se nachází řídící, ale i podřídící zařízení. Každé zařízení má pro správné směrování v sobě uloženou tabulku o topologii dané sítě. Samotné směrování se provádí pomocí směrování zdroje, kdy je v samotném přenášeném paketu umístěna informace o cestě k příjemci, to se provádí pomocí protokolu LSRR nebo SSRR. Toto směrování umožňuje jednodušší odstranění poruchy, která se projeví pomocí neodeslaní potvrzovací zprávy, tím se zaručuje spolehlivý přenos informace. O samotný přenos se stara fyzická a adresová vrstva, ta je definována v normě G. 9959. Jelikož se dá směrování provádět i přes třetí nezainteresovaný uzel dosahuje protokol dostatečné vzdálenosti pro pokrytí domácnosti, navíc je schopen pojmout až 232 zařízení na síť. [32] [33] [34]

Z-wave je samozřejmě také interoperabilní, díky čemuž je možno spolupracovat s výrobky od různých výrobců s velmi dobrou vzájemnou součinností, tedy téměř bez omezení. Pomocí jedné jednotky lze spojit různorodé produkty a komunikovat s nimi nebo je spravovat. Navíc se systém stal, díky licenci open source, otevřený softwarovým vývojářům. [32] [33] [34]

Obr. 6.1 Ukázka různých druhů zařízení, které lze spojit pomocí Z-Wave.[34]

5.3 Zabezpečení:

Protokol Z-Wave je založen na čipu, pro který má licenci pouze firma Sigma Desings a Mitsumi. Pro šifrování je použitý standard šifrování AES, který data rozdělí do bloků o velikosti 128 bitů, a přidá klíč o velikosti, která může být různá, nejčastěji se používá 128 či 256 bitů, AES pracuje pomocí matice 4x4 díky tomu je možnost prohazovat řádky, pro lepší zakódování. [33]

Navíc Z-Wave používá postup párování zařízení, kdy je každému zařízení přidán jedinečný PIN kód nebo QR. Pro zařízení, jež jsou vybaveny lepším zabezpečením, vydala Z-Wave Alliance certifikát Security 2. Jedná se již o velmi pokročilé zabezpečení. Nejsnadnější pro napadení se tak stává řídící jednotka připojená, například k síti WiFi, tu zabezpečuje však samotný provozovatel. [33]

5.4 Standardy

Jak již bylo napsáno hlavním úkolem je vytvořit velice kompatibilní a bezpečný protokol pro připojení, co největšího množství různých zařízení, a k tomu slouží Z-Wave. Z-Wave Alliance, však přišla s rozšířením a roku 2013 vychází nový protokol Z-Wave Plus, ten sebou přináší ještě větší kompatibilitu mezi zařízeními, přináší i některé nové funkce, a zlepšenou bezpečnost, tento protokol přichází především pro čipy nové řady 500 SoC. [33]

5.5 Výhody, nevýhody

Výhody:

- Možnost připojení velkého počtu zařízení, uzlů k jedné síti.
- Velmi dobrá kompatibilita pro připojení různorodých zařízení.
- Pracuje na jiné frekvenci než WiFi, Bluetooth.
- Zabezpečení.
- Snadná instalace, vyžaduje pouze řídící jednotku a čidla.
- Minimální spotřeba energie.
- Možnost připojit k internetu pro ovládání na dálku.
- Frekvence na, které vysílá má mnohem menší dopad na náš organismus než frekvence WiFi
- Otevřený systém, tudíž vysoce dostupný pro vývojáře.
- Fyzická a adresová vrstva je globálně standardizovaná.

Nevýhody:

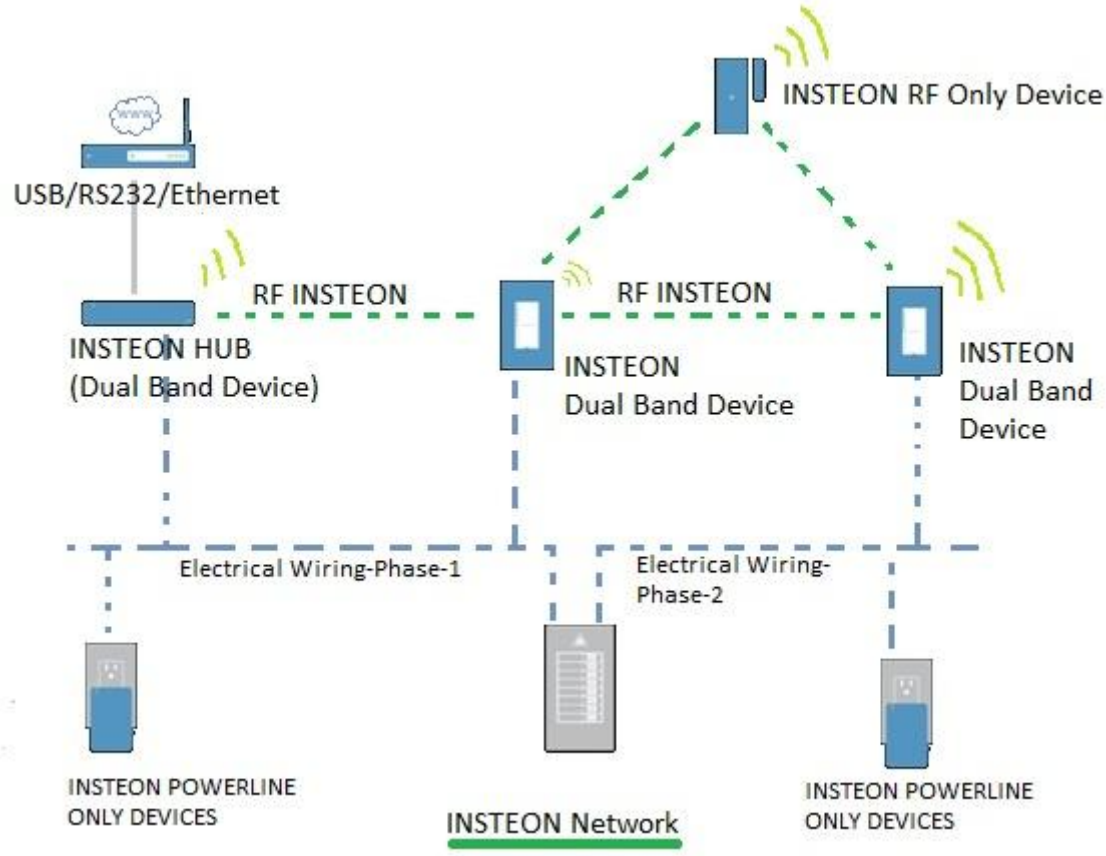
- Velmi malá rychlost přenosu.
- Nedostatečný manuál.
- Dlouhá odezva při nastavování jednotky pomocí webového rozhraní.

[35]

6 Některé další rádiové technologie

6.1 Insteon

Protokol Insteon, byl uveden na trh roku 2005, pod stejnojmennou značkou Insteon, jako technologie pro plně automatickou domácnost (IoT), která umožňuje ovládat termostaty, mikrovlnné trouby, různé senzory, dálkové ovladače a různé další elektrické přístroje. Insteon využívá topologii typu dvojí sítě (duble-mesh), označovanou jako dvoublokovou, dokáže tedy využívat jak přenosy pomocí kabeláže, tak bezdrátové přenosy dat. To se stává jeho hlavní výhodou, navíc je zpětně kompatibilní s technologii X10 elektrické vedení zpráv, dříve hojně využívanou. Navíc je zpětně kompatibilní s každou svojí starší verzí. Do sítě je teoreticky možno přidat neomezený počet zařízení. [1] [2] [24] [25]



Obr. 7.1 Síť Insteon. [24]

Každá vyslaná zpráva technologii Insteon prochází detekcí a opravou, navíc každý přístroj v síti se chová jako hub (opakovač) a rozesílá informaci na každé zařízení, dokud mu nepřijde potvrzovací zpráva, využívá tedy simulcastu neboli současného vysílání všech zařízení najednou, pro určení příjemce jsou v paketu použity 3 bajty. Modulace u bezdrátové technologie je pomocí klíčování fázovým posuvem (FSK). Při připojení k zařízení pomocí elektroinstalace budovy i bezdrátově využívá komunikaci, která není rušena. Zařízení jsou navíc schopna fungovat i bez centrálního ovladače, ale i s ním, jakožto s regulátorem. Řízení se dá provádět pomocí vzdáleného přístupu, například přes mobilní telefon, tak pomocí centrálního řadiče, připojením k modemu.[24][25]

K síti se dané zařízení připojuje automaticky, instalace je tedy velmi jednoduchá. K zabezpečení proti odposlouchání slouží šifrování zpráv, naopak pro zabezpečení připojení vyžaduje, aby každé zařízení Insteon mělo svůj unikátní ID kód, ten funguje jako taková MAC adresa, také ID kód zařízení přiřazuje samotný výrobce. Firmware tedy na základě ID a fyzickým stlačením tlačítka na přístroji Insteon, určuje, zda je přístroj přidán do struktury sítě či se ručně zadává pomocí centrálního řadiče prvku, kam zadáme ID nového přístroje. Přesto se zabezpečení bezdrátové části Insteon setkává s kritikou.[24]

[25]

6.1.1 Specifikace

- Rychlost přenosu: 13 kbit/s.
- Velikost zprávy: 10 bajtů standardně, rozšíření až 24 bajtů.
- Frekvence: 902 až 924 MHz.
- Modulace: FSK.
- Citlivost: -103 dBm.
- Rozsah: 50 m.
- RAM: 80 bajtů.
- ROM: 3 kB.

Požadavky:

- RAM: 256 bajtů
- EEPROM: 256 bajtů
- Flash: 7 kB

Rozdělení vysílaného paketu:

- Adresa přijímače: 3 bajty.
- Adresa zdroje: 3 bajty.
- Informace: 14 bajtů
- Potvrzovací zpráva: 1 bajt.
- Ostatní (příkaz, Flags): 3 bajty.

[26] [25]

6.1.2 Výhody, nevýhody

Výhody:

- Velikost sítě
- Možnost využít bezdrátovou síť i kabeláž.
- Rychlost odezvy.
- Plná kompatibilita se starší verzí.
- Interoperabilita různorodých výrobců, zařízení.
- Vysílací pásmo, jež tolik nezatěžuje lidský organismus.
- Vysílací pásmo, jež není tolik zatíženo.
- Jednoduchost, automatické přihlášení.

