VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SYSTEMS

IDENTIFIKACE A DEKÓDOVÁNÍ BEZDRÁTOVÉ KOMUNIKACE S VYUŽITÍM SDR

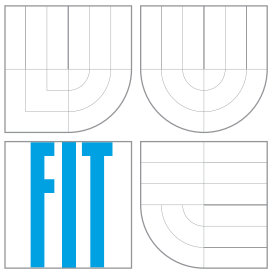
BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

FILIP MATULKA

BRNO 2015

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SYSTEMS

IDENTIFIKACE A DEKÓDOVÁNÍ BEZDRÁTOVÉ KOMUNIKACE S VYUŽITÍM SDR

IDENTIFICATION AND DECODING OF WIRELESS COMMUNICATION USING SDR

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

FILIP MATULKA

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. ZDENĚK VAŠÍČEK, Ph.D.

BRNO 2015

Abstrakt

Cílem této práce je vytvořit systém využívající konceptu softwarově definovaného rádia, který je schopen automatické identifikace komunikačních parametrů a následného dekódování bezdrátové komunikace. Práce se zaměřuje na provoz bezdrátových komunikací v bezlicenčním frekvenčním pásmu a uvažuje základní metody modulace. Výsledek práce je otestován na dvou nezávislých bezdrátových systémech, které ověřily schopnost automatické identifikace komunikačních parametrů.

Abstract

The goal of this thesis is to create the system that uses concept of software defined radio. This system is capable of automatically identifying the communication parameteres and subsequent decoding of wireless communication. The thesis focus on the wireless system operationg in unlicened frequency band and cosidering fundamental modulation metods. The result is tested on two independent wireless systems that verify ability to automatically identify the communication parameters.

Klíčová slova

bezdrátová komunikace, softwarově definované rádio, dekódování

Keywords

wireless communication, software defined radio, decoding

Citace

Filip Matulka: Identifikace a dekódování bezdrátové komunikace s využitím SDR, bakalářská práce, Brno, FIT VUT v Brně, 2015

Identifikace a dekódování bezdrátové komunikace s využitím SDR

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením pana Ing. Zdeňka Vašíčka, Ph.D.

.....
Filip Matulka
19. května 2015

Poděkování

Rád bych poděkoval mému vedoucímu bakalářské práce, Ing. Zdeňku Vašíčkovi, Ph.D., za poskytnutí cenných rad a věcných prostředků pro zpracování této práce.

Obsah

Kapitola 1

Úvod

Stále se zvyšující počet zařízení nás utvrzuje v myšlence, že bezdrátová zařízení jsou automaticky odolná proti odposlechu, neboť pracují ve frekvenčním pásmu, který není přístupný běžným uživatelům. Navíc výrobce bezdrátového zařízení by si přece nedovolil data nějakým jednoduchým způsobem zpřístupnit. S rozvojem technologií a dostupností platforem na bázi softwarově definovaného rádia (SDR) se však bezdrátová komunikace stála artiklem dostupným pro běžného uživatele. Na trhu existují levné přijímače, které jsou schopny pracovat ve frekvencích od desítek MHz až do jednotek GHz. Pokročilejší platformy dovolují dokonce i v tomto frekvenčním spektru vysílat. Lze tak např. realizovat vlastní GSM buňku, pomocí které je možné uskutečňovat telefonní hovory. Uvědomíme-li si tuto skutečnost, absence kabelů u bezdrátových sytému je daní za plné zpřístupnění našeho zařízení blízkému okolí.

Podíváme-li se blíže na princip bezdrátového přenosu zjistíme, že přijímač je schopen přenášenou informaci korektně přijmout pouze jsou-li nastaveny klíčové parametry komunikace, jako je nosná frekvence, typ modulace, atd. Systém založený na principu SDR umožňuje provést integraci více zařízení a navrhnout jeden prvek, který bude např.: sbírat data ze senzorů různých výrobců. Komunikační parametry zabezpečí zařízení proti kolizi s jinými systémy a částečně řeší bezpečnost, protože neznalost komunikačních parametrů zamezí potenciálnímu útočníkovi možnost data správně dekódovat.

Na internetu lze nalézt řadu návodů zabývajících se specifickým dekódování přijatého signálu. Například lze poměrně snadno zachytit data, snímky, ze série družic METEOSAT a mít tak k dispozici povětrnostní podmínky nad daným územím a to bez nutnosti připojení k internetu. Nutnou podmínkou takových aplikací je dopředná znalost parametrů přenosu, který se bude zachytávat. V poslední době lze nalézt stále se rozrůstající se počet SDR přijímačů, které jsou připojeny k internetu. Na stránkách přijímače je typicky zobrazena část spektra a uživatel si může toto spektrum streamovat a později analyzovat. Neexistuje však řešení, které by bylo schopno automaticky analyzovat širší spektrum a dekódovat probíhající komunikace a jejich parametry.

Cílem této práce je sestrojit systém pro automatické identifikování parametrů přenosového kanálu jako je kmitočet nosné vlny, přenosovou rychlost, typ modulace a následně vypsat bitovou posloupnost komunikace. Systém se skládá z hardwarové a softwarové části. Příjem signálu je zajištěn pomocí SDR realizovaného pomocí DVB-T přijímače, který lze pořídit přibližně za dvě stě korun. Tento přijímač je přepnut do režimu, kdy poskytuje surová data, která jsou následně zpracována v softwaru.

Kapitola 2

Princip bezdrátové komunikace

Nežli se budeme věnovat vlastní implementaci, je nutné se nejprve seznámit s principem realizace přenosu digitálního signálu pomocí bezdrátového kanálu. Tato část se proto bude věnovat popisu komunikačních parametrů. Vzhledem k tomu, že veškerá teorie týkající se bezdrátové komunikace přesahuje rámec teto bakalářské práce, je čtenář odkázán na detaily např.: do [7]. Aby bylo možné přenést informaci z vysílače na přijímač volným prostorem je nutné vstupní signál nesoucí užitečnou informaci, též zvaný jako **modulační signál** nebo také jako signál v základním pásmu, převést (modulovat) pomocí některého druhu modulace a nosné vlny na **modulovaný signál**, který má podobné vlastnosti jako nosná vlna. Nosná vlna (anglicky *carrier wave*) se se svými vlastnostmi lépe šíří volným prostorem, má vždy mnohem vyšší frekvenci než modulační signál a má sinusový průběh. Pokud vytváříme komunikační systém je nutné předem rozhodnout na jaké nosné frekvenci bude systém pracovat. Pro účely volného vysílání[1] bylo vyhrazeno tzv. bezlicenční frekvenční pásmo, které se typicky používá pro rádiově řízené modely, bezdrátové ovládání vrat, domácí meteorologické stanice, atd. Mezi nejrozšířenější bezlicenční frekvenční pásma patří pásma 434 MHz (rozsah je 433.05-434.79 MHz) a 868 MHz (rozsah je 863-870 MHz). Dalším často používaným frekvenčním bezlicenčním pásmem je 2.4 GHz (dnes i 5 GHz), ve kterém funguje mnoho standardů např.: WiFi, ZigBee, BlueTooth, atd.

V případě digitální komunikace se datové bity přenášejí pomocí tzv. symbolů, které představují nejmenší jednotku, která lze pomocí kanálu přenést. Symbolová rychlost je analogií bitové rychlosti s jediným rozdílem, kdy v komunikačním systému založeném na vícebitovém symbolu dochází ke zvýšení bitové rychlosti, než kdyby byl systém založen na jednobitovém symbolu. Pokud některý komunikační systém disponuje symbolovou rychlostí 1000 symbolů za sekundu a velikost symbolu jsou dva bity, rovná se jeho bitová rychlost dvojnásobku symbolové rychlosti. Pokud by měl systém velikost symbolu čtyři bity a symbolovou rychlost stejnou jako v předchozím případě, měl by bitovou rychlost čtyřnásobnou atd.

2.1 Nosná vlna

Základním prostředkem, který umožňuje unifikovat jednotlivé bezdrátové komunikace je frekvence nosné vlny. Za účelem snazší unifikace je přidělené frekvenční pásmo rozděleno do kanálů. Každý kanál má většinou stejnou šířku a bývá rozdělen komunikačním standardem.

[1] Bez nutnosti platit za frekvenční rozsahy jako je tomu např.: u televizního vysílání nebo mobilních sítí.

Nejdůležitějším parametrem je nosná vlna, jejíž frekvence ve spektru obsadí místo pro komunikaci. Rozhodující pro komunikaci je tedy frekvence nosné vlny a ne frekvence modulačního signálu. Pokud bude mít komunikační systém nastavenou nosnou vlnu o frekvenci např.: 434.1 MHz může za určitých okolností zároveň komunikovat jiný komunikační systém na jiné nosné vlně o frekvenci např.: 434.2 MHz. I přes to, že se v obou komunikačních systémech používá pro vysílání nosná vlna se sinusovým průběhem, která se ve spektrální části za ideálních podmínek projeví jako úzkopásmová špička, muže se vlivem digitální modulace, která vnáší do přenášeného signálu nespojitosti (např.: nejjednodušší modulace typu ON/OFF prudce přeruší přenášený sinusový signál teoreticky v libovolném bodě), stát, že se ve spektru šířka pásma modulovaného signálu rozšíří. Pokud by bylo toto rozšíření příliš velké, mohlo by dojít k rušení komunikace i těchto dvou komunikačních systému, které nemají nastavenou stejnou frekvenci nosné vlny. Zavedení kanálů frekvenčního pásma není tedy jen kvůli rovnoměrnému rozdělení komunikací v celém pásmu, ale také pro stanovení maximální šířky komunikace, kterou může využít. Zvolený způsob modulace společně s přenosovou rychlostí pak musí zajistit, že šířka pásma nebude překročena.

Pokud dva komunikační systémy komunikují na stejné nosné vlně, musí se zajistit časový multiplex, kdy v danou chvíli vysílá pouze jeden z vysílačů. Pokud by vysílaly oba systémy ve stejnou chvíli na stejné nosné vlně, nebude nikdy možné komunikaci správně demodulovat.