- Jen jedna třída kompatibility.
- Cenově velmi výhodné.

Nevýhody:

- Bezpečnost.
- Dosah.
- Velmi malý obsah přenášené informace.

[25] [26]

6.2 RFID

Zkratka RFID (Radio Frequency Identification), pocházející z anglického jazyka, znamená radiofrekvenční identifikaci. Pro komunikaci využívá RFID tagy, ty pracují na podobném principu jako čárový kód, RFID je také považováno za nástupce čárových kódů. Oproti nim má nespornou výhodu v tom, že pro čtení tagu není potřeba přímá viditelnost. Přesto dnes není možné vytlačit čárové kódy z důvodu ceny. Frekvence, jež RFID používá je v Evropě 125 kHz, 134 kHz, 13,56 MHz a frekvenční pásmo 865 – 869 MHz.[27] [29]

S myšlenkou na vznik bezdrátové technologie zpracování informací přišla před lety největší maloobchodní firma WalMart, která před několika desetiletími stála u zrodu čárového kódu. Základem byla myšlenka vyvinout takovou technologii, která dokáže objekt identifikovat na větší vzdálenost, bez přímé viditelnosti tak, aby v reálném čase bylo možno zpracovat více objektů současně. Patent pro tuto technologii však získal roku 1983 Charles Walton, ten však není příbuzný se zakladateli společnosti WalMart. V současné době se technologie RFID velice rozvíjí a dochází k nasazení v mnoha dalších oblastech trhu. Největší uplatnění nachází v logistice, výrobě, sledování objektů - logistických jednotek (zboží, palet, kontejnerů), sledování majetku, sledování zavazadel na letištích a evidence osob.

Systém RFID se skládá ze tří základních prvků, a těmi jsou tagy, čtecí zařízení a databáze která obsahuje identifikační číslo EPC.[27]

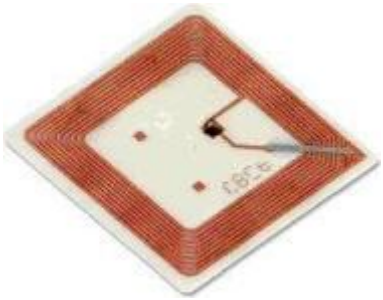
6.2.1 RFID tag

Tag se skládá z integrovaného obvodu v podobě velmi malého čipu a antény. Tagy třídíme do různých skupin, podle nichž určujeme jejich schopnosti, rozdělení je k dispozici zde [28]. Tagy rozlišujeme na aktivní, potřebuje mít připojenou baterii, a na pasivní, při

přiložení čtecího zařízení získá energii pro vysílání pomocí elektromagnetického pole. Jak již bylo zmíněno, rozlišujeme tagy na aktivní a pasivní, toto rozlišení určuje čip v tagu. [27] [28]

Aktivní RFID čip vysílá svá data do okolí, díky malé baterii umístěné v čipu, a výdrž se uvádí 1-5 let. Čipy však mají menší odolnost vůči teplotě, a tak je nutné provádět výměnu baterie častěji. Aktivní čip se používá především pro sledování osob, vozidel, zvířat. Dosah pro příjem dat je až 100 metrů, jejich paměť je 100Kb, avšak jejich cena je poněkud vyšší.[28]

Pasivní čipy jsou výrazně levnější, ale jejich dosah je maximálně 10 m, jejich dosah určuje frekvence, pokud je frekvence vyšší UHF jejich dosah může být až 10 m, při frekvenci nižší LF 125 kHz, je dosah přibližně 0,5 m [30]. Tyto čipy mají dlouhou životnost, jsou nenáročné na obsluhu a jejich paměť je 64-256 bitů. [27] [28]



Obr. 7.2 RFID tag [31]

6.2.2 EPC

RFID čipy mají v sobě uložené od výrobce unikátní číslo EPC, dnes se jedná většinou o 96 bitové číslo, dříve šlo o 64 bitové, ale již se přemýšlí o přechod na 128 bitové číslo. EPC poskytuje jedinečnou identitu pro každý RFID čip, jeho struktura je definovaná v EPCglobal Tag Data Standard, a je k dispozici na webu [28]. EPC lze rozdělit na 4 základní části: [30][28]

- Záhlaví – délka, typ a struktura kódu (8bitů).
- EPC manager – informace sloužící k identifikaci dané firmy (28bitů).
- Object class – informace sloužící k identifikaci výrobce (24 bitů).
- Sériové číslo – identifikace daného zařízení (36bitů).

6.2.3 Middleware

Software zajišťující filtrování a směrování údajů v reálném čase, notifikaci a předávání dat do následující komponenty sítě EPCglobal Network (EPCIS) nebo do jiných modulů informačního systému konkrétního obchodního partnera. [28] [31]

6.2.4 Výhody a nevýhody

Výhody:

- Není potřebná přímá viditelnost pro zpracování dat.
- Mobilita.
- Rychlost pořízení informace.
- Hromadné čtení dat.
- Možnost zjednodušení inventur.

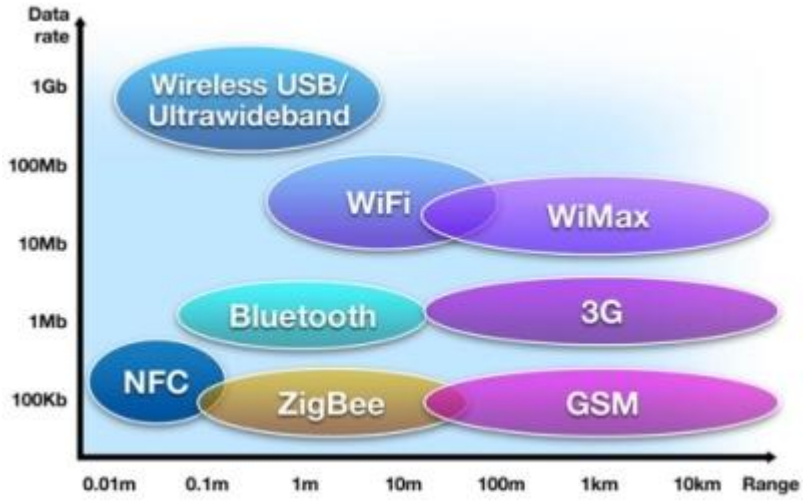
Nevýhody:

- Náklady na celkovou realizaci.
- Vyšší cena čipů.
- Možnosti zneužití z důvodu sledování.
- Paměť čipů.

[31]

6.3 NFC

NFC je technologie bezdrátové komunikace, která je pro vysokofrekvenční pásma a umožňuje výměnu dat, informací na krátké vzdálenosti (PAN). Z toho vychází anglické označení Near Field Communication. NFC vychází z předešlé technologie RFID, také využívá takzvané tagy, jako zařízení pro získání informací, typy tagů a standardy jsou k dispozici zde [41]. Avšak na rozdíl od RFID není zařízení NFC schopno přijímat či vysílat signál v řádech několika metrů, NFC má maximální hranici pro přenos je 20 cm, jako daleko účinnější se však doporučuje přenos na vzdálenost okolo 4 cm. Stejně jako u RFID jsou zde aktivní i pasivní tagy. NFC tedy má velmi malou spotřebu energie. Technologie by se dala také přirovnat k IrDa portu, avšak zde je velká výhoda, že mezi komunikujícími zařízeními může být například zeď, proto je možné tagy umístit například pod omítku. NFC pracuje na frekvenci 13,56 MHz. [39] [40]



Obr. 7.2 Postavení NFC mezi ostatními bezdrátovými technologiemi. [40]

Technologie se snaží docílit zjednodušení běžných denně provozujících činností, především prostřednictvím mobilního telefonu, který dnes je nedílnou součástí každého z nás. NFC se snaží nahradit například peněženku, papírová menu v restauracích, zrychlení, zjednodušení importu kontaktů, odemčení dveří, identifikaci zavazadel, a spousty dalších činností [39]. Jeho velký rozmach je tedy způsoben především díky mobilním telefonům, to však neznamená, že se s touto technologii nemůžeme setkat i jinde. [40]

Vznik NFC se datuje k roku 2002, kdy společnosti Philips a Sony začaly s vývojem technologie alternativní k technologii RFID. RFID se totiž ukázalo jako snadno odposlouchavatelné. Roku 2004 se k těmto společnostem přidává i Nokia a dochází k založení neziskové organizace NFC forum. Díky tomu se NFC začala velmi rychle šířit do světa, navíc se podařilo využít potenciálu mobilních telefonů. I přes to se 6 let nedařilo využít plně potenciál spojení telefon a NFC až roku 2010, kdy tomu velmi napomohl systém pro mobilní telefony Android, dříve zvládali telefony jen jednoduché aplikace NFC. [40]

6.3.1 Přenos

Technologie NFC je alternativa RFID, tuto technologii rozšiřuje neaktivními tagy a je kompatibilní. Jedná se o rádiovou komunikaci na frekvenci 13,56MHz, rychlost přenosu dat může dosahovat až 424 kbit/s. Přenos dat je prováděn pomocí dvou variant:

1. Peer-to-Peer – přenos mezi dvěma rovnocennými přístroji.
2. Zařízení se dělí na „iniciátory“ a „cíle“, iniciátor je aktivní přístroj, jež je schopen generovat rádiový signál, a tím přenášet svůj požadavek, naproti tomu cíl pouze

čeká na žádost od iniciátora a následně na ní odpovídá, jedná se o pasivní zařízení. K využití jednotlivých výhod v mobilním telefonu, je však nutné mít staženou aplikaci, která umožní použití NFC a dané výhody. [37] [39] [40] [41]

6.3.2 Zabezpečení

Krátká vzdálenost komunikace je sice pro zabezpečení výhodou, avšak rozhodně to není postačující zabezpečení. NFC jako takové neobsahuje ochranu proti odposlechům, to se stává především v případě použití technologie při placení, jako velmi nevhodné, proto musí být použity kryptovací protokoly vyšších vrstev v ISO/OSI modelu či TCP/IP modelu. K zabezpečení NFC přenosu se používají různá hesla, zámky. Ty však dodává sám uživatel, výrobci se snaží zabezpečit NFC pomocí kryptografie, a software pomocí antivirů, zachytávajících malware a spyware. K ochraně při placení se používá Secure element, jde o čip sloužící jako zabezpečená paměť pro uložení zašifrovaných dat. Navíc při ztrátě telefonu jde NFC zablokovat, stejně jako se dá zablokovat sim karta. [37]

6.3.3 Výhody, nevýhody

Výhody:

- Jednoduchost – pro navázání spojení je potřeba jen přiblížení obou přístrojů.
- Všestrannost – NFC se dá využít v nejrůznějších situacích.
- Základní vrstvy NFC jsou z dostupných a otevřených standardů.
- Kompabilita – NFC se dá využít s již dostupnými technologiemi bezdrátových karet. Propojit například s Wi-Fi či Bluetooth.
- Díky malé vzdálenosti přenosu je těžké zachytit tento přenos, k dispozici jsou navíc přídavné aplikace pro zabezpečení.
- Frekvenční pásmo není tak zatížené jako například 2,4 GHz využívané Wi-Fi a dalšími technologiemi.

Nevýhody:

- Vzdálenost přenosu.
- Rychlost přenosu.

[39] [41]

7 Porovnání

Tab: 8.1 Porovnání [24] [26] [44]

	Wi-Fi	**Bluetooth**	**Zigbee**	**Z-Wave**	**Insteon**	**RFID**	**NFC**
Aplikační záměr	Web	Náhrada za kabel	Monitorování a řízení	Monitorování a řízení	Plně automatická domácnost	Náhrada kódů	Zjednodušení každodenních úkonů
Spotřeba energie	Vysoká	Střední	Střední	Střední	Střední	Nízká	Nízká
Přenosová rychlost	200 Mb/s (1000 Mb/s 802.11ac)	721 kbit/s	250 kbit/s	100 kbit/s	13 kbit/s	Nízká	424 kbit/s
Komunikační dosah (m)	100	200	100	>100	50	100	0,2
Velikost sítě (teoreticky)	256	200	1000	232	Neomezený	2	2
Maximální velikost zprávy	2 KB	27 bajtů	100 bajtů	64 bajtů	24 bajtů	neurčitá	neurčitá
Náklady	$$$	$	$$	$	$	$	$
Přihlášení do sítě	Procesní	Procesní	Procesní	Procesní	Automatické	Automatické	Automatické

8 Praktická část

8.1 Bluetooth Low Energy

Bluetooth Low Energy (dále již jen BLE), je často k dispozici pod obchodním názvem Bluetooth Smart, vydán pod specifikací Core Specification verze 4.0, přesto že dnes je pod záštitou Bluetooth SIG, dříve jako technologie Wibree byla vydána roku 2006 organizací Nokia. Avšak po následujících jednání bylo dohodnuto, že dojde k přejmenování a spojení s technologii Bluetooth, k tomu dochází v roce 2010. Následně vychází i další verze specifikace BLE a to sice 4.1 a 4.2. Dnes nejnovější verze je 5.0 vydaná 2016.[48] [49] [50] [51]

BLE vznikla především pro zařízení, kde je potřebná úspora energie, neměla za úkol nahrazení předešlé specifikace. Používá se především u mobilních telefonů, handsfree, bezdrátové myši a další zařízení.

BLE vznikl z důvodu velkého nároku na spotřebu energie čehož dosahuje především díky zkrácení doby aktivního vysílání, příjímání. Jako i ostatní komunikační jednotky využívá logického rozdělení na vrstvy pomocí upravené verze ISO/OSI modelu, ten se zde nazývá stack.[49]

8.1.1 Fyzická vrstva

Komunikace mezi dvěma zařízeními probíhá rámci fyzické vrstvy na frekvenčním pásmu 2,4 GHz, pro tento přenos se používá celkem jednoduchá frekvenční modulace GFSK, klíčování využívá předěl mezi frekvencí 185 kHz, vyšší frekvence označují logickou 1 a nižší jsou pro logickou 0. Tato vrstva také určuje přenosovou rychlost 1Mb/s.[52]

8.1.2 Linková vrstva

Linková vrstva se stará o vysílání v samotném reálném čase, tím vznikají vysoké nároky především na tuto vrstvu. Ta rozděluje všech 40 kanálů do dvou skupin, v jedné skupině se nachází pouhé tři kanály, ty se používají především k určení a k zachycení samotného zařízení. Jsou zde použity advertising pakety, o nich je více v kapitole 9.1.3.1.1. Druhá skupina o 37 kanálech je použita již během samotného spojení pro přenos paketů, z důvodu bezpečnosti se kanály, na kterých jsou data přenášena, mění. Samotná data jsou již od vyšších vrstev zapouzdřena v paketu, linková vrstva je však přidáním záhlaví

(obsahuje řídící informace) a zápatí (obsahuje především kontrolní součet) znovu zapouzdří do rámce, který je následně vysílán, a tak se pro samotný přenos dají vysílat data o objemu maximálně 255 bajtů v rámci jednoho rámce. Tyto data jsou však doprovázena alespoň 10 bajty v kterých jsou zaneseny přístupové adresy, kontrolní součet, preambule a hlavička.[52]

Jelikož poměr mezi samotnou aktivitou Bluetooth a nečinností po bodu komunikace, jasně vyznívá pro nečinnost, došlo k řízení komunikace pomocí periodických opakujících se intervalech o dané délce, došlo k výraznému snížení spotřeby energie, jelikož po vzájemné komunikaci, která proběhne v intervalu kdy je Bluetooth plně aktivní, dochází k vypnutí.[52]

8.1.3 Protokoly

BLE využívá ke své komunikaci různé funkce, protokoly:

- HCI – standardizované rozhraní pro propojení mezi nízkými vrstvami (linková,fyzická) a vyššími, ty jsou schopny odesílat příkazy do nižších vrstev a z nich naopak přijímat. Jde především o protokol UART.
- L2CAP – Tento protokol se stará o rozdělené či naopak sloučení paketů z vyšších vrstev, tak aby bylo možné je zapouzdřit do rámce.
- Security Manager – má za úkol spárovat zařízení a výměnu klíčů pro spárování, kterými je následný obsah komunikace kódován.
- ATT – protokol starající se o atributy, vytváří rozhraní pro zařízení s vyšší úrovní (klient – server), každý atribut má UUID, vlastní data a práva, ty určují kdo a jak může k atributům přistupovat, ATT protokol tak umožňuje tyto atributy procházet. Je zde několik typů zpráv které se vážou k atributům:
    - Požadavek – například na čtení či potvrzený zápis
    - Odpověď
    - Příkaz – na zápis
    - Notifikace – serverem odeslaná data pro klienta (nepotřebují potvrzení)
    - Identifikace – serverem odeslaná data pro klienta (potřebují potvrzení)
    - Potvrzení

[17] [52]

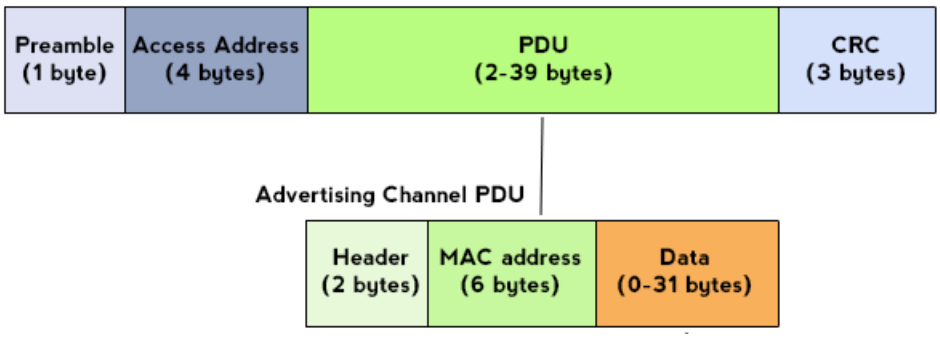
8.1.3.1 GAP

GAP je velmi důležitým profilem pro přenos informací pomocí BLE zařízením, umožňuje spolupráci mezi zařízeními, a to i od různých výrobců, také specifikuje, jak se zařízení bude chovat při skenování, navazování bezpečného přenosu, odesílání dat a také určuje, zda je komunikace vůbec možná. GAP má role zařízeních, a také dva základní koncepty:

- Periferní – jedná se o malá zařízení s nízkým výkonem, připojují se k centrálnímu zařízení. (senzory, monitory srdečních funkcí) [53]
- Centrální – vyšší výkon a paměť. (tablety, notebooky, mobilní telefon) [53]

8.1.3.1.1 Advertising paket

Tyto pakety se vysílají mimo spojení neboli když zařízení s nikým nekomunikuje. K vysílání dochází vždy minimálně na jednom ze tří kanálů vymezených pro tyto pakty. V případě, že dorazí odpověď na toto vysílání od zjistitelného zařízení, které chce komunikovat. Advertising paket je odesílán v určitých periodických intervalech 20 ms až 10,24 s, čím je interval kratší, tím se zvyšuje možnost zachycení zprávy centrálním zařízením, navíc zde není vzájemná sinchronuzace mezi Advertising paketem a skenerem, který se snaží pakety zachytávat. Skener naslouchá danému kanálu jen po určitou dobu, proto latence závisí na intervalu odesílání Advertising paketu, intervalu skenování a také na intervalu skenování určitého kanálu. Samotné skenování má dva typy, a to sice pasivní, skener přijme ale advertiser se nedozví o přijetí, a aktivní kdy advertiser dostává odpověď. Advertising paket BLE se skládá z preambule, adresy přístupu, záhlaví, adresy zařízení, samotných dat a kontrolního kódu, viz Obr.9.1.[17] [51] [52] [53]



Obr. 9.1 Advertising paket [51]

Pomocí Advertising paketu lze také docílit broacastu, tím že některé zařízení odesílá tyto pakety a k příjmu dochází u více zařízení. Zařízení tak může komunikovat s více zařízeními. Pokud však narazí na přijímač typu observer, který vyhledává a přijímá Advertising pakety, dojde k zastavení broucastu a k výhradnímu spojení mezi těmito

dvěma zařízeními. [53]

8.1.3.2 GATT

GATT se zaměřuje na výměnu dat mezi zařízeními, k čemu využívá ATT protokol, který popisuje strukturu uložených služeb a charakteristik. Veškeré informace, které získá zapisuje do vyhledávací tabulky. I GATT má pro zařízení určité role, ty jsou však nezávislé s rolemi GAP: [53]