2.2 Modulace

Modulace je proces, ve kterém modulační signál mění vlastnost nebo více vlastností nosné vlny a vzniká tak signál tzv. modulovaný signál, který obsahuje modulační signál i nosnou vlnu. Opačnou operací je demodulace prováděná za účelem získat z modulovaného signálu zpět signál modulační. Existují tři základní typy modulací, které lze mezi sebou libovolně kombinovat:

- Amplitudová modulace (AM) (anglicky *amplitude modulation*)
- Frekvenční modulace (FM) (anglicky *frequency modulation*)
- Fázová modulace (PM) (anglicky *phase modulation*)

2.2.1 Amplitudová modulace

Amplitudová modulace patří mezi modulace s jednou nosnou vlnou. To znamená, že se v modulovaném signálu vyskytuje pouze jedna frekvence, u které se mění amplituda na základě hodnoty amplitudy modulačního signálu. Uvažujme nosnou vlnu s úhlovou frekvencí Ω a s amplitudou A:

$$c(t) = A \cdot \sin(\Omega t).$$

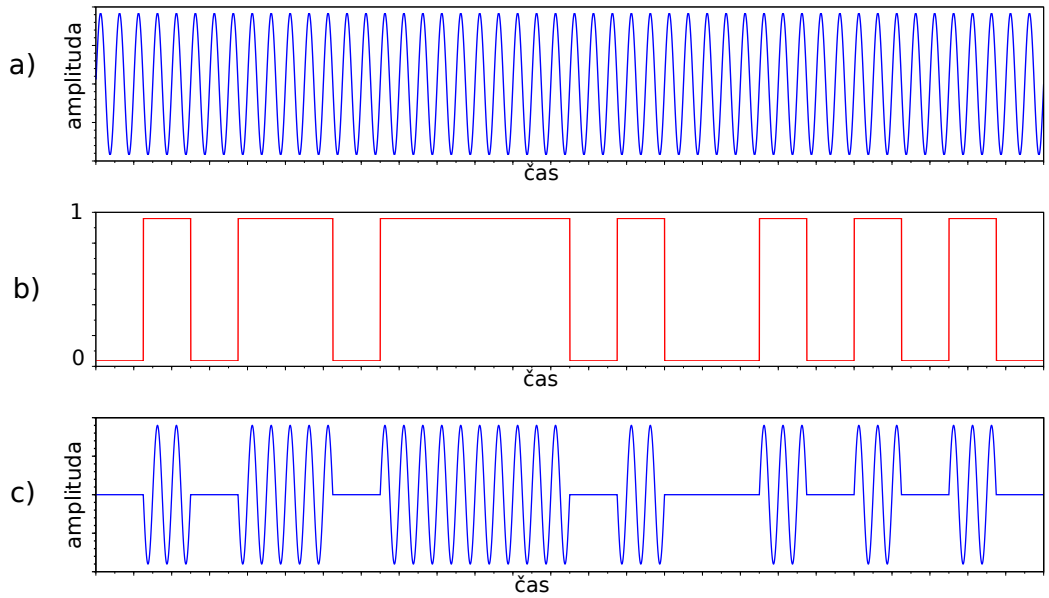
Dále uvažujme modulační signál *m(t)* s úhlovou frekvencí ω, která má mnohem nižší úhlovou frekvenci než Ω (příkladem modulačního signálu muže být akustický signál) a s amplitudou M:

$$m(t) = M \cdot \sin(\omega t).$$

Modulační signál musí splňovat podmínku $M = \langle 0, 1 \rangle$ (M je modulační index[2]), takže $1 + m(t)$ je vždy kladná. Nesplnění této podmínky vede na problémy v demodulaci, protože by docházelo k překryvům modulovaného signálu sebou samým. Výsledný signál je součinem nosné vlny a kladné formule vlny modulační:

$$s_{AM}(t) = (1 + m(t)) \cdot c(t) = (1 + M \cdot \sin(\omega t)) \cdot A \cdot \sin(\Omega t),$$

kde $s_{AM}(t)$ je signál modulovaný amplitudovou modulací. V případě digitálního přenosu je $(1 + m(t))$ sled hodnot symbolů, nejčastěji s hodnotou 1 a 0. Představíme-li si za pomocí matematického vyjádření takový digitálně modulovaný signál, mel by průběh signálu, jenž je uveden na obrázku 2.1.



Obrázek 2.1: Ukázka průběhu nosné vlny (a) modulačního signálu (b) a modulovaného signálu (c), který je výsledkem amplitudové modulace.

Jak je vidět na obrázku 2.1, v případě, že se hodnota číslicového signálu rovná logické 0, má modulovaný signál nulovou amplitudu a tam, kde logické 1 má modulovaný signál amplitudu rovnou okamžité amplitudě nosné vlny. Tato digitální verze amplitudové modulace je známá pod názvem klíčování amplitudovým posuvem (ASK z anglického *amplitude shift keying*, nebo také OOK *on/off keying*), zároveň se jedná o nejrozšířenější typ modulace bezdrátových zařízení v pásmu 434 MHz. Výhoda je bezesporu ve snadné implementaci. Nevýhoda této modulace je, že v případě, kdy se vysílá dlouhý sled logických 0 může díky nulové amplitudě v modulovaném signálu snadno dojít k zaměně za stav, který odpovídá klidu (kdy se nevysílá) a to způsobí desynchronizaci fázového závěsu přijímače. Jedno z možných v praxi používaných řešení, které dovoluje předejít tomuto stavu je např.: kódovat data Manchestrovým kódováním, kde i sled logických 0 způsobí změnu. Nevýhodou Manchestrovým kódováním je však snížení přenosová rychlost na polovinu.

[2]Modulační index, známý také jako modulační hloubka, má přímý vliv na to, jaký tvar bude mít modulovaný signál.

2.2.2 Frekvenční modulace

Frekvenční modulace patří mezi modulace, která má sice také jednu nosnou vlnu podobně jako amplitudová modulace, avšak modulační signál mění frekvenci nosné vlny způsobem, že se pak tato modulace ve spektru projeví jako soubor frekvencí pohybující se kolem nosné vlny. Vždy je však aktivní pouze jedna frekvence a proto mluvíme o modulaci s jednou nosnou vlnou. Frekvence nosné vlny se mění modulačním signálem. Uvažujme nosnou vlnu s úhlovou frekvencí Ω_c a s amplitudou A:

$$c(t) = A \cdot \sin(\Omega_c t),$$

kde Ω_c je v případě frekvenční modulace funkce času. Funkci úhlové frekvence vyjádřenou jako sinusovou funkci (použijeme *cos* pro jednodušší integraci), lze zapsat takto:

$$\Omega_c(t) = \Omega + \Delta\Omega \cos(\omega t).$$

Kde Ω je úhlová frekvence nosné vlny, $\Delta\Omega$ je frekvenční odchylka (také jako frekvenční zdvih), ω je úhlová frekvence modulační vlny. Dosažením dostaneme tvar:

$$s_{FM}(t) = A \cdot \sin((\Omega + \Delta\Omega \cos(\omega t))t) = A \cdot \sin(\Phi(t, \omega)),$$

kde $\Phi(t, \omega)$ je okamžitá fáze pro kterou platí (úhlová frekvence je fyzikální podstatou změna fáze za jednotku času):

$$\Phi(t, \omega) = \int \Omega_c(t)dt = \int \Omega + \Delta\Omega \cos(\omega t)dt = \Omega t + \frac{\Delta\Omega}{\omega} \sin(\omega t).$$

Dosazením funkce $\Phi(t, \omega)$ do $A \cdot \sin(\Phi(t, \omega))$ dostáváme tvar rovnice frekvenční modulace:

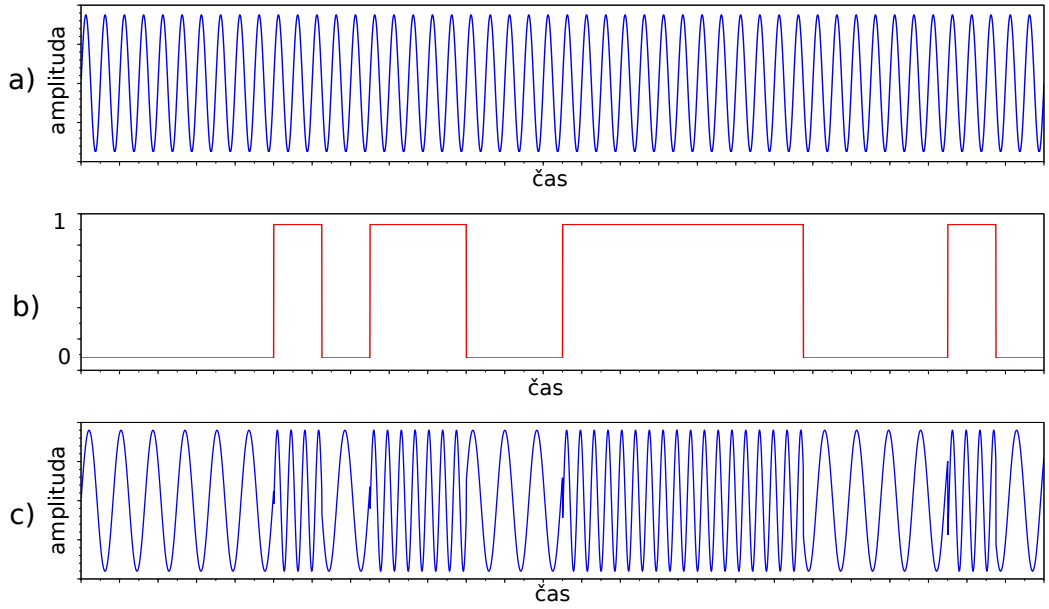
$$s_{FM}(t) = A \cdot \sin(\Omega t + M_{fm} \sin(\omega t))$$

Poměr $M_{fm} = \frac{\Delta\Omega}{\omega}$ se nazývá modulační index a na rozdíl od amplitudové modulace se na něj nevztahuje žádná podmínka. Výsledek $M_{fm} \sin(\omega t)$ pak dosahuje kladných i záporných hodnot, čímž se ve spektru projeví jako oscilace kolem nosné vlny. Modulační signál digitální komunikace vznikne nahrazením funkce $sin(\omega t)$ sledem hodnot -1 a 1, které korespondují logickým hodnotám 0 a 1. Signál modulovaný digitální frekvenční modulací je zobrazen na obrázku 2.2.

Na obrázku je patrná změna frekvence modulovaného signálu na hranách změn logických úrovní modulačního signálu. Nižší frekvenci odpovídá logická 0, vyšší frekvenci odpovídá logická 1. Tato digitální verze frekvenční modulace se nazývá klíčování frekvenčním posuvem (FSK z anglického *frequency shift keying*) a používá se hojně v systémech s vyšším důrazem na bezpečnost, protože u FSK odpadá nevýhoda v podobě nulové amplitudy modulovaného signálu jako je tomu v případě ASK.

Kromě základní varianty FSK, označované také jako 2-FSK, existují i další varianty, které umožňují přenést více datových bitů najednou. Často se také používá varianta 4-FSK, kdy se vysílají čtyři různé frekvence. Tato modifikace umožňuje přenést dva bity současně. Tzn. dosahuje 2x vyšší přenosové rychlosti oproti běžné FSK, při zachování šířky přenosového pásma.

Jako ekvivalent modulačního indexu M_{fm} u frekvenční modulace je také v literatuře často používán pojem rozptyl (anglicky *deviation*). Rozptyl lépe vystihuje sémantiku modulačního indexu, protože ten je rozdílem maximální a minimální frekvence. Pokud tedy máme systém implementující 2-FSK modulaci a rozptyl je nastaven na hodnotu 20 kHz,



Obrázek 2.2: Ukázka průběhu nosné vlny (a) modulačního signálu (b) a modulovaného signálu (c), který je výsledkem frekvenční modulace.

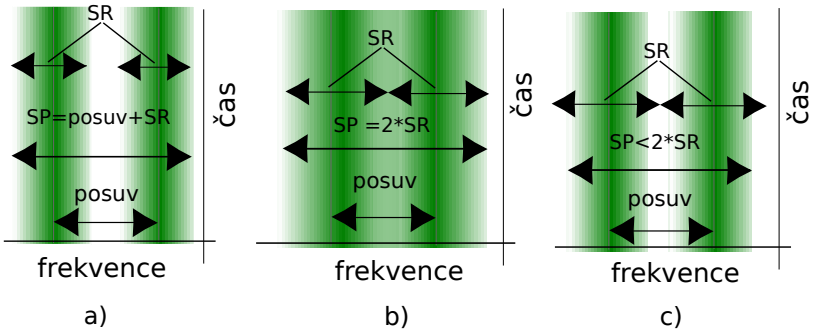
je jeden symbol reprezentován frekvencí nosné vlny sníženou o 20 kHz a druhý symbol reprezentován frekvencí nosné vlny zvýšenou o 20 kHz.

Vysoká přenosová rychlost rychlost může i případě FSK ovlivnit její funkčnost, pokud bude nastaven malý rozptyl (modulační index). Přechody v modulačním signálů mohou rozšířit okupované spektrum FSK tolik, že se mohou obě frekvence (2-FSK) budou navzájem rušit. Obrázek 2.3a) zobrazuje spektrum v čase signálu modulovaného metodou FSK s dostatečným rozptylem, kdy se frekvence neruší. Při zvýšení přenosové rychlosti dojde vlivem rychlých přechodů modulačního signálu k rozšíření okupovaného spektra, viz 2.3b), kde se hodnota SR (šířka pásma přenosové rychlosti) oproti a) zvětší, stejně tak SP (celková šířka komunikace). Jednou možností je zvýšení rozptylu tak, aby se frekvence vzájemně nerušili, ale tím se zabere ještě větší spektrum potřebné pro komunikaci. Druhým inteligentnějším řešením je použití gaussovského filtru na modulační signál, který zakřiví jeho hrany. Výsledkem bude nižší energie přechodů, které tím nebudou rozšiřovat šířku pásma nosných vln. Lze tak při stejné přenosové rychlosti za použití filtru zabrat menší pásmo, než bez filtru. Takovému rozšíření se říká gaussovské klíčování frekvenčním posunem (GFSK). Obrázek 2.3c) zobrazuje spektrum v čase pro signál modulovaný metodou GFSK. Všimněme si, že u c) je šířka pásma přenosové rychlosti SR stejně velká jako u b), ale celková šířka zabraného pásma pro komunikace SP je oproti b) menší. Metoda GFSK nám pomáhá efektivně využít přidělené spektrum.

2.2.3 Fázová modulace

U tohoto typu modulace mění modulační signál fází nosné vlny. Protože patří společně s frekvenční modulací k modulacím, které mění úhel nosné vlny, může se zdát že se jedná o stejný typ modulace. Uvažujme nosnou vlnu $c(t)$ o úhlové frekvenci Ω a amplitudou A a fází ϕ, která je ve fázové modulace funkcí času:

$$c(t) = A\sin(\Omega t + \phi),$$



Obrázek 2.3: Ukázka spektra v čase pro modulaci FSK s malou přenosovou rychlostí (a), modulaci FSK s velkou přenosovou rychlostí (b), modulaci GFSK s velkou přenosovou rychlostí (c).

dále modulační signál *m(t)* o úhlové frekvenci ω a amplitudou M:

$$m(t) = M \sin(\omega t).$$

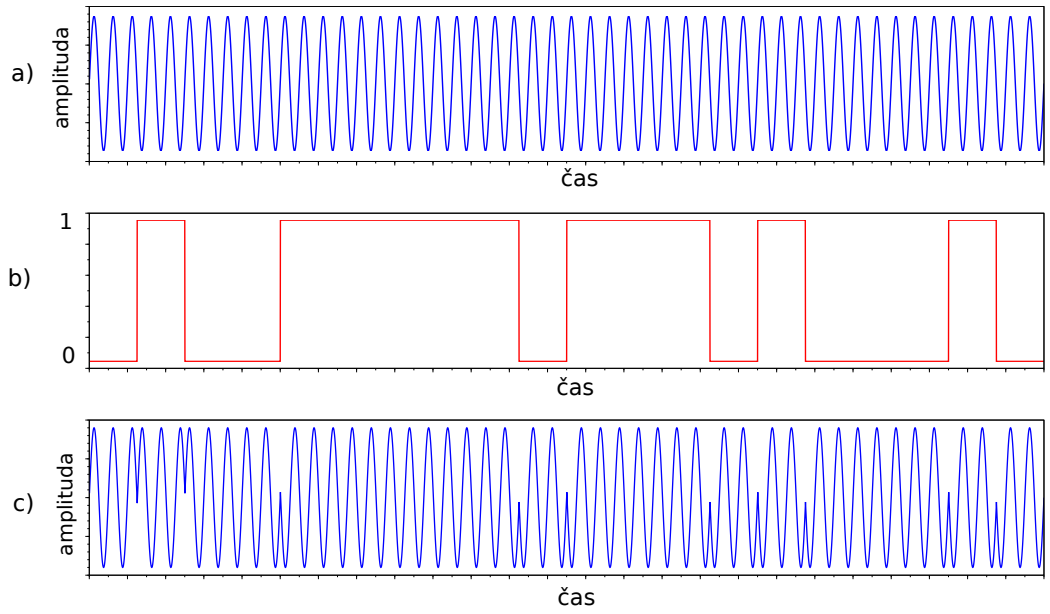
Dosažením modulačního signálu *m(t)* za fází ϕ ve vzorci nosné vlny, získáme tvar rovnice fázové modulace:

$$s_{PM}(t) = A \sin(\Omega + m(t)).$$

Pokud bychom nahradili signál *m(t)* za posloupnost diskrétních hodnot -1,1, které odpovídají logickým hodnotám 0,1, získáme digitální podobu fázové modulace nazývané jako klíčování fázovým posuvem (PSK z anglického *phase shift keying*). Výhoda digitální fázové modulace je přítomnost pouze jedné nosné vlny, takže modulace nezabírá příliš velký frekvenční rozsah a odstraňuje problémy ASK, kde byl výskyt logické 0 reprezentován jako vysílací klid. Obrázek 2.4 zobrazuje princip fázové modulace.

Z obrázku 2.4 je patrná změna fáze modulovaného signálu o 180° na hranách změn modulačního signálu. Fáze -180° odpovídá logické hodnotě 0, změna +180° odpovídá logické hodnotě 1.

Fázová modulace se velice často používá ve spojení s amplitudovou modulací v digitálním přenosu využívající vícesymbolovou techniku, např. televizní vysílání. Naopak v analogové podobě se téměř vůbec nevyskytuje, protože při ní dochází k pomalé změně fáze, což připomíná frekvenční modulaci.

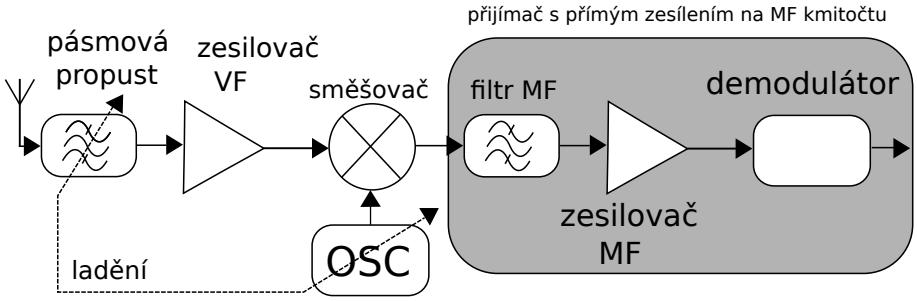


Obrázek 2.4: Ukázka průběhu nosné vlny (a) modulačního signálu (b) a modulovaného signálu (c), který je výsledkem fázové modulace.

Kapitola 3

Rádiový přijímač

Koncept konvenčního rádiového přijímače tak, jak jej známe z přijmu rozhlasových vln je zobrazen na obrázku 3.1. Jedná se o tzv. superheterodyn, jehož základním prvkem je směšovač, který převádí zachycený vysokofrekvenční signál do mezifrekvenčního kmitočtu, který je jednotný pro všechny laditelné vysokofrekvenční kmitočty. Bloky následované za směšovačem jsou pak pevně nastaveny a pracují vždy se stejnou frekvencí - mezním kmitočtem. Takové řešení je ovšem jednoúčelové, protože demodulátor nelze měnit jednoduše tak, aby bylo možné zpracovávat signál s jinými komunikačními parametry.



Obrázek 3.1: Blokové schéma superheterodynu.

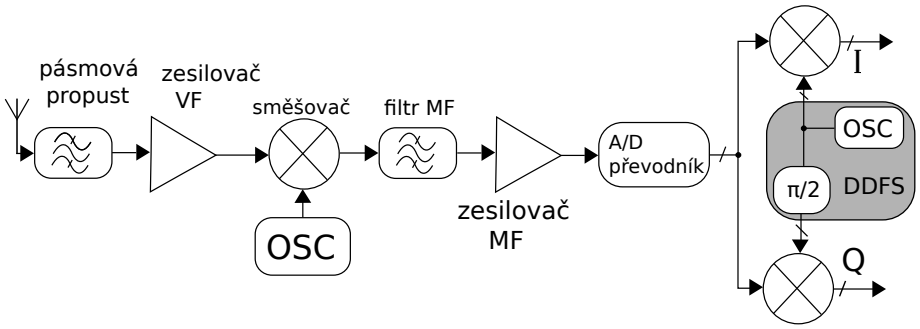
3.1 Přijímač na bázi softwarově definovaného rádia

Obecný koncept softwarově definovaného rádia je dosažen přímým spojením antény s A/D převodníkem (v případě vysílače navíc s D/A převodníkem) a tím tak umožňuje okamžité číslicové zpracování na vysokofrekvenčním kmitočtu. Tento koncept je však zejména kvůli nedostatečnému vzorkovacímu rozsahu A/D (D/A) převodníku nerealizovatelný a z tohoto důvodu bude dále v textu softwarově definovaným rádiem myšlena modifikace konvenčního rádiové přijímače.

Realizace přijímače typu SDR je dosažena záměnou bloků ve schématu 3.1 za bloky, které rozdělí schéma na analogovou a digitální část. Vždy je součástí SDR analogově digitální převodník, který toto rozdělení vytváří. Digitalizovanou část lze zpracovávat procesorem a pouhou změnou jeho softwaru lze rádio parametrizovat tak, aby podporoval různé druhy komunikačních protokolů nebo komunikačních parametrů. Typů softwarově definovaných rádií je mnoho, ale představen bude pouze jeden z nich, který byl také použit

jako hardwarová část k bakalářské práci. Různá schémata softwarově definovaného rádia je možno nalézt např. v [6].

Jedná se o tzv. přijímač s číslicovým zpracováním na mezním kmitočtu, který má dobrý poměr operací v digitální i analogové části. Porovnáme-li blokové schéma uvedené na obrázku 3.2 zjistíme, že obsahuje bloky, které jsme již viděli ve schématu superheterodynu popsaného výše, avšak demodulátor je nahrazen analogově digitálním převodníkem a dvojicí násobiček.