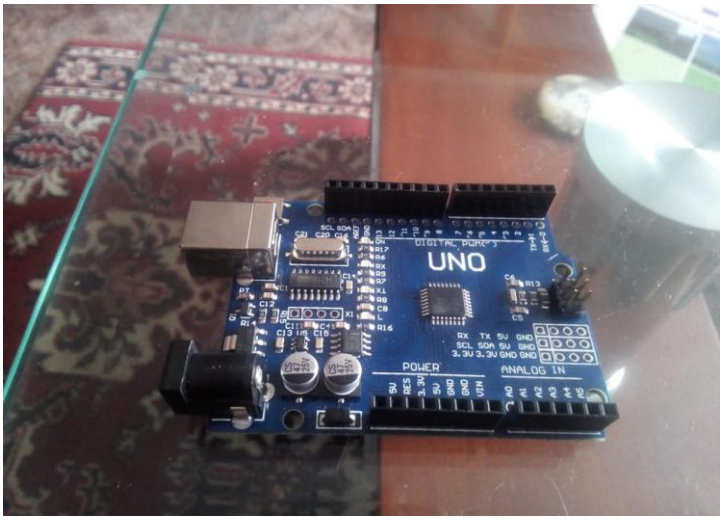
- Klient - po vyhledání služeb poskytovaných serverem, se spojení nastaví jako jedinečné, zařízení může číst přijímat a zapisovat do serveru. [53]
- Server – zařízení obsahující ATT protokol, zpřístupní služby klientovy, a posílá mu informace o aktualizacích, každé BLE zařízení obsahuje alespoň základní server.[53]

8.2 Arduino

Arduino je otevřená elektronická platforma založená na jednoduché počítačové desce a vývojovém prostředí, které slouží pro tvorbu softwaru. První vydání se datuje k roku 2005, plánem bylo vytvořit prototypovou platformu, na které by se studenti a lidé začínající s programováním hardware mohli jednoduše učit a zároveň byl zajištěn jejich rychlý rozvoj. Jednodeskový počítač je založen na mikrokontrolerech ATmega od společnosti Atmel.[47]

Arduino je schopné připojovat různé rozšiřující periferie, ať již vstupní či výstupní, jako jsou různé motory, LED diody, čidla, senzory či displey. Kit Arduino je možné si sestavit, podle vlastní potřeby. Základní ardueino tvoří mikrokontrolér, krystal, napájecí zdroj a převodním pro komunikaci s počítačem, nebo koupit již sestavený. Kit na sobě ukrývá jak digitální, tak analogové vstupně-výstupní piny, některé digitální piny podporují PWM. Programovací jazyk Arduino je založený na jazyce Wiring a IDE je založené na prostředí Processing. Software Arduino je open source nástroj, který umožňuje rozšíření přes knihovny například pomocí knihoven C++. Pro pokročilé je zde možnost přepnout na programovací jazyk AVR C.[46]

Pro rozšíření se používájí takzvané Arduino Shieldy, ke kterým vychází knihovny k použití Shieldu. Návrhy vychází pod licencí Creative Commons, lze však připojit i vlastní elektronické obvody. K tomu použít například kontaktní pole. Navíc software je možné použít Arduino na operačních systémech Windows, Macintosh, OSX a Linux, to je výhoda oproti ostatním, které se většinou zaměřují jen na jeden operační systém.[46]



Obr. 9.2 Kit Arduino UNO R3.

8.2.1 Bluetooth 4.0 HM-10 BLE klon

Modul HM-10 je malý SMD modul Bluetooth 4.0 podporující BLE. Pro svou funkčnost používá čip CC2540 nebo CC2541, celý modul je vyráběn společností Jinan Huamao, avšak existuje velké množství různých klonů, modul pracuje na systému Android. Proud v pohotovostním stavu se pohybuje mezi 90-400 μA, a rozměrově je velmi malý 43x15 mm. Obsahuje 6 pinů:

- STATE – Užívá dvou hodnot HIGH a LOW, tento pin se užívá především k připojení LED diody, která slouží jako informační.
- RXD – Pin, který se používá k přijímání dat ze sériové komunikace.
- TXD – Pin, který se využívá k vysílání dat prostřednictvím sériové komunikace.
- GND
- VCC – Slouží k napájení modulu.
- EN – Při připojení k jinému zařízení prostřednictvím Bluetooth, může přerušit toto spojení.

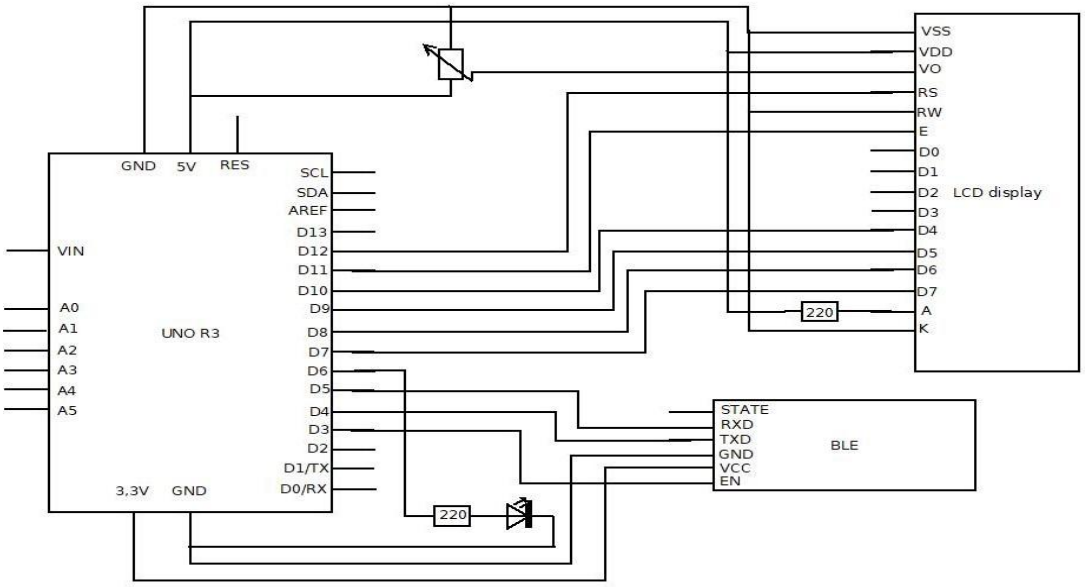
Modul komunikuje prostřednictvím sériového kanálu, prostřednictvím rozhraní UART. Odesílání dat funguje na principu nastavení nejprve vlastní charakteristiky na hodnotu, zprávu, kterou chceme odesílat, až následně po tomto nastavení se zpráva odešle. Vzdálené zařízení mezitím skenuje a čeká na příchod zprávy. Po přijetí odešle potvrzení. Řetězec, který se odesílá, nesmí přesáhnout hodnotu 20 znaků, jinak dojde k rozdělení a odesílání pomocí více zpráv, v každé správě se odesílá i UUID zařízení.

8.3 Program pro přenos prostřednictvím BLE

8.3.1 Použité sou

8.3.2 částky a schéma zapojení

- Kit Arduino UNO R3
- I IC I2C Display LCD 1602 16X2 Znaků LCD Modul Modrý 16-PIN
- Potenciometr 1KOhm lineární
- LED dioda červená 5mm
- 2 x Rezistor 220Ω
- Arduino Android IOS HM-10 klon Bluetooth 4.0 BLE CC2540 CC2541 Sériový Bezdrátový Modul – Datový list s veškerými parametry v příloze



Obr. 9.3 Schéma zapojení.

8.3.3 Vize programu

Program byl navržen pro bezdrátovou komunikaci prostřednictvím Bluetooth LE, k tomu byl použit kit od společnosti Arduino, UNO R3. Jako jednotku schopnou BLE byl zvolen klon Bluetooth 4.0 HM-10, který zvládá tuto komunikaci prostřednictvím sériového terminálu. Jako druhé Bluetooth komunikační zařízení byl vybrán mobilní telefon Doogee S30 s terminálem Seriál Bluetooth Terminal od vývojářů Kai Morich, tato aplikace je bezplatná.

Na programu je snaha demonstrovat některé možnosti využití této technologie přenosu. Program má být především přehledný s možností obousměrné komunikace. Proto zde nalezneme funkci pro odesílání textových zpráv pojmenovanou CHAT a funkci pro zjištění doby. Další možností je funkce LED, která demonstruje možnost ovládání osvětlení například v domácnosti. Poslední funkcí je možnost ovládání textu na LCD display prostřednictvím BLE přenosu. Zbytek kódu i s popisem viz Příloha.

```
void setup() {
  bluetooth.begin(9600);                                    // skrze Softwarovou sériovou linku rychlostí 9600 baud
  Serial.begin(9600);                                       // komunikace po sériové lince rychlostí 9600 baud
  pinMode(led, OUTPUT);                                    // nastavení pinu s LED diodou jako výstup
  lcd.begin(16, 2);                                        //pocet míst na LCD (16 sloupců,2řádky)
  lcd.print("INFORMACNI PANEL");
  vypisMENU();
}
```

Obr. 9.4 Nastavení rychlosti a spuštění komunikace.