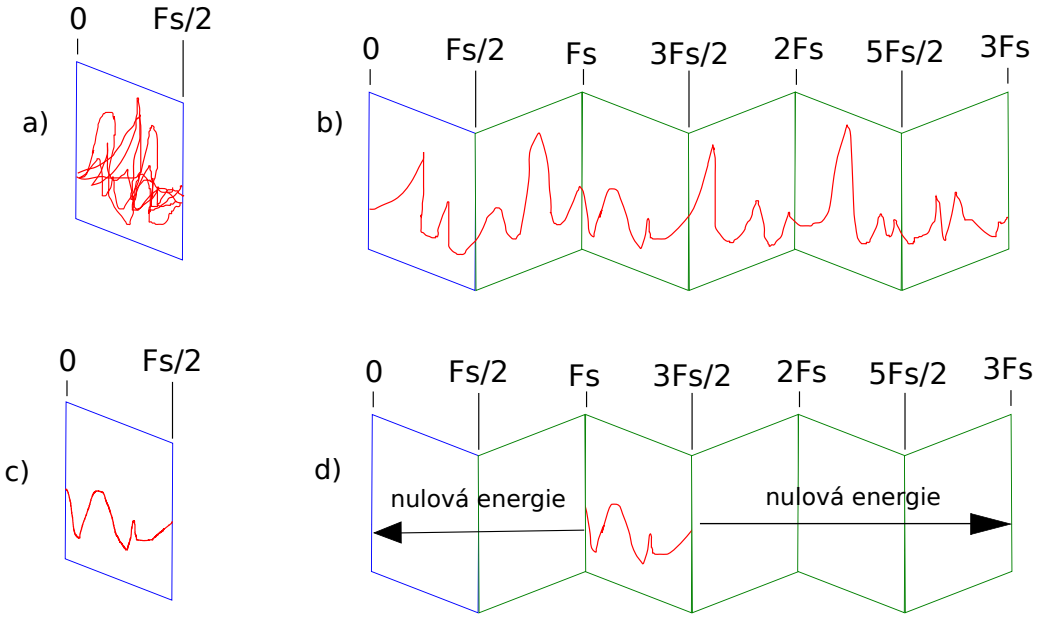
Obrázek 3.2: Blokové schéma přijímače s číslicovým zpracováním na mezním kmitočtu.

Jádro tvoří programovatelný oscilátor společně se směšovačem. V dnešní době existují jednočipové oscilátory, kterou jsou schopny poskytnout poměrně přesný signál napříč spektrem (desítky MHz až jednotky GHz). Bloky v analogové části (před vstupem do A/D převodníku) jsou většinou digitálně laditelné, takže výsledné zařízení nemá žádné mechanické prvky a ladění, stejně jako definice komunikace, komunikačních parametrů atd., probíhá také v softwaru. Účelem kvadraturního syntezátoru typu DDFS je převádět signál do základního pásma. Výstup ve formě posloupnosti I/Q dat je typicky přenášen do softwaru bežící na PC, který již zajišťuje další dekódování. Pomocí tohoto konceptu lze např. přijímat běžné radiostanice pracující v pásmu kolem 100 MHz nebo dokonce dekódovat přenos bezdrátové komunikace pomocí WiFi. Záleží pouze na šířce přenosového kanálu a výkonnosti použitého hardwaru (PC). I/Q data, nazývaná také jako kvadraturní signál, budou podrobně popsána v kapitole 3.2.1.

3.2 Spektrum a signál

Jak již bylo naznačeno dříve, obecný koncept SDR nelze prakticky realizovat. Hlavním důvodem je malá vzorkovací frekvence A/D (D/A) převodníku, který dosahuje na extrémních obvodech maximálně několika stovek Msps (milion vzorků za sekundu, z anglického *million samples per second*). Zaměříme-li se blíže na vlastnosti Shannonova (Nyquistova, Kotělnikova) teorému, lze si spektrum[1] graficky znázornit, jako plochu s ohyby na celých násobcích poloviny vzorkovací frekvence, které připomíná leporelo viz obrázek 3.3b) [3]. Jednotlivé plochy se často nazývají okna. Pokud bychom vstupní signál neupravili patřičnými bloky (viz obrázek 3.2 především blok pásmová propust) vypadal by náhled na výsledné spektrum tak, jako bychom leporelo složili a dívali se na celé spektrum přes 1. okno, viz obrázek 3.3a). Nulová energie v nezkoumaných oknech je nutným předpokladem pro správnou demodulaci signálu. Obrázek 3.3d) zobrazuje spektrum přijatého signálu po potlačení frekvencí mimo frekvenční rozsah A/D převodníku a jeho výsledná projekce do 1.okna je na obrázku 3.3c).

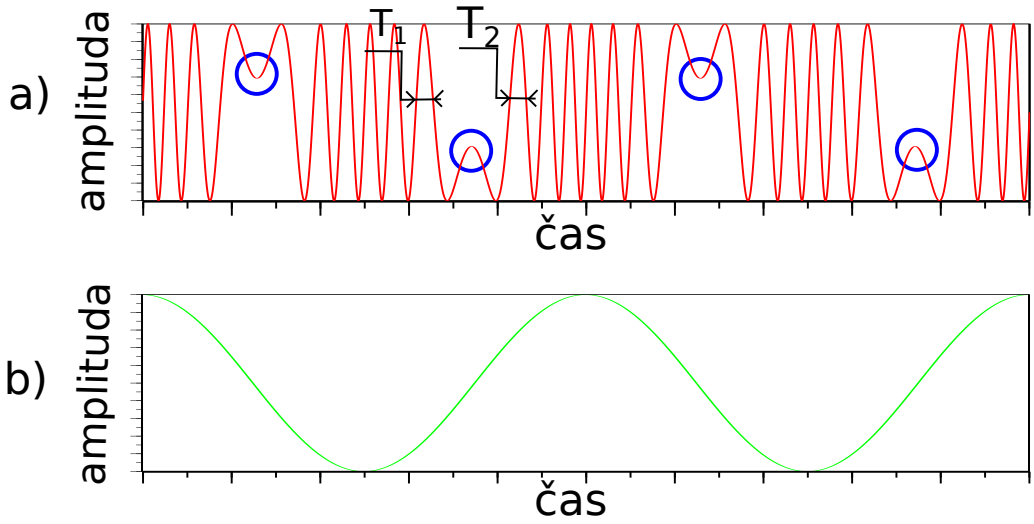
[1] Jako spektrum je v této práci myšlena rádiová část elektromagnetického záření.



Obrázek 3.3: Spektrum a jeho projekce do 1.okna.

V kapitole 2.2 a jejich podkapitolách jsem naznačil podobu signálu ve které opouští vysílací zařízení. Na straně přijímače je přesná podoba signálu dána tím na jakou nosnou vlnu se přijímač naladí. Uvažujme hodnotu frekvence nosné vlny někde v 3. okně (interval od F_S do $\frac{3F_S}{2}$). Pokud se útlum na frekvencích mimo zkoumané okno provede dle předpokladů, objeví se na výstupu signál frekvenčně posunut relativně k frekvenci oscilátoru. To znamená, že pokud při nosné vlně modulovaného signálu o frekvenci f_s=434.1 MHz naladíme oscilátor přijímače na hodnotu f_p=434 MHz, projeví se tento frekvenční rozdíl změnou nosné frekvence modulovaného signálu na hodnotu 100 kHz. Tato konverze ovšem není způsobena směšovačem, jak by se mohlo zdát, ale soustavou složenou bloku DDFS a dvojicí násobiček, která pracuje na mezifrekvenčním kmitočtu. Zajímavá je situace ASK modulace, kdy v případě přesného naladění přijímače na frekvenci nosné vlny $f_s = f_p$ dostaneme rovnou modulační signál navzorkovaný vzorkovací frekvencí A/D převodníku. Problém ovšem naopak nastává u FSK, kde se frekvence nosné vlny mění podle modulačního signálu a není tak možné nastavit přesně frekvenci oscilátoru na frekvenci signálu. Mohlo by se zdát zvolit jako dobrý kompromis hodnotu oscilátoru f_p přesně na frekvenci $f_p = f_s = \Omega$ ze vztahu popisující frekvenční modulaci v kapitole 2.2.2. Jen pro zopakování se při frekvenční modulaci pohybuje frekvence signálu od $\Omega - M_{fm}$ do $\Omega + M_{fm}$. Za předpokladu, že frekvence nosné vlny a frekvence oscilátoru jsou si rovny $f_s = f_p$, bude mít modulovaný signál frekvenci v rozsahu $-M_{fm}$ do $+M_{fm}$, což na reálném signálu není dost dobře rozlišitelné, protože perioda T je totožná pro $-M_{fm}$ jako pro $+M_{fm}$ čímž $f_{-M_{fm}} = f_{+M_{fm}} = \frac{1}{T}$.

Obrázek 3.4 graficky zobrazuje problémy reálného signálu, pokud bude souhlasná frekvence nosné vlny s frekvencí oscilátoru rádia. Červeně je znázorněn modulovaný signál, zeleně modulační signál. V modrých kroužcích dochází ke změně frekvence frekvenční modulace z kladného do záporného spektra, avšak perioda T1 a T2 jsou stejné a nelze zjistit zda se jedná o kladnou či zápornou frekvenci.



Obrázek 3.4: Reálný signál modulovaná frekvenční modulací (a) a modulační signál (b). T_1 a T_2 jsou stejně dlouhé.

3.2.1 Kvadraturní signál

Aby bylo možné bezpečně rozlišit záporné a kladné frekvence signálu, upraví se signál do podoby kvadraturního signálu (anglicky *quadrature signal*). Kvadraturní signál, který má základ v komplexních číslech je tvořen párem periodických signálů se vzájemně posunutou fází o 90°. Komplexní číslo (j značí imaginární složku):

$$z = a + jb,$$

si lze představit jako vektor začínající v počátku komplexní roviny a končící v souřadnicích dané komplexním číslem *[a,b]*. Uvažujme velikost vektoru r a fázor ϕ o úhlu sevřeným s reálnou osou komplexní roviny, pak vztah mezi a,b,r,ϕ je dle [12]:

$$a = r\cos\phi, b = r\sin\phi, r = \sqrt{a^2 + b^2}, \phi = \arctan\frac{b}{a}.$$

Komplexní číslo lze tedy zapsat také jako:

$$z = r\cos\phi + jr\sin\phi.$$

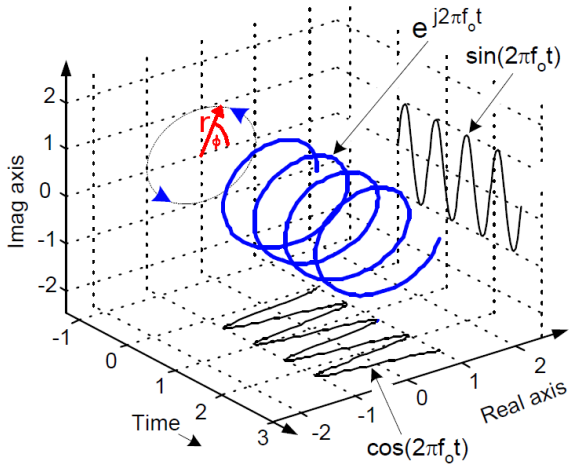
Veškeré symboly a vztahy komplexního čísla v čase jsou na obrázku 3.3, kde $r\cos\phi + jr\sin\phi = re^{j\phi}$ a tedy $z(t) = re^{j\phi t}$.[2]

Protože jsou funkce *sin, cos* vzájemně fázově posunuté o 90°, lze si složky komplexního čísla vyjádřit ve tvaru:

$$I = r\cos\phi, Q = r\sin\phi,$$

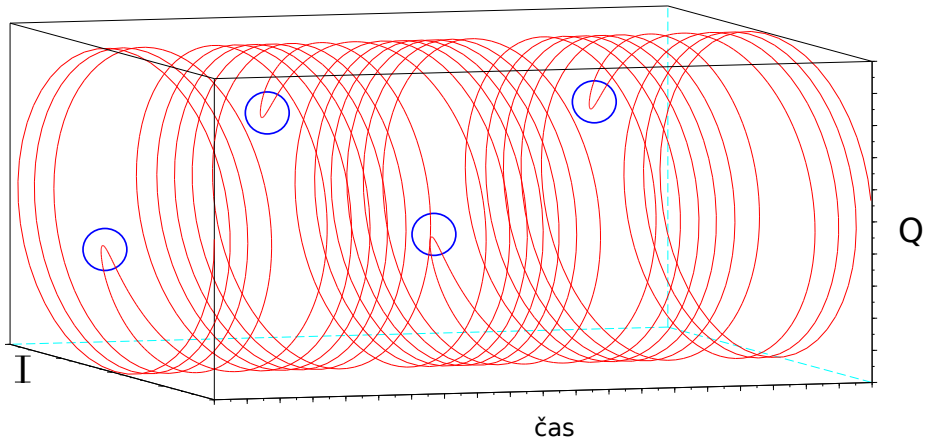
kde I značí synfázní (anglicky *in-phase*) složku a Q kvadraturní (anglicky *quadrature-phase*) složku, kvadraturního signálu. Výhoda signálu složeného z komplexních čísel (komplexní signál) oproti signálu složenému z reálných čísel (reálný signál) je absence záporných frekvencí v komplexním signálu. U komplexního signálu lze totiž rozlišit zda se každá z jeho frekvencí nachází v záporném nebo kladném spektru. Na rozdíl u reálného signálu, kde

[2]Obrázek byl převzat z [5] a doplněn o vektor s velikostí r a fází ϕ.



Obrázek 3.5: Komplexní exponenciála.

$-f = f$ tzn. kladné frekvence se rovnají těm záporným. Dle [11] lze každý modulovaný signál rozložit na složky kvadraturního signálu a tak se použití kvadraturních signálů jeví jako výhodné. Další výhodou analýzy komplexního signálu opět vychází z podstaty rozlišení záporných a kladných frekvencí a to rozšířením šířky spektra po navzorkování analogově digitálním převodníkem, kde měli okna (viz obrázek 3.3) původně šířku polovinu vzorkovací frekvence $(0; f_s/2)$, tentokrát bude šířka, díky rozlišení záporných frekvencí, dvojnásobná $(-f_s/2; f_s/2)$. Lze tak analyzovat širší spektrum současně.



Obrázek 3.6: Komplexní signál.

Problematika je znázorněna na obrázku 3.6, kde je opět v modrých kruzích vyznačena změna frekvence, která již rozlišitelná je. Fázor, který znázorňuje změnu frekvence, se ve vrcholu modrého kruhu začne točit opačně, což indikuje přechod do záporného/kladného frekvenčního spektra.

Kapitola 4

Navržené řešení

Nezbytnou komponentou pro dosažení cíle bakalářské práce je hardwarové zařízení, které dokáže bezdrátový signál zachytit a digitalizovat. Z pohledu hardwaru tedy přichází v úvahu mnoho řešení softwarově definovaného rádia [6]. Pokud je k dispozici blokové schéma přijímače a jsou známy jeho výhody a nevýhody, lze si jej postavit ze součástek dostupných na internetu. Často se jedná o relativně hustě integrované obvody, které nevyžadují příliš součástek okolo. Z prvotních návrhů připadaly v úvahu dvě různá řešení pokaždé jako kombinace dvou větších integrovaných obvodů s malým množstvím externích součástek. Koncept jednoho z řešení navíc uvažoval i možnost vysílání a potřeboval další menší integrované obvody navíc. Bohužel každé z řešení bylo zatíženo finanční náročností okolo 2000 Kč za integrované obvody a nutné součástky okolo. K tomu by se ještě musely připočíst náklady na výrobu a nejspíše také návrh desky plošných spojů externí firmou, protože realizace by vyžadovala znalost návrhu vysokofrekvenčních zařízení, umístění prokovů, použití SMD součástek v pouzdře 0402, atd., což by celkovou realizaci hardwaru prodražilo možná i několikanásobně.

Při digitální komunikaci, dochází ke skokovým změnám, které se detekují lépe než změny analogové modulace (modulačním signálem je nejčastěji akustický signál). Z tohoto důvodu nemusí být signál převeden bloky DDFS a dvojice násobiček přímo do základního pásma, který je jinak pro analogový signál důležitý. Protože ale tyto bloky k dispozici na použitém hardwaru jsou, ladí se v aplikaci přijímač automaticky na nejnižší frekvenci špičky sníženou o 20 kHz. Vytvoří se tak vlastně podmínky pro analýzu signálu na kmitočtu s nejnižší hodnotou 20 kHz. Nejedná se přesně o mezifrekvenční kmitočet, protože ten se udává jako $f_{mf} = |f_{vf} - f_{osc}|$, tedy odečtení frekvence oscilátoru přijímače od nosné frekvence. Výhoda tohoto postupu je zajištění absence záporných frekvencí a možnost analyzovat signál z amplitudy reálného signálu. Výhody kvadraturního signálu se tedy využijí pouze ve Fourierově transformaci při zkoumání spektra.

4.1 Hardware

Vzhledem k tomu že předmětem bakalářské práce byl návrh software nikoliv stavba hardwarového přijímače, kterých je na trhu nepřeberné množství, vydali jsme se cestou použití laciného řešení na bázi softwarově definovaného rádia. Jedná se o přijímač osazený vysokofrekvenčním tunerem Rafael Micro R820T převádějící přijatý signál do mezifrekvenčního kmitočtu, integrovaný obvod Realtek RTL2832U, které obsahují veškerou funkcionalitu pro dekódování televizního digitálního vysílaní. Výhodou tohoto řešení je možnost uvést obvod

do stavu, kdy jsou k dispozici přímo kvadraturní data. Poprvé tuto možnost popsal finský vývojář kernelu V4L/DVB Antti Palosaari s dostupností pro platformy Microsoft Windows a Linux. Tento přijímač má však také svou nevýhodu, vzhledem k cíli snížit náklady na výrobu, je postaven na poměrně nekvalitním oscilátoru, který způsobuje odchylku v případě, detekce frekvence nosné vlny. To je patrné např. při zahřátí přijímače, kdy se frekvence může posunout až o kolik jednotek kHz. Dodejme, že nekvalitní oscilátor nemá vliv na příjem televizního ani rozhlasového vysílání, neboť se v těchto případech používá automatický tracking frekvence nosné. Vadí nám to však v případě, kdy parametry neznáme a chceme určit jakou frekvenci nosné má určitý signál. Jedna možnost je určit výsledek s chybou +- %, druhá možnost je využít nějakého referenčního vysílače, a přijímač zkalibrovat. Základní parametry použitého přijímače jsou: frekvenční rozsah tuneru je 25 - 1750 MHz, maximální vzorkovací frekvence analogově digitálního převodníku (po decimaci) je 3.2 Msps s rozlišením 8 bitů. Se zvoleným přijímačem tedy není možné především kvůli frekvenční šířce 868 MHz pásma, ale také kvůli velké frekvenční mezeře mezi 434 a 868 MHz analyzovat obě frekvenční pásma najednou. K jednokrokové analýze by byl potřeba analogově digitální převodník se vzorkovací frekvencí minimálně 868 - 433.05 = 434.95 Msps.

4.2 Software

Uživatelská aplikace, jako softwarová část bakalářské práce, je napsána ve vývojovém prostředí QtCreator v jazyce C++. Uživatelská aplikace pro analýzu a dekódování bezdrátové komunikace zpracovává signál má tři režimy činnosti:

- 1. stav - zjišťování bezdrátových komunikací ze spektra,
- 2. stav - analýza parametrů komunikace konkrétní bezdrátové komunikace,
- 3. stav - dekódování signálu pomocí zjištěných parametrů.

Mezi jednotlivými stavy se lze kdykoliv, pokud to dává smysl, přepnout. Samozřejmě není možné například začít dekódovat bezdrátovou komunikaci, aniž by byly zjištěny její parametry.

Už bylo řečeno, že bezdrátová komunikace probíhá v bezlicenčních frekvenčních pásmech 434 a 868 MHz, kde šířka prvního pásma je 1.74 MHz (433.05 - 434.79 MHz) a druhého 7 MHz (863 - 870 MHz). V případě použití převodníku s nižší vzorkovací frekvencí, je zapotřebí frekvenční pásma rozdělit na přibližně stejné části a v aplikaci přepínat mezi těmito částmi.

V případě bezlicenčního pásma 434 MHz není nutné provádět přelaďování, neboť lze celé pásmo analyzovat současně. Analýza vyššího spektra pak probíhá ve $7/3.2 = 2.1875 \doteq 3$ krocích. Pokud je pásmo rozděleno do jednoho kroku, naladí se přijímač na frekvenci rovnou polovině šířky tohoto frekvenčního pásma. V případě vícekrokové analýzy, se centrální kmitočet přijímače naladí na polovinu vzorkovací frekvence, jako by byla o 10% nižší. Dochází tak k překryvům oken spektra o 5% vzorkovací frekvence z každé strany, takže nemůže dojít ke ztrátě některé komunikace, která by komunikovala na hraně spektrálních oken.

Vzhledem k tomu, že analýza v prvním režimu probíhá ve frekvenční oblasti, je nutné z I/Q dat, upravené jednoduchou implementací dolní propusti, získat obraz ve frekvenční doméně. Ten se získá pomocí diskrétní Fourierovy transformace implementovanou knihovnou FFTW [13]. FFTW je implementována v jazyce C a dle experimentů dosahuje velmi

dobrých výsledků v porovnání s běžně na internetu dostupnými implementacemi rychlé Fourierovy transformace při zpětné i dopředné transformaci.