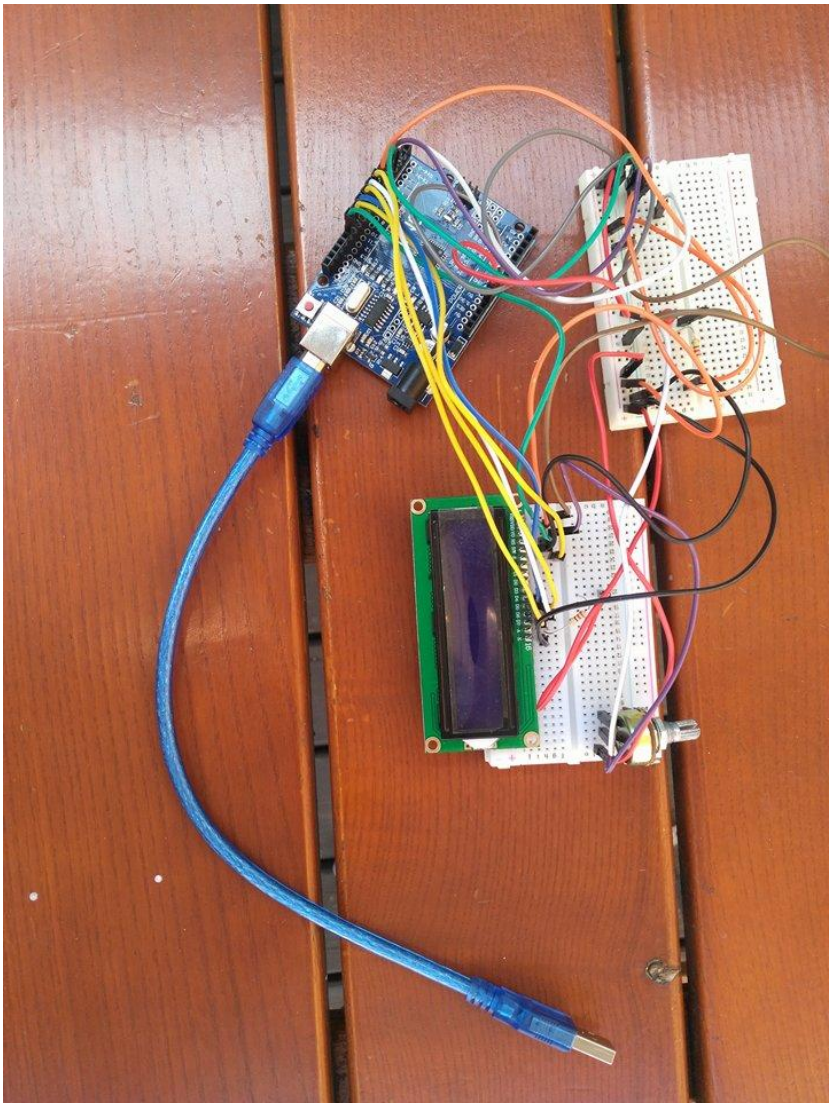
8.3.4 Realizace

8.3.4.1 Zapojení

Jako první součástku připojujeme Bluetooth modul, ten obsahuje 6 pinů, pro správnou funkci stačí však zapojení pouze 4. Na pin VCC napojíme napájení pro modul HM-10 se napájecí napětí pohybuje mezi 3,3-6V, avšak doporučeno je 5V. Po připojení napájecího napětí je potřeba připojit zem GND do stejnojmenného pinu, při správném zapojení dochází k blikání LED diody na modulu. Mezi velmi důležité piny pro sériovou komunikaci patří TXD (vysílání) a RXD (přijímání), ty jsou napojeny na digitální výstup Arduino kitu (D4, D5). Následně je výhodné zapojit obvod obsahující červenou LED diodu, k tomu je zapotřebí přiřadit předřadný odpor 220 Ω. Katodu diody připojíme na zem a anodu s předřadným odporem na D6, tento výstup podporuje PWM, to následně umožňuje regulaci.

Zapojení LCD display je o něco složitější, a je potřeba přidat potenciometr k regulování odporu a tím i napětí. Po připojení regulovaného pinu potenciometru na VO pin LCD lze regulovat jeho kontrast. Napájecí napětí 5V přivedeme na pin VDD a také na pin 15 (A), před tento pin zařadíme předřadný odpor (220 Ω). Tento pin je určen pro podsvícení, zadní osvětlení má nestarost pin 16 označovaný jako K na ten přivedeme zem. Zem je nutné přivézt i na RW tento pin udává možnost čtení či zápisu do registru. Pin RS vybírá mezi registrem příkazů a datovým registrem, tento pin je potřeba připojit na Arduino UNO R3 u našeho zapojení na pin D12, D11 pin napojíme na LCD pin E, ten se stará o odesílání dat do datových vstupů, ty jsou 8bitové a stačí pro naše zapojení 4piny,

které jsou zapojená na digitální piny kitu.



Obr. 9.5 Zapojení.

8.3.4.2 Programování

Při programování je nejprve potřebné zapnout sériovou komunikaci, k tomu je potřebné inicializovat knihovnu SoftwareSerial.h a následně sériovou komunikaci Buetooth k tomu je potřebné znát zapojení a správně přiřadit piny stejně jako u inicializace LCD displey, k tomu je potřebná knihovna LiquidCrystal.h.

V hlavní funkci Setup zapneme sériové komunikace a nastavíme jejich rychlost v Baudech, ta závisí na nastavení BLE modulu při nastavení jež není shodné, dochází k záměně znaků a nesrozumitelnosti komunikace. Zde také nastavíme LED diodu, které přiřadíme pin 6.

Program dále pokračuje do funkce look funkce je bez návratové hodnoty a opakující se. Navíc slouží jako volání funkce menu, kam odesílá řídící znak, ten je typu

char. 5ídící znak se získá ze zásobníku kam je ukládá pomocí našeho zadávání do sériové komunikace, či prostřednictvím Blutooth kanálu, ve funkci menu je tento znak porovnáván a následně je vykonáván příkaz ke kterému patří.

Pokud se nepodaří příkaz přiřadit, vypíše se neznámí příkaz, jinak je znak přiřazen a příkaz vykonáván. K určení příkazu je použita funkce switch a case.

Při zadání příkazu L se vyvolá funkce pro zadávání znaků do LCD display. Display má 16x2 míst první řádek je však použit, a tak je možné použít pouze 16 znaků pro sdělení prostřednictvím LCD. Po odeslání další informace je původní přepsaná. Při vystoupení z funkce je potřeba zadat první znak /, díky porovnávání prvního znaku lze pomocí znaku lomeno vrátit se zpět do funkce look. Obdobně je řešena funkce chat, jen se posílá obousměrná komunikace.

Při zapnutí LED diody, program vyžaduje hodnotu proměnné jas, ta je nastavena původně na hodnotu 210 a může se pohybovat jen mezi hodnotami 0 až 250. Pomocí příkazů plus a mínus lze proměnou jas měnit. Ke změně hodnoty je použita pomocná proměnná s proměnnou skok, ta udává velikost změny.

8.3.5 Problémy při vytváření programu

První větší problém nastal při snaze komunikovat prostřednictvím mobilního telefonu. Přesněji řečeno při zadávání znaků do fronty (bufferu). Kdy při použití více znaků byly vyhodnoceny všechny znaky, navíc při odesílání docházelo vždy k odeslání dalšího znaku prostřednictvím terminálu. To bylo vyřešeno změnou struktury příchozích znaků, již není načítána hodnota byte, nýbrž jsou znaky načteny jako řetězec String. Posléze je první znak na místě 0 uložen do proměnné, typu char, a následně porovnáván s příkazy. Navíc proměnná, typu char, se mnohem lépe porovnává.

Další zásadním problémem byla nefunkčnost modulu Bluetooth 4.0 HM-10, který pravděpodobně z důvodu závady klonu přestal vysílat a přijímat.

Posledním problém nastal při nastavování BLE modulu, který se při resetu nastavil pouze do vysílacího modulu. Navíc v datovém listě jsou jisté nesrovnalosti.

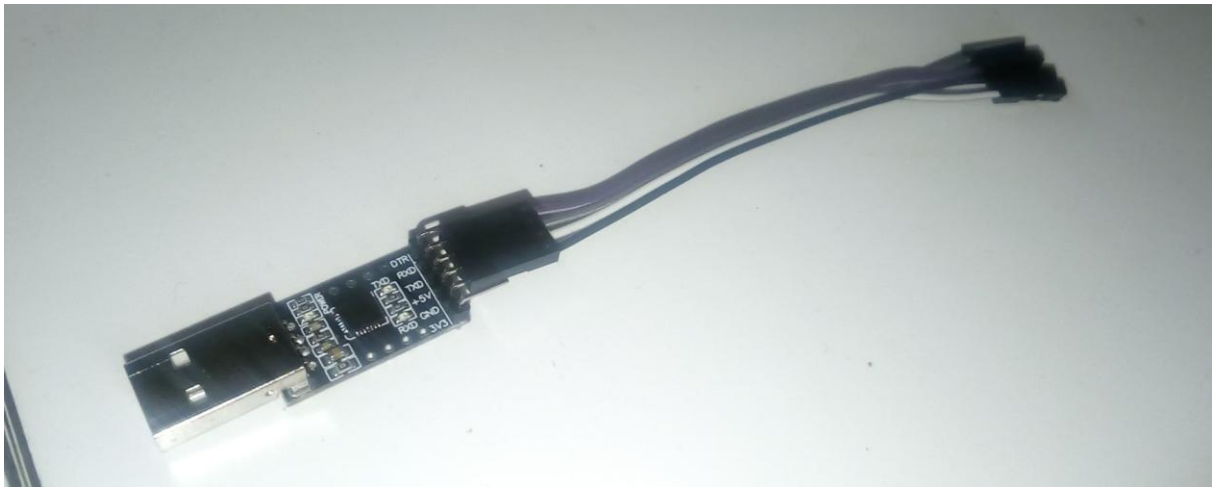
```
if (bluetooth.available() > 0) {                    // zjisteni zda je znak ve fronte
  retez = bluetooth.readStringUntil(lom);           // uložení retezce do promené
  Prvniznak = retez[0];                             //prvniznak= prvni znak z retezce
  Serial.print("Příkaz: ");
  Serial.write(Prvniznak);
```

Obr. 9.6 Načítání fronty z připojeného zařízení.

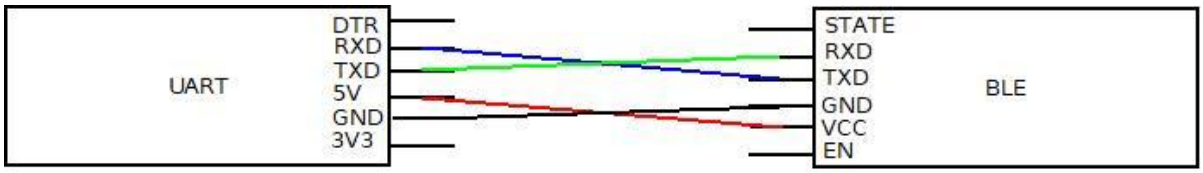
8.3.6 AT příkazy

Bluetooth 4.0 BLE HM-10 modul se ovládá pomocí příkazů AT. Některé tyto příkazy nalezneme již v datovém listě (viz. Přílohy). K jiným dopomáhá příkaz AT+HELP. Bohužel datový list sebou nese množství nesrovnalostí, a tak je lepší k nastavení modulu použít UART, který se skládá ze 6 pinů. Pro nastavení modulu HM-10 však postačí 4 piny. Při propojení je potřeba především propojit pin RXD vždy s TXD a opačně, tedy křížem. Pin TXD slouží jako vysílací pin, a proto je nutné ho spojit s pinem příjímacím RXD. Pin STATE slouží především jako informační pin. Pin EN je zde z důvodu ukončení aktivního spojení.