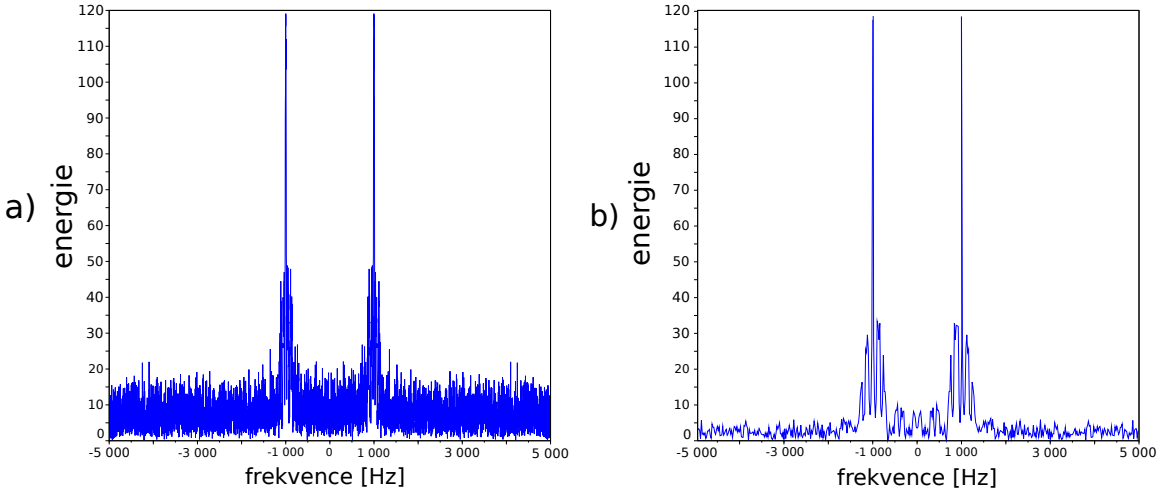
Vstupem DFT je signál, jehož spektrum má být analyzováno. Je zřejmé, že vstupní signál je nutné zpracovat po blocích, otázka však je, kolik vzorků zvolit. Budeme-li používat dlouhé okno a v něm časově velmi krátkou komunikaci. Fourierova transformace způsobí, že se energie šumu, ač s velmi malou amplitudou, kumuluje do hodnoty blízké energii užitečné komunikace. Kvůli tomu, že komunikace bezdrátových zařízení může probíhat v krátkých časových slotech a s modulaci ASK, kde se logická 0 rovná nulové amplitudě signálu, musí se zvolit spíše menší okno. Naopak velmi krátké okno by způsobilo jen zbytečnou režii v podobě neustálého přeladďování frekvence oscilátoru, při hledání bezdrátových komunikací. Osvědčilo se okno o velikosti 32768 (s ohledem na FFTW, které je založeno na faktorizaci N). Obrázek 4.1 zobrazuje vlevo spektrum s větší velikostí okna transformace a vpravo s 10x menší velikostí okna transformace. Všimněme si především energie signálu (maxima špiček), které jsou v obou případech přibližně stejné. To je důsledkem stejně dlouhé (500 vzorků) datové komunikace. Energie šumu, je však v levém spektru větší, protože obsahuje 10x delší šum. Často se v rádiové technice používá poměr signál-šum, což značí poměr mezi maximální energií šumu a maximální energií signálu. Spektrum vlevo by mělo špatný (malý) poměr signál-šum, spektrum vpravo dobrý (velký) poměr signál-šum. Vysokofrekvenční tuner je na vstupu vybaven vysokofrekvenčním zesilovačem s automatickým zesílením, takže se nastavuje zesílení podle toho jakou energii má signál. V praxi by to znamenalo, že bude mít levé spektrum ještě horší poměr signál-šum a spektrum vpravo ještě lepší poměr signál-šum. Signál použitý v ukázce byl modulován modulací ASK. Při správném nastavení okna transformace lze přítomnost komunikace zjistit překročením zvolené hraniční meze ve spektru rozlišující užitečný signál od šumu. Tato mez je v aplikaci nastavitelná, aby bylo možné potlačit komunikace, které mají malou energii, ovšem nejsou šumem a také nejsou zkoumanou komunikací. Problém nastává v případě, kdy chceme v reálném prostředí [1] analyzovat komunikaci, která má nižší energii, než jiný komunikační systém, která nám analýzu ruší. Podstata softwarově definovaného rádia totiž spočívá v příjmu jakékoliv komunikace a tak není možné nepotřebnou komunikaci s vyšší energií nijak odstranit.

Obrázek 4.1 ukazuje, dvě spektrální špičky. Jedna kolem frekvence 1000 Hz a druhá kolem -1000 Hz. Na první pohled by se mohlo zdát, že se jedná o 2-FSK modulaci s rozptylem 1000 Hz. Nicméně toto není náš případ, neboť jak bylo uvedeno, signál byl modulován pomocí ASK. K tomuto artefaktu došlo z důvodu nerozlišitelnosti kladné/záporné frekvence reálného signálu.

Dá se předpokládat, že špička ve spektru značí bezdrátovou komunikaci. Pokud se ve spektru taková špička objeví, uloží se do seznamu, který si uchovává potenciální nosné frekvence. Už jednou známé signály se znovu neukládají, přičemž je pro každý signál nastavena tolerance 50 kHz, tzn. pro komunikaci s nosnou vlnou o frekvenci 434.05 MHz se považuje za stejnou komunikaci jako kdyby byla na frekvenci 434.1 MHz. Tato tolerance zajišťuje eliminaci chyb způsobené chybou ve Fourierově transformaci při její opakované exekuci a také chyby hardwaru, které byly detekovány při testování (omezená přesnost a variabilita oscilátoru vlivem změny teploty). Frekvenční tolerance také pomáhá sdružovat špičky jedné komunikace s frekvenční modulací 2-FSK, 4-FSK, která se ve spektru projevuje jako několik špiček okolo nosné. Poté co uživatel vybere frekvenci, může přepnout aplikaci do stavu 2 a začne analýza parametrů vybrané komunikace.

Uživatelské rozhraní aplikace zobrazuje obrázek B.3.

[1] Obecně mnoho různých komunikačních systému, na různých nosných vlnách o různých energií a parametrů.



Obrázek 4.1: Vlevo spektrum signálu s velikostí velikosti okna N=5000. Vpravo spektrum s velikostí okna N=500.

4.2.1 Automatické detekce komunikačních parametrů

Druhý režim pracuje následovně. Nejprve je přijímač přeladěn na frekvenci vybrané ze seznamu potenciálních nosných frekvencí. Výstup je opět analyzován pomocí FFT a aplikace čeká, až se objeví komunikace na stanovené frekvenci. V případě, že se objeví komunikace na vybrané nosné frekvenci nebo její tolerované hodnotě, je informace o frekvenci nosné spolu s vypočítanou symbolovou rychlostí předána třídě, která zajišťuje výpočet statistických informací.

Změna znaménka fáze frekvenční modulace nemůže nastat, protože analýza signálu pracuje vždy se signálem s kladnou frekvencí o minimální frekvenci 20 kHz a tak má modulovaný signál připravený k analýze podobu signálu, představené v kapitole 2.2.

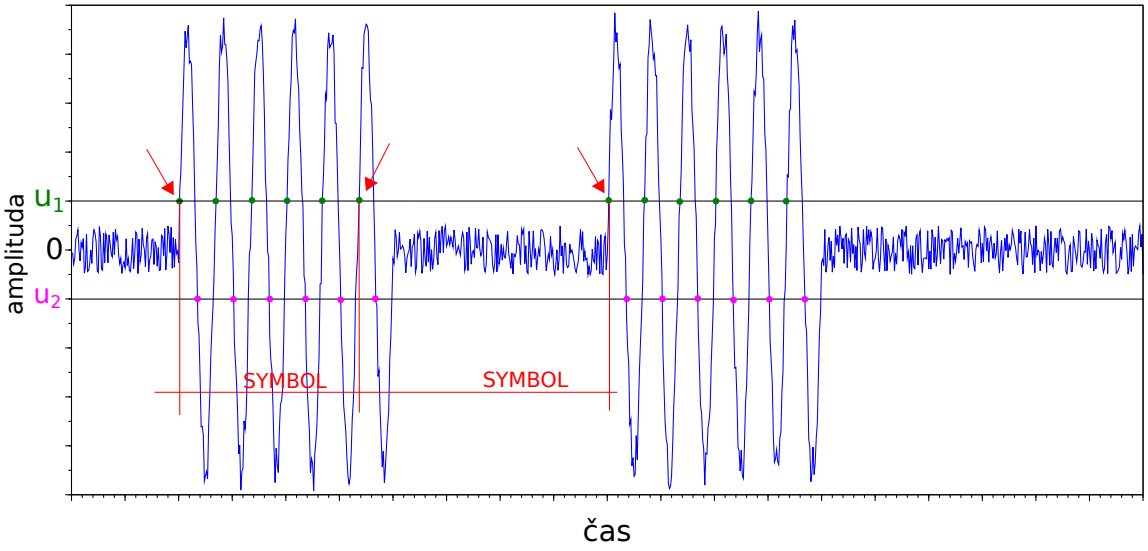
Stanovení symbolové rychlosti

Existuje řada metod, jak stanovit symbolovou rychlost. Většina využívá autokorelace pracující buď s modulačním signálem nebo s jeho spektrální částí [8, 9, 7]. Naproti tomu však existují i metody, které pracují pouze se spektrem [1, 10] nebo jsou specializovány na určitý typ modulace [2]. Bohužel všechny z nich uvažují nasazení v moderních systémech s vícesymbolovou technikou fázové nebo amplitudově-fázové modulace a vysokými přenosovými rychlostmi. Navíc systémy jsou většinou navrženy pro hardware například jako modul k DVB-T tuneru, nebo je nutná alespoň částečná znalost parametrů komunikace (např.: v podobě výběru standardizovaných přenosových rychlostí,...). Systémy ale často disponují vysokým procentem úspěšnosti detekce symbolové rychlosti při dobrém poměru signál-šum. Metody založené na autokorelaci jsou navíc i odolné proti horšímu poměru signál-šum. Nutnost podpory základních metod modulací (ASK,FSK) je od těchto algoritmů upuštěno.

Základní myšlenkou výpočtu symbolové rychlosti je měření periody signálu v průběhu symbolu a záznam dob, kdy dojde ke změně délky doby periody, které indikují změnu symbolu. Vlivem šumu v signálu není při hledání periody, hledanou hodnotou stav, kdy sinusový průběh signálu opakovaně protíná osu x (časovou osu), ale hodnota u_1 odsazena o 10% dvojnásobku maximální amplitudy signálu. Symetricky k tomuto odsazení se pak jako konec periody hledá hodnota u_2 odsazena o -10%. Jelikož perioda signálu označuje

dobu signálu až do doby nastání jeho výchozího stavu, musí proběhnout sled hodnot u_1, u_2 a následně opět u_1, kde rozdíl hodnot u_1 značí periodu. Hodnoty u_2 slouží pouze k rozlišení přechodu signálu přes nulovou mez.

Konec/počátek symbolu je detekován jako změna frekvence modulovaného signálu a to platí jak v amplitudové tak frekvenční modulaci stejně pouze s malým rozdílem. Navíc kvůli nežádoucím artefaktům, pocházejících z neznámých zdrojů, se musí v analyzovaném signálu přistupovat ke změně frekvence, značící změnu symbolu, obezřetněji.

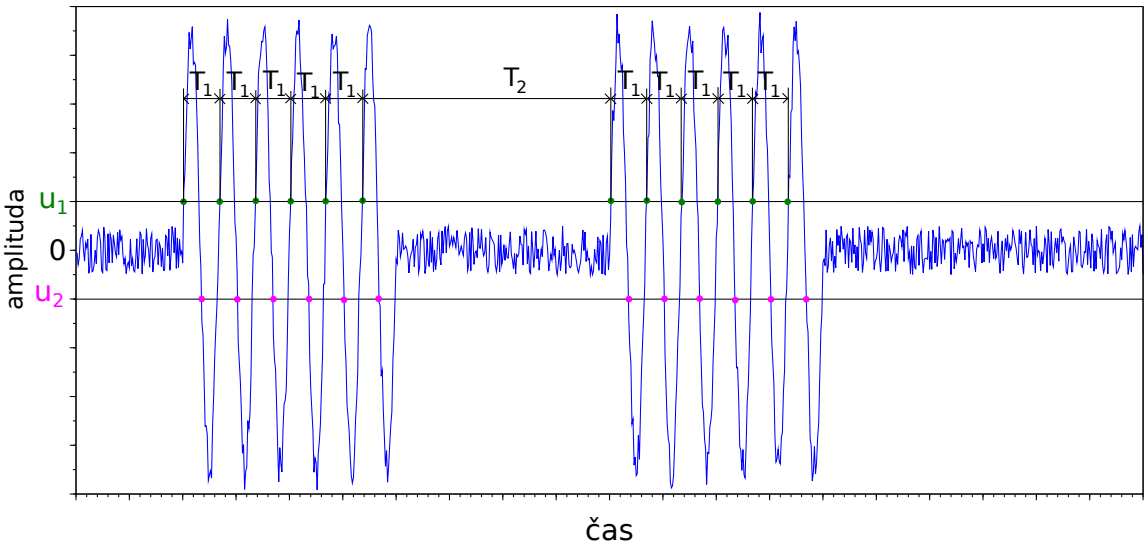


Obrázek 4.2: Princip určení přenosové rychlosti na základě analýzy přijímaného signálu v časové doméně.

Obrázek 4.2 zobrazuje signál modulovaný metodou ASK. Jsou v něm vyznačeny polohy různých kombinací hodnot u_1, u_2. Všimněme si především červených šipek, které aplikace vyhodnotí jako změna symbolu. Z obrázku je také vidět, že detekce symbolů nejsou přesně na patě začátku/konce sinusového průběhu, ale až v místě protnutí hraniční meze. Z tohoto důvodu je logické, že doba symbolu neodpovídá přesně reálné době symbolu. Tato chyba ale nemá markantní podíl na chybné detekci. Zaprvé period je v průběhu symbolu mnohem více než je zobrazeno na obrázku, takže doba mezi patou konce/počátku sinusového průběhu a průnikem signálu hraniční mezí je tedy velmi krátká. Zadruhé symbolová rychlost se počítá jako průměr, a z obrázku je vidět, že zatímco doba prvního symbolu je kratší, doba druhého symbolu je naopak delší. Navíc dle formule amplitudové modulace je nosná vlna modulována modulačním signálem v kterémkoliv okamžiku fáze nosné vlny. V praxi se tak běžně stává, že logická změna dělí sinusový průběh nosné vlny v neznámém místě a tak symbol nemusí končit hodnotou u_2, ale hodnotou u_1. Všechny tyto situace vedou na využití pravděpodobnostního modelu.

Již bylo řečeno, že detekce změny symbolu u signálu modulovaný metodou ASK je změna periody podobná pouze s malou odlišností jako u signálu modulovaný metodou FSK. U metody ASK je to totiž detekce **jediné** dlouhé periody, zatímco u metody FSK je to detekce změny periody a její **následné ustálení**. Detekce period naznačují obrázky 4.3 a 4.4.

Na obrázcích vidíme, že zatímco u metody ASK se při detekci symbolu čeká na jedinou změnu periody (přechod T_1 na T_2 nebo naopak), u metody FSK se čeká na změnu periody

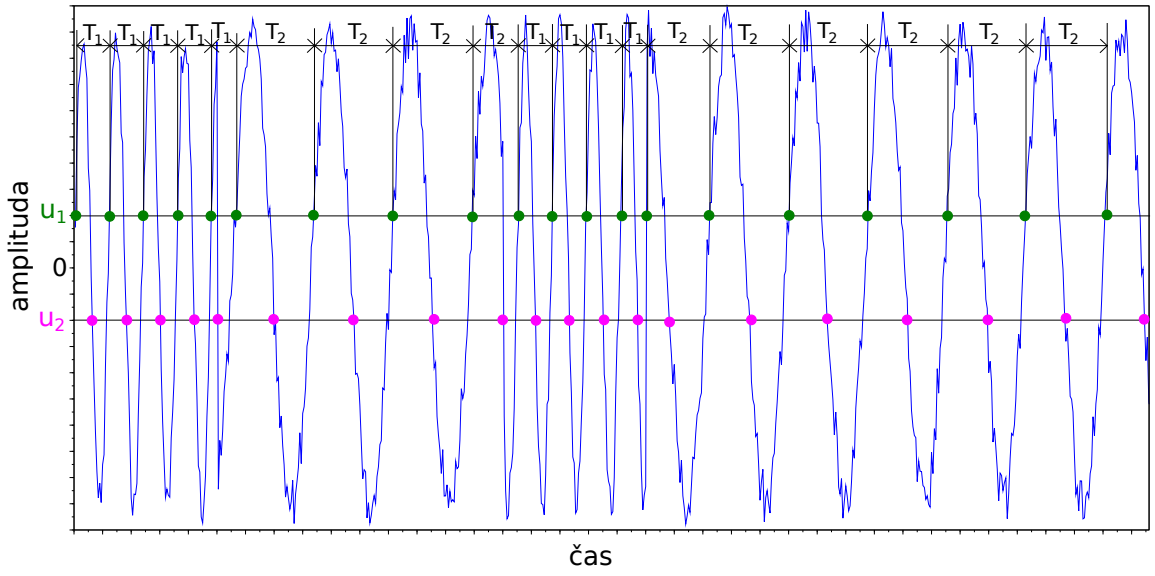


Obrázek 4.3: Ukázka detekcí period v signálu modulovaného metodou ASK.

plus její ustálení (přechod T_1 na T_2 a ustálení T_2 nebo naopak). Důvod proč se u FSK nečeká pouze na změnu periody je možný výskyt artefaktů v signálu, který se projeví osamocenou změnou periody. V souvislosti s výskytem artefaktů v signálu je dobré ještě doplnit, že u metody ASK se čeká na prodlouženou dobu periody T_1, protože perioda artefaktů je vždy mnohem kratší než T_1. Tím je výpočet symbolové rychlosti do jisté míry imunní vůči těmto chybám v signálu. Ovšem výpočet symbolové rychlosti musí být stanoven z doby trvání jednoho jediného symbolu. Pokud bychom stanovili symbolovou rychlost z posloupnosti dvou a více po sobě jdoucích stejných symbolů, nezískali bychom symbolovou rychlost ale její násobky. Vlastností bezdrátových komunikací je vždy přítomnost synchronizačních preambulí (počátků komunikací), které se vyznačují střídáním symbolů jednotkové délky a často také disponuje mechanizmem odesílaní maximálně dvou stejných symbolů po sobě. Teoreticky stačí zachytit synchronizační preambuli, což může posloužit jako dobrý základ pro statistické vyhodnocení symbolové rychlosti. Protože ale není možné v aktuálním režimu synchronizační rámec hledat (stále neznáme symbolovou rychlost) provádí se vyhodnocení symbolové rychlosti nad každým přijatým signálem a spoléhá se na to, že rámec bezdrátové komunikace disponuje větší četností jednotkových symbolů. Rozdílný přístup k stanovené symbolové rychlosti u každého typu modulace zvlášť vyžaduje stanovení typu modulace ještě před určením symbolové rychlosti. V aplikaci je toho dosaženo tak, že se vyhodnocují všechny parametry (frekvence nosné, typ modulace, symbolová rychlost) současně a změna typu modulace provede ve statistické třídě reset symbolové rychlosti.

Stanovení frekvence nosné vlny a modulace

Oproti stanovení symbolové rychlosti není stanovení frekvence nosné vlny bezdrátové komunikace tolik důležitým parametrem pro demodulaci. Stanovení frekvence nosné vlny slouží pouze pro detekci bezdrátové komunikace. Pro stanovení frekvence připadají v úvahu dvě možnosti. První možnost využívá rychlou Fourierovu transformaci a okamžitý výpočet frekvence podle zvolené meze relativně k frekvencí oscilátoru přijímače. Druhá možnost spočívá v zisku periody nosné vlny ze signálu (metodou popsanou výše) a připočtení frekvence této periody k frekvenci oscilátoru přijímače. Protože se Fourierova transformace, kvůli detekci



Obrázek 4.4: Ukázka detekcí period v signálu modulovaného metodou FSK.

energie signálu, provádí nad každou přijatou sekvencí I/Q dat. Byla zvolena první varianta.

Protože vstupem rychlé Fourierovy transformace je diskrétní signál o délce N, je nutné každému bodu přiřadit odpovídající frekvenci, která závisí na vzorkovací frekvenci analogově digitálního převodníku. Ze spektra získané Fourierovou transformací zjistíme špičku a na její polohu aplikujeme jednoduchou transformační funkci, která převádí index na frekvenci:

$$c = i \cdot d_f + f_{osc}, i < N/2,$$

$$c = f_{osc} - d_f \cdot (N - i), i \geq N/2,$$

kde c značí frekvenci nosné vlny, i je poloha špičky v diskrétním spektru, d_f je frekvenční krok, f_{osc} je frekvence oscilátoru přijímače a N je velikost fronty vstupních vzorků. Příklad: ze spektra zjistím špičku komunikace na poloze $i = 1200$. Vím, že f_{osc} jsem nastavil na hodnotu 434 MHz, vzorkovací frekvence A/D převodníku je 3.2 Msps a do rychlé Fourierovy transformace vstupuje 32768 vzorků signálu. Pak $d_f = f_{vz}/N = 3.2 \cdot 10^6/32768 \doteq 98Hz$, $c = 1200 \cdot 98 + 434 \cdot 10^6 = 434.1176$. Frekvence nosné vlny je 434.1176 MHz.

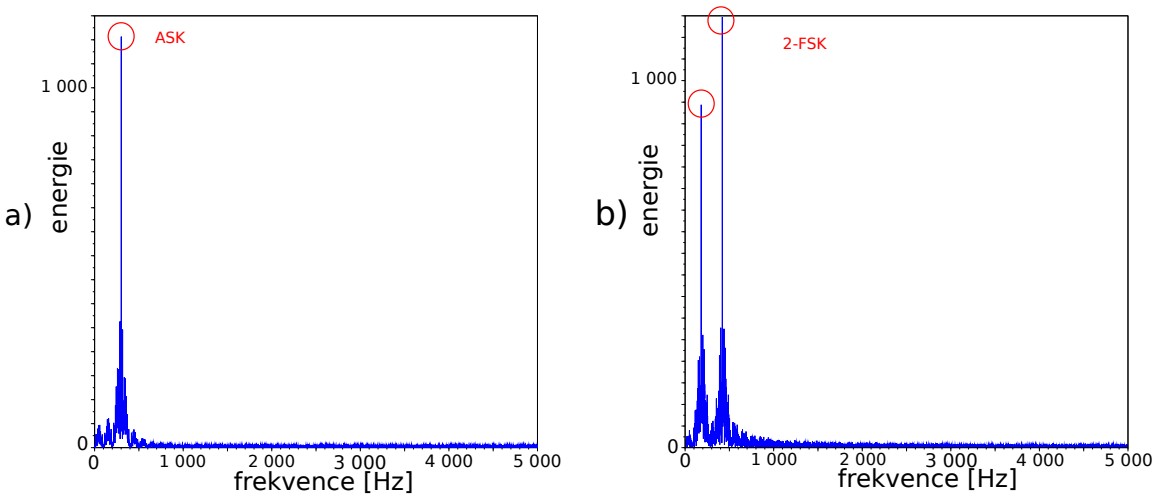
Tento způsob určení frekvence nosné je zatížen dvěma druhy chyb. Jednak se jedná o zaokrouhlovací chyby frekvenčního kroku (98 Hz místo přesné 97.65625 Hz). Zadruhé může při výpočtu Fourierovy transformace dojit k chybné diskretizaci spektra, protože žádná ze sekvencí kvadraturního signálu není stejná, ačkoliv zobrazují stejnou část datové komunikace. Tyto chyby jsou ovšem zanedbatelné, protože se pohybují v řádu stovek Hz.

Získané frekvence nosné vlny jsou ukládány stejně jako symbolová rychlost do struktury `Stats`. U metody ASK je frekvence nosné vlny rovna průměru frekvenčních špiček získaných ze spektra. Metoda FSK je ovšem ve spektru vyjádřena dvěma (2-FSK) nebo čtyřmi (4-FSK) špičkami. Nelze tedy frekvenci nosné vlny vyjádřit jako průměr jedné špičky spektra, ale jako průměr průměrů špiček.