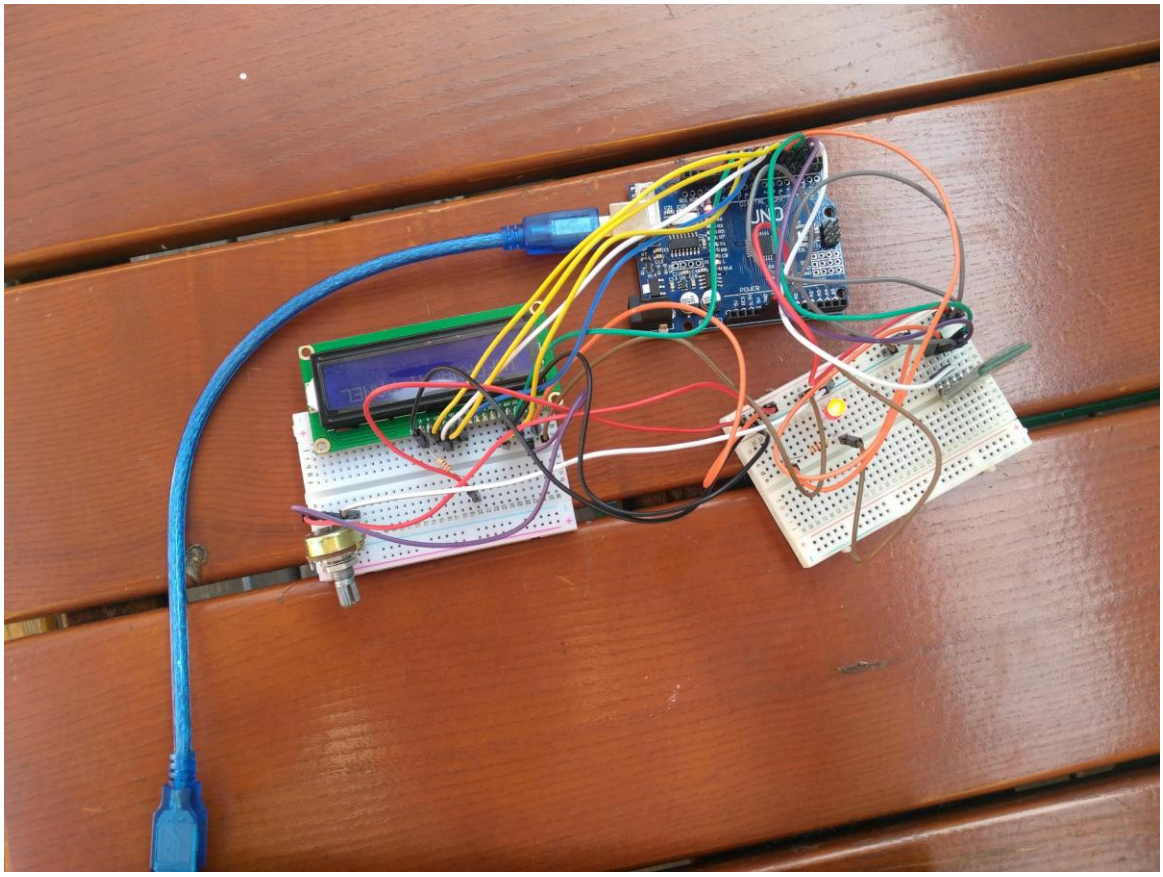
Mezi důležité příkazy patří především příkaz AT+MODE, který určuje schopnost zařízení, dává mu mód všesměrový, vysílací či příjicí. Dalším zajímavým příkazem je příkaz AT+ROLE, zde je na výběr z možností MASTER nebo SLAVE. U MASTER se jedná o zařízení, které je schopno vyhledat, navázat a sestavit spojení s jiným Bluetooth zařízením. Mezi další příkazy patří nastavení UUID či zvolení hesla pro spárování. Nastavení stop bit, který má funkci závěrného bitu, jež identifikuje při asynchronních přenášených bitech konce datových slov. Dalším zajímavým nastavením je nastavení paritního bitu, který slouží pro detekci chyb, a určuje sudost, či lichost jedničkových bitů ve slově. Nalezneme i příkaz pro nastavení diody. Nastavení se provádí velmi jednoduše, přesto je potřeba si dávat pozor především na AT+RENEW. Tento příkaz sice vrátí modul do továrního nastavení, avšak dá velké množství práce ho zpětně nastavit, i proto se tento příkaz nedoporučuje. Další informace pro nastavení modulu HM-10 jsou dostupné na datovém listě či [54].



Obr. 9.7 UART.



Obr. 9.8 Zapojení UART a modul HM-10.



Obr. 9.9 Zapojení všech komponentů a spuštění program.

9 Závěr

Cílem bakalářské práce bylo seznámení se s dostupnými možnostmi bezdrátové komunikace prostřednictvím rádiových signálů na krátké vzdálenosti.

V teoretické části jsem nejprve rozebral elektronickou komunikaci a uvedl její tři základnídruhy. V další části jsem se zaměřil na rozdělení podle určitých parametrů, mezi které patří typ komunikace, frekvenční pásmo, rozsah komunikace a licence používaných pásem. Dále jsem se také zmínil o modulaci signálu a rozdělení ISO/OSi modelu, jehož části struktury používá elektronická komunikace.

Po obecném charakterizování jsem se mohl zaměřit přímo na určité technologie a standardy elektronické komunikace. Jako vše má své výhody a nevýhody, tak ani tato komunikace není výjimkou, a proto každý druh má své specifické využití. Standard Wi-Fi patří mezi nejrozšířenější, a dokonce svým dosahem patří již mezi LAN sítě. Velkou problematikou tohoto standardu je velká spotřeba energie v čemž zaostává za ostatními. Naopak technologie Bluetooth využívá od verze 4.0 možnosti LowEnergy, díky níž není neustále zatížena a tím snižuje spotřebu energie. Bluetooth se rozšiřuje i do oblasti IoT, kde tvoří konkurenci protokolů Zigbee a Z-Wave. Oba protokoly jsou energeticky příznivé a tvoří zajímavé možnosti využití v chytrých domácnostech, zdravotnictví a automatizaci průmyslu. Na který se specializuje především Zigbee. Podle mě zajímavou možnost tvoří komunikace pomocí protokolu Insteon, který využívá možnost dvojí sítě. To nabízí zajímavé zprostředkování dvoublokové topologie, bohužel v rámci rychlosti přenosu zaostává. Následující technologii, kterou jsem se zabýval, je RFID a z ní vycházející NFC. Obě technologie jsou velmi odlišné od ostatních a zaměřují se na naprosto jiný okruh trhu. Systémy NFC nacházejí rychle svá uplatnění a věřím, že její obliba poroste. Možnosti využití mobilního telefonu místo platební karty, čipu nebo jako medium nahrazující papírovou formu, jsou více než zajímavé. Naproti tomu RFID která vznikla jako náhrada za čárové kódy, nachází místo především v lokalizaci zvířat či ve skladech. Mojí snahou bylo přiblížit vypsané technologie seznámit s nimi a pomoci s výběrem.

Do praktické části této práce jsme vybral specifikaci Bluetooth 4.0 LE, pomocí ní vytvářím bezdrátový, tato specifikace sice nejprve nesla název Wibree, následně se podařilo tento standard dostat pod Bluetooth SIG. Snažím se tuto technologii rozebrat a vyzdvihnout hlavní části. Zmiňuji se také o hardwaru, softwaru Arduino.

Mě samotného překvapilo řešení Bluetooth LE, a to jakým stylem šetří svou spotřebu energie, čemuž používá Advertising pakety. Bluetooth od svého vzniku udělalo velký

pokrok, ale největší skok přišel právě díky LE.

Samotný program má demonstrovat, jednu z hlavních možností užití BLE a to u chytrých žárovek, kterou jsem nahradil červenou LED diodou. Program ukazuje též na možnost využívání Informačních tabulí, či možnost komunikace v rámci menší sítě, například v některé firmě prostřednictvím sériového využití BLE.

Tato práce mě především seznámila s možnostmi bezdrátové komunikace, dala mi ucelený pohled na tuto problematiku a i zkušenosti, díky kterým věřím, že bych byl schopen v praxi rozhodnout, v jakém případě je vhodnější použít kterou z těchto možností. Před zadáním této práce jsem znal především Wi-Fi dnes, mě například velmi zajímá možnost použití Insteon technologie.

Seznam literatury a informačních zdrojů

[1] DUKA, Miroslav. *Základy wifi sítí* [online]. Cheb, 2009 [cit. 2018-04-04]. Dostupné z: http://absolventi.gymcheb.cz/2010/miduka/oktava/vos.html. Seminární práce.

[2] JELÍNEK, Vladislav, ed. *Počítačové sítě* [online]. , 26 [cit. 2018-04-28]. Dostupné z: http://slideplayer.cz/slide/1947985/

[3] *IEEE 802.11* [online]. 2010 [cit. 2018-27-3]. Dostupné z: http://wi-fi.unas.cz/ieee-802-11.php

[4] *Wi-Fi Wireless LAN* [online]. 2010 [cit. 2018-04-04]. Dostupné z: http://wi-fi.unas.cz/

[5] WiFi isn't short for "Wireless Fidelity". *Boingboing* [online]. 8.11.2005 [cit. 2018-04-04]. Dostupné z: https://boingboing.net/2005/11/08/wifi-isnt-short-for.html

[6] ING. JAKUB DŽUBERA, Ing. Jakub. *Elektrorevue* [online]. [cit. 2018-04-04]. Dostupné z: http://www.elektrorevue.cz/clanky/04066/index.html

[7] *NOVÉ TECHNOLOGIE BEZDRÁTOVÁ KOMUNIKACE A PŘENOS INFORMACÍ POMOCÍ LED ŽÁROVEK* [online]. In: . 2014 [cit. 2018-03-27]. Dostupné z: http://www.inuru.com/index.php/nove-zdroje/technologie/660-prenos-informaci-pomoci-led-zarovek

[8] ECKHARDTOVÁ, Dita. Bez drátů ve zkratce: Bluetooth versus WiFi (Seznamte se s 'Wireless') Zdroj: https://technet.idnes.cz/bez-dratu-ve-zkratce-bluetooth-versus-wifi-seznamte-se-s-wireless-1cv-/notebooky.aspx?c=A040119_5250250_tech-a-trendy-nb. *Technet.idnes* [online]. [cit. 2018-03-27]. Dostupné z: https://technet.idnes.cz/bez-dratu-ve-zkratce-bluetooth-versus-wifi-seznamte-se-s-wireless-1cv-/notebooky.aspx?c=A040119_5250250_tech-a-trendy-nb

[9] Wireless. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 2015 [cit. 2018-04-04]. Dostupné z: https://en.wikipedia.org/wiki/Wireless

[10] ČESKÁ REPUBLIKA. Národní kmitočtová tabulka: Sbírka zákonů č. 423 / 2017. In: *Sbírka zákonů*. 2017, ročník 2017, číslo 423. [cit. 2018-03-27] Dostupné z:

https://www.ctu.cz/sites/default/files/obsah/stranky/539/soubory/narodnikmitoctova tabulka.pdf

[11] Žalud, V., *Multimediální přenosy signálů* , ČVUT, Praha 1995, [cit. 2018-03-29]

[12] Využívání vymezených rádiových kmitočtů. *Český telekomunikační úřad* [online]. [cit. 2018-03-29]. Dostupné z: https://www.ctu.cz/vyuzivani-vymezenych-radiovych-kmitoctu

[13] *Wi-fi* [online]. [cit. 2018-03-29]. Dostupné z: http://www.lnzps.estranky.cz/clanky/vyhody-a-nevyhody-wifi.html

[14] Výhody Wi-Fi. *IBS s.r.o.* [online]. [cit. 2018-04-04]. Dostupné z: http://www.ibs.cz/vyhody-wifi

[15] Bezdrátové sítě (WiFi, Bluetooth, ZigBee) a možnosti jejich implementace. *Docplayer*[online]. [cit. 2018-04-04]. Dostupné z: http://docplayer.cz/12704159-Bezdratove-site-wifi-bluetooth-zigbee-a-moznosti-jejich-implementace.html

[16] MIKÉSKA, Ing. Zdeněk. Specifikace rádiové části systému Bluetooth. *Elektrorevue* [online]. [cit. 2018-04-18]. Dostupné z: http://www.elektrorevue.cz/clanky/04003/index.html

[17] *Bluetooth* [online]. [cit. 2018-04-18]. Dostupné z: https://www.bluetooth.com

[18] KOVAŘÍK, David. Bluetooth – modrozub pod drobnohledem (vědecké okénko). *Mobilizujeme* [online]. 18.12.2011 [cit. 2018-04-18]. Dostupné z: https://mobilizujeme.cz/clanky/bluetooth-modrozub-pod-drobnohledem-vedecke-okenko

[19] Technologie Bluetooth a BlueJacking. *Security-Portal.cz* [online]. 2005 [cit. 2018-04-18]. Dostupné z: http://www.security-portal.cz/clanky/technologie-bluetooth-bluejacking

[20] DOLEŽAL, R. Bezpečnost Bluetooth: [online]. 2007, [cit. 2018-04-18]. Dostupné z: https://dsn.felk.cvut.cz/wiki/_media/vyuka/cviceni/x36mti/prezentace2007/dolezr1-doc.pdf

[21] Uživatel:Remektom. *HPM wiki* [online]. [cit. 2018-04-18]. Dostupné z: http://noel.feld.cvut.cz/vyu/a2b31hpm/index.php/U%C5%BEivatel:Remektom

[22] KOTON, J., ČÍKA, P., KŘIVÁNEK, V. Standard nízkorychlostní bezdrátové komunikace ZigBee [online]. Brno: VUT, 2006 – [cit. 2018-04-18]. Dostupné na www: http://access.feld.cvut.cz/view.php?cisloclanku=2006032001

[23] KYSELÝ, Tomáš. *UNIVERZÁLNÍ BEZDRÁTOVÝ KOMUNIKAČNÍ SPOJ POMOCÍ ZIGBEE MODULŮ* [online]. Brno, 2014 [cit. 2018-04-18]. Dostupné z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=86166. BAKALÁŘSKÁ PRÁCE. VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ. Vedoucí práce PROF. ING. ALEŠ PROKEŠ, PH.D.

[24] *INSTEON* [online]. [cit. 2018-04-28]. Dostupné z: https://www.insteon.com/technology#technologycompared

[25] *Smarthome: WHAT IS HOME AUTOMATION?* [online]. [cit. 2018-04-28]. Dostupné z: https://www.smarthome.com/sc-what-is-home-automation

[26] *Insteon: WHITEPAPER: Compared* [online]. 2005 [cit. 2018-04-28]. Dostupné z: http://cache.insteon.com/documentation/insteon_compared.pdf

[27] Co je RFID. *RFID portal* [online]. [cit. 2018-05-18]. Dostupné z: https://www.rfidportal.cz/index.php?page=rfid_obecne

[28] STANDARD EPC. *RFID-EPC* [online]. [cit. 2018-05-18]. Dostupné z: https://www.rfid-epc.cz/co-je-rfid/standard-epc

[29] RFID. In: *Wikipedia: the free encyclopedia*[online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2018-05-18]. Dostupné z: https://cs.wikipedia.org/wiki/RFID

[30] Electronic Product Code. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikim edia Foundation, 2001- [cit. 2018-05-18]. Dostupné z: https://en.wikipedia.org/wiki/Electronic_Product_Code

[31] RFID. *BARTECH* [online]. [cit. 2018-05-18]. Dostupné z: http://bartech.cz/reseni/technologie/rfid/

[32] *ZWAVE: Developer* [online]. [cit. 2018-05-04]. Dostupné z: http://zwavepublic.com/developer

[33] Z-Wave. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2018-05-04]. Dostupné z: https://en.wikipedia.org/wiki/Z-Wave

[34] Z-Wave. *Alza.cz* [online]. [cit. 2018-05-04]. Dostupné z: https://www.alza.cz/z-wave-art17515.htm

[35] Výhody technologie Z-Wave. *SmarterHOME: Home Automation a Control* [online]. [cit. 2018-05-04]. Dostupné z: https://smarterhome.sk/cs/informacie/vyhody-z-wave-10

[36] What the heck are ZigBee, Z-Wave, and Insteon? Home automation standards explained. *Digital TRENDS* [online]. [cit. 2018-05-04]. Dostupné z: https://www.digitaltrends.com/home/zigbee-vs-zwave-vs-insteon-home-automation-protocols-explained/

[37] ROSENBERG, Martin a Tomáš MERTLÍK. Technologie NFC – popis, bezpečnost a využití. *Elektrorevue: časopis pro elektotechniku*[online]. 2013, 2013, (2), 8 [cit. 2018-05-19]. Dostupné z: www.elektrorevue.cz/cz/download/technologie-nfc---popis--bezpecnost-a-vyuziti/

[38] Co je NFC?. *Digital TRENDS* [online]. [cit. 2018-05-19]. Dostupné z: https://www.alza.cz/co-je-nfc#nfcvyuzitivpraxi

[39] KILIÁN, Karel. Co je NFC a k čemu je dobré ho použít?. *SvětAndroida* [online]. 10.5.2016 [cit. 2018-05-19]. Dostupné z: https://www.svetandroida.cz/co-je-nfc-k-cemu-je-dobre-ho-pouzit/

[40] DOUPAL, František. NFC - bezdrátová komunikace blízké budoucnosti?. *NOTEBOOK.cz*[online]. 17.8.2011 [cit. 2018-05-19]. Dostupné z: https://notebook.cz/clanky/technologie/2011/nfc-bezdratova-komunikace-blizke-budoucnosti

[41] Near Field Communication. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 2012 [cit. 2018-05-19]. Dostupné z: https://en.wikipedia.org/wiki/Near_Field_Communication?oldid=505633671

[42] Modulace. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2018-05-21]. Dostupné z: https://cs.wikipedia.org/wiki/Modulace

[43] JANŮ, Stanislav. Bluetooth 5: vyšší rychlost a lepší dosah už příští týden Více na: https://www.mobilmania.cz/bleskovky/bluetooth-5-vyssi-rychlost-a-lepsi-dosah-uz-pristi-tyden/sc-4-a-1334708/default.aspx. *Mobilmania.cz* [online]. 11.6.2016 [cit. 2018-05-22]. Dostupné z: https://www.mobilmania.cz/bleskovky/bluetooth-5-vyssi-rychlost-a-lepsi-dosah-uz-pristi-tyden/sc-4-a-1334708/default.aspx

[44] SCHAFFEROVÁ, Magdalena. Jak se vyznat v záplavě sítí pro internet věcí. *ZOOCO: Žijte chytře* [online]. 20.10.2017 [cit. 2018-05-21]. Dostupné z: https://www.zooco.io/blog/jak-se-vyznat-v-zaplave-siti-pro-internet-veci/

[45] RICHTEROVÁ, PH.D., doc. Ing. Marie. *Šíření rádiových vln: Podstata jednotlivých druhů spojení, výhody a nevýhody jejich použití* [online]. Brno [cit. 2018-05-22]. Dostupné z: https://moodle.unob.cz/pluginfile.php/18130/mod_resource/content/1/%C5%A0%C3%AD%C5%99en%C3%AD%20r%C3%A1diov%C3%BDch%20vln.pdf. UNIVERZITA OBRANY v Brně.

[46] *Arduino.cz* [online]. [cit. 2018-05-30]. Dostupné z: https://arduino.cz/

[47] Co je to Arduino?. *CzechDUINO.cz: První český Arduino obchod* [online]. [cit. 2018-05-30]. Dostupné z: http://czechduino.cz/?co-je-to-arduino,29

[48] GRABIANOWSKI, Ed. Is Wibree going to rival Bluetooth?. *Howstuffworks* [online]. [cit. 2018-05-30]. Dostupné z: https://electronics.howstuffworks.com/wibree.htm

[49] TIP#883: Co je to Bluetooth LE, BLE, Bluetooth Low Energy, Bluetooth Smart, Bluetooth 5)?. *@365tipu* [online]. 2017-09-06 [cit. 2018-05-30]. Dostupné z: https://365tipu.cz/2017/09/06/tip883-co-je-to-bluetooth-le-ble-bluetooth-low-energy-bluetooth-smart-bluetooth-5/

[50] PALIVEC, Pavel. Bluetooth Low Energy. *Dps-az* [online]. [cit. 2018-05-30]. Dostupné z: https://www.dps-az.cz/soucastky/id:9912/bluetooth-low-energy

[51] HAVLENA, Matouš. Bluetooth Low Energy. *Matouš Havlena: Osobní blog* [online]. [cit. 2018-05-30]. Dostupné z: http://www.havlena.net/en/location-technologies/ibeacons-how-do-they-technically-work/

[52] How Bluetooth LE works?—Link layer. *Medium* [online]. 2016-05-08 [cit. 2018-05-30]. Dostupné z: https://medium.com/@zpcat/how-bluetooth-le-works-link-layer-b18475250259

[53] *Adafruit: Bluetooth smart* [online]. Autor: Kevin Townsend [cit. 2018-05-30]. Dostupné z: https://learn.adafruit.com/introduction-to-bluetooth-low-energy/introduction

[54] CURREY, Martyn. HM-10 Bluetooth 4 BLE Modules. *Martyn Currey* [online]. 2017-01-05 [cit. 2018-06-02]. Dostupné z: http://www.martyncurrey.com/hm-10-bluetooth-4ble-modules/

Přílohy (Struktura přiloženého CD)

Struktura CD s přílohami obsahuje následující:

- `DataSheet/` - Adresář obsahuje datové listy komponentů potřebných pro zapojení praktické části.
  - `Arduino_UNO_Starter.pdf` – Obsahuje názvy pinů na kitu UNO R3.
  - `HM-10.pdf` – Datový lit s parametry k modulu Bluetooth HM-10 4.0 BLE klon.
  - `UART.pdf` – Datový list s parametry k převodníku/programatoru 6Pin USB TTL UART
- `Program/` - Adresář obsahující potřebné soubory k programu.
  - `Libraries/` - Adresář obsahující knihovny.
  - `TP_BLE/` - Adresář obsahující kód.
    - `TP_BLE.ino` – Ardujno soubor obsahující kód.
- Schéma_zapojeni/ -Adresář obsahující schémata.
  - `Schema_obvod.jpeg` – Schéma zapojení obvodu.
  - `Schema_obvod_bar.jpeg` – Schéma zapojení obvodu barevně pro snažší zapojení.
  - `UART_HM-10.jpeg` – Schéma zapojení UART a modul HM-10 pro nastavení.
- `Obr/` -Adresář obsahující fotografie zapojených komponentů.

Program TP_BLE:

```
// nastavení propojovacích pinů Bluetooth a LED diody
#define RX 5
#define TX 4
#define led 6
char a = 0;
//ukoncovaci znak
int lom = 10;
int jas = 210 ;                                                    // jas
LED
int skok = 10;                                                     // jas
int pom;
//pomocna promena
String END = END;
// připojení knihovny SoftwareSerial
#include <SoftwareSerial.h>
//připojení knihovny pro LCD
#include <LiquidCrystal.h>
// inicializace Bluetooth modulu z knihovny SoftwareSerial
SoftwareSerial bluetooth(TX, RX);
// inicializace LCD pinů
LiquidCrystal lcd(12, 11, 10, 9, 8, 7);

void vypisMENU () {

//bluetooth výpis
  bluetooth.println("MENU:");
  bluetooth.println("T...Zjištění času spuštění");
  bluetooth.println("L...BLE Informačni panel");
  bluetooth.println("1...Zapnutí LED.");
  bluetooth.println("\t  + ...Zvýšení jasu LED");
  bluetooth.println("\t  - ...Snížení jasu LED");
  bluetooth.println("0...Vypnutí LED");
  bluetooth.println("C...Zapnutí CHATU.");
  bluetooth.println("?...MENU.");

//serial výpis
  Serial.println("MENU:");
  Serial.println("T...Zjištění času spustění");
  Serial.println("L...BLE Informačni panel");
  Serial.println("1...Zapnutí LED");
  Serial.println("\t\t  + ...Zvýšení jasu LED");
  Serial.println("\t\t  - ...Snížení jasu LED");
  Serial.println("0...Vypnutí LED");
  Serial.println("C...Zapnutí CHATU");
```

```
  Serial.println("?...MENU");
}


void setup() {
  bluetooth.begin(9600);                                          // skrze
Softwarovou sériovou linku rychlostí 9600 baud
  Serial.begin(9600);                                             //
komunikace po sériové lince rychlostí 9600 baud
  pinMode(led, OUTPUT);                                          //
nastavení pinu s LED diodou jako výstup
  lcd.begin(16, 2);                                               //pocet
míst na LCD (16 sloupců,2řádky)
  lcd.print("INFORMACNI PANEL");
  vypisMENU();
}

void LCD () {                                                    // Funkce
ovladajici LCD display
  pom = 1;
  bluetooth.println("Informacni tabule: /t/...konec");
  bluetooth.println("Maximálně 16 znaků");
  while (pom) {
//opakovaci podminka
    if (bluetooth.available() > 0) {                             // zjisteni
zda je znak ve fronte
        String prijem;
        prijem = bluetooth.readStringUntil(lom);
        for (int i = 0; i < 15; i++) {
          lcd.setCursor(i, 1);                                    //umisteni
kurzoru na LCD
          a = prijem[i];                                          //nacteni
znaku jednotlive
          lcd.print(a);                                           //vypis
           }
          a = prijem[0];                                          //do
pomocne promene a nactem prvni znak z retezce
          if (a == '/') {                                         //
porovnavam zda ukoncit program
            lcd.setCursor(0, 1);
            lcd.print("____________________");                    //vymazani
obsahu LCD
         pom=0;
        }
      }
    }
```

```
  }

void ledka (int j) {                                                    // vypis
jasu, a funkce
  bluetooth.println("Zapnuta LED dioda.");
  Serial.println("Zapnuta LED dioda.");
  bluetooth.println(j);
  Serial.println(j);
  bluetooth.println(" + ... Zvýší jas.");
  Serial.println(" + ... Zvýší jas.");
  bluetooth.println(" - ... Sníží jas.");
  Serial.println(" - ... Sníží jas.");
}


void chat () {                                                          //funkce
pro chat
  String BLEdata;
  String Data;
  pom = 1;
  bluetooth.println("CHAT: \t /...konec CHATU");
  Serial.println("CHAT: \t /...konec CHATU");
  while (pom) {                                                         //podminka
pro opakovani
    if (bluetooth.available() > 0) {                                    // zjisteni
zda je znak ve fronte
      BLEdata = bluetooth.readStringUntil(lom);                         //nacteni
do retezce
      Serial.print("Přijato: ");
      Serial.println(BLEdata);                                          //vypis
konverzace
      bluetooth.println(BLEdata);                                       //BLE vypis
konverzace
      delay(10);                                                        // krátká
pauza mezi načítáním znaků
      a = BLEdata[0];
      if (a == '/') {                                                   //funkce
pro porovnani s ukoncovacim znakem
        pom = 0;
      }
    }

    if (Serial.available() > 0) {
      while (Serial.available() > 0) {
        Data = Serial.readStringUntil(lom);
        bluetooth.print("Přijato: ");
```

```
        bluetooth.println(Data);
        Serial.println(Data);
        // krátká pauza mezi načítáním znaků
        delay(10);
        a = Data[0];
        if (a == '/') {
          pom = 0;
        }
      }
    }

  }
}



void menu (char znak) {                                          //tridici
funkce
  switch (znak) {                                                //porovnani
s nactenym prikazem
    case '0':
      analogWrite(led, 0);                                       //nastaveni
0 jasu, vypnuti LED
      bluetooth.println("Vypnuti LED diodu.");
      Serial.println("Vypnuti LED diodu.");
      vypisMENU ();
      break;
    case '1':
      analogWrite(led, jas);                                     // zapnuti
LED na hodnotu jasu
      ledka (jas);                                               //volani
vypisu jasu a pridruzenych funkci
      break;
    case 'T':                                                    // zmeri a
vypise cas od zapnuti
      bluetooth.print("Čas od spuštění: ");
      bluetooth.print(millis() / 1000);
      bluetooth.println(" vteřin.");
      Serial.print("Čas od spuštění: ");
      Serial.print(millis() / 1000);
      Serial.println(" vteřin.");
      break;
    case '+':                                                    //pridani
jasu
      pom = jas;
      if (jas < 250) {
```

```
        jas = pom + skok;
        analogWrite(led, jas);                                    // LED
zapnuta na hodnotu jasu
      }
      bluetooth.println(jas);
      Serial.println(jas);
      break;
    case '-':                                                     //snizeni
jasu
      pom = jas;
      if (jas > 0) {
        jas = pom - skok;
        analogWrite(led, jas);
      }
      bluetooth.println(jas);
      Serial.println(jas);
      break;
    case 'L':
      LCD ();                                                     //funkce pro
prenos z bluetooth na LCD
      vypisMENU();
      break;
    case 'C':
      chat();                                                     // funkce pro
chat mezi seriovou komunikaci Arduino a BLE
      vypisMENU();
      break;
    case '?':
      vypisMENU();
      break;
    default:                                                      // v pripade
spatne zadaneho prikazu
      bluetooth.print(znak);
      Serial.print(znak);
      bluetooth.println("....Neznamy prikaz \t?...MENU");
      Serial.println("....Neznamy prikaz \t?...MENU");
  }
}



void loop() {
  char Prvniznak;
  String retez;
  if (Serial.available() > 0) {
// zjisteni zda je znak ve fronte
```

```
    retez = Serial.readStringUntil(lom);
// uložení retezce do promené
    Prvniznak = retez[0];
//prvniznak= prvni znak z retezce
    Serial.print("Příkaz: ");
    Serial.write(Prvniznak);
//vypsani prvniho znaku
    bluetooth.print("Příkaz: ");
    bluetooth.write(Prvniznak) ;
    bluetooth.println();
//BLE vypsani prvniho znaku
    Serial.println();
    menu(Prvniznak);
// prevod do funkce menu
  }
  if (bluetooth.available() > 0) {
// zjisteni zda je znak ve fronte
    retez = bluetooth.readStringUntil(lom);
// uložení retezce do promené
    Prvniznak = retez[0];
//prvniznak= prvni znak z retezce
    Serial.print("Příkaz: ");
    Serial.write(Prvniznak);
    bluetooth.print("Příkaz: ");
    bluetooth.write(Prvniznak) ;
//BLE vypsani prvniho znaku
    bluetooth.println();
    Serial.println();
    menu(Prvniznak);
  }
}
```

Použité knihovny ke stažení:

SoftwareSerial……. https://www.robot-r-us.com/e/995-softwareserial.html

LiquidCrystal……. https://www.arduinolibraries.info/libraries/liquid-crystal