Z pohledu bezdrátových zařízení fungujících v bezlicenčních pásmech 434 Mhz a 868 MHz se nejčastěji setkáváme s čistě amplitudovou nebo s čistě frekvenční modulací v její

digitální podobě. Vyplývá to z potřeb těchto bezdrátových zařízení, které nevyžadují přenášet velké množství bitů za jednotku času. Proto bude uvažována pouze identifikace ASK a FSK modulace.

Pro správný výpočet frekvence nosné vlny komunikačního systému je zapotřebí znát typ modulace. Typ modulace je také důležitým faktorem při dekódování. Frekvence odpovídající špičce signálu detekované napříč spektrem, se ukládají do struktury `Stats` a podle toho kolik špiček struktura obsahuje se rozhodne o typu modulace. Jedna špička značí metodu ASK, dvě špičky metodu 2-FSK a čtyři špičky metoda 4-FSK. Na obrázku 4.5 vlevo je spektrum signálu modulovaný metodou ASK vpravo spektrum metody 2-FSK.



Obrázek 4.5: Spektra bezdrátových komunikací. Vlevo ASK, vpravo 2-FSK.

4.2.2 Datové struktury

Analýza parametrů komunikace probíhá do určité míry statisticky. Pro aplikaci byla proto navržena datová struktura `Stats`, která reflektuje potřeby statistického zpracování dat. Základem struktury je vektor, jehož prvky jsou struktury `Row`. Struktura `Row` obsahuje tři položky a sice:

- *average* - průměrnou hodnotu z ukládaných dat,
- *nextFree* - číslo dalšího prázdného záznamu, nebo také jako počet záznamu ve struktuře,
- *array* - ukazatel na pole statistických hodnot.

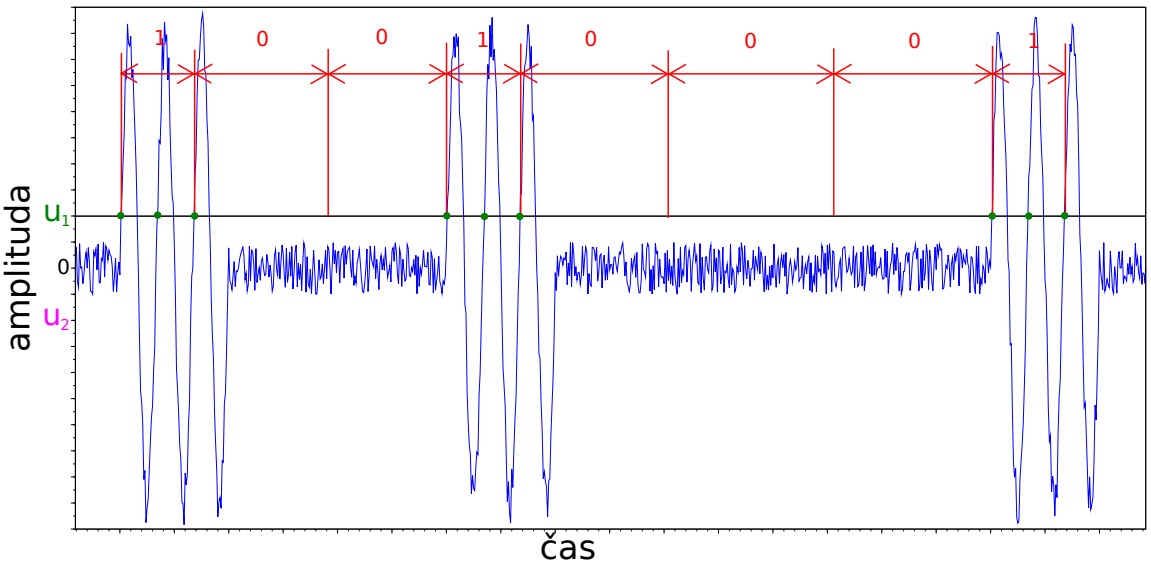
Struktuře `Stats` se při inicializaci nastaví parametry, podle kterých se následně rozhoduje, jak naložit s požadavkem na zápis hodnoty do struktury. Jedním z parametrům je opět tolerance se kterou se skupina hodnot považuje za tutéž. Druhým parametrem je maximální délka pole *array*. Např.: proměnná *symbolRate*, která je typu `Stats`, uchovávající symbolovou rychlost má nastavenou toleranci i délku *array* na hodnotu 100. Pokud přijde požadavek na zápis hodnot symbolových rychlostí 600, 630, 670 a 800, vytvoří vektoru dvě struktury typu `Row` a do nich se uloží hodnoty následovně. V první budou hodnoty 600, 630 a 670, v druhé jediná hodnota 800. Střední hodnota všech hodnot uložených do struktury se ukládá do proměnné *average*. Díky struktuře `Row` lze tak jednoduše zjistit, který

prvek vektoru má jakou velikost pole *array* i střední hodnotu hodnot tohoto pole. Ukládání průběžných parametrů do polí a dále pak práce s polem pouze přes jeho průměrnou hodnotu, může být důsledkem občasné chybné detekce parametru, protože se může do pole *array* uložit mnoho krajních hodnot, které pak negativně zkreslují výsledek. Krajních hodnot je naštěstí málo a tak se v průměru projevuje spíše přesnější detekce. Struktura `Stats` provádí pouze legitimní operace nad vektorem prvků `Row`, jako je vkládání, testy hodnot atd.

4.2.3 Režim dekódování komunikačního kanálu

V této práci budeme považovat za dekódování detekci konce nebo začátku datového rámce a zisk všech symbolů datového rámce, jinými slovy demodulace a následné vzorkování demodulovaného signálu symbolovou rychlostí.

Za účelem dekódování bude potřeba rozšířit vstupní frontu, která byla kvůli Fourierově transformaci omezena na 32768 vzorků, na hodnotu 2^{19}. Fourierova transformace se totiž ve stavu dekódování nepoužívá a provádí se pouze analýza I/Q dat. Prodloužení fronty tedy pomáhá zachytit delší část komunikace naráz. Při vypsání bitové posloupnosti se využije algoritmu pro stanovení symbolové rychlosti. Jednotlivé délky detekovaných symbolů se následně dělí symbolovou rychlostí, které byla zjištěna ve fázi analýzy komunikačních parametrů. Výsledkem je číslo, které udává počet stejných symbolů v detekované posloupnosti, viz obrázek 4.6.



Obrázek 4.6: Princip dekódování modulovaného pomocí ASK na základě znalosti symbolové rychlosti.

Pokud se stanoví symbolová rychlost dostatečně přesně, lze dekódovat velmi dlouhé sledy stejných symbolů jdoucí bezprostředně za sebou. Bitová kombinace reprezentující jeden symbol se následně ukládá do souboru.

U metody FSK je nutné zjistit, která frekvence odpovídá jakém symbolu. Za tímto účelem se při frekvenční modulaci ukládají hodnoty T_1 a T_2, jak jsou zobrazeny na obrázku 4.4, do statistické struktury `Stats`, následně jsou seřazeny podle velikosti a k nim mapovány symboly tak, že nižší hodnotě periody (vyšší frekvence) odpovídá nejvyšší symbol. Symbol

se pak převádí na bitovou posloupnost podle typu modulace, např.: při modulaci 2-FSK se nejnižší perioda mapuje na symbol 1 a ten následně na logickou 1, atd.

4.2.4 Problémy v průběhu analýzy nebo dekódování

Během analýzy mohou vznikat další problémy, které mohou ovlivnit přesnost procesu dekódování. Jedná se především o stanovení nesprávné symbolové rychlosti v důsledku malého počtu jednosymbolových sekvencí. Právě a jen a pouze z nich lze symbolovou rychlost vypočítat. Pokud má tedy datový rámec krátkou synchronizační preambuli a v komunikaci není dostatek jednosymbolových sekvencí, může se stát že bude symbolová rychlost detekována chybně. Tato chyba bývá potlačena především už na úrovni datové komunikace a není příliš častá. Další chyba souvisí také se symbolou rychlostí. Jedná se o případy, kdy má komunikační systém příliš rychlou symbolovou rychlost. Při realizaci algoritmu jsem využíval analýzu spektra v okolí bydliště, kde se nacházely zařízení pracující do symbolové rychlosti 5000 symbolů za sekundu. Tato mez se také projevila v samotném algoritmu. Další problém se týká stanovení nosné frekvence a typu modulace u signálu modulovaný FSK. Frekvenční špičky jsou vyjádřením počtu zastoupením jednotlivých symbolů. Například u 2-FSK je jeden symbol logická 0 a druhý symbol logická 1. Početnější zastoupení jednoho ze symbolu bude značeno větší energií špičky ve spektru. To je patrné v obrázku 4.5b, který zobrazuje spektrum signálu modulovaného metodou 2-FSK. Je vidět, že špička blíže k nulové frekvenci je nižší, než druhá špička. To je způsobeno nepoměrem logických symbolů v komunikaci, konkrétně větším počtem logických 1. Může se tedy přirozeně stát, že by komunikační systém posílal pouze jeden logický symbol a tím by se ve spektru projevila pouze jedna špička, reprezentující četnost symbolu. V takovémto případě by se nejspíše místo modulace 2-FSK stanovil typ modulace jako ASK. Tento případ je však nepravděpodobný, protože přenos začíná typicky synchronizačním slovem, které se skládá ze střídajících se hodnot 0,1.

Vlivem rozdílného přístupu stanovení symbolové rychlosti u každého typu modulace, je nutno nejdříve typ modulace určit. Protože plnění statistické struktury pro frekvenci nosné vlny i symbolové rychlosti probíhá současně, může být jedním z problémů stav, kdy typ modulace změní na jiný v průběhu plnění statistických struktur. Představme si situaci, kdy vysílač vysílá signál modulovaný metodou ASK. Struktury `Stats` se naplní z poloviny daty a následně dojde ke změně frekvence vlivem diskretizace spektra. Tato změna může být klidně pouze v řádu stovek Hz. Ve struktuře, kam se ukládají nosné frekvence, bude vytvořen nový záznam o nové nosné frekvenci, což se pak projeví jako změna typu modulace a s tím i změna algoritmu pro stanovení symbolové rychlosti. Nebo naopak, kdy je opravdový signál modulovaný metodou 2-FSK, ale poměr vysílaných symbolů je vysoký ve prospěch jednoho ze symbolů, což se projeví jako detekce modulace ASK a s tím i možná nesprávná detekce symbolové rychlosti.

Společným problémem analýzy i dekódování je rušení cizím komunikačním systémem. U analýzy bylo již řečeno, že signály s nižší energií, ačkoliv komunikující na stejné nebo podobné nosné frekvenci, je možné zanedbat. To bylo ale myšleno pouze v situaci, kdy zkoumaný komunikační systém nevysílá. Pokud budou vysílat oba dva komunikační systémy naráz nikdy nebude možná analýza, resp. analýza se provede špatně. U dekódování je tento problém o to větší, protože se nepoužívá Fourierova transformace, takže není možné zaručit, který komunikační systém komunikuje. Problémy s rušením je možné potlačit opakováním analýzy bezdrátové komunikace.

Kapitola 5

Ověření funkčnosti navrženého řešení

Funkčnost navrženého systému byla ověřena s pomocí vývojového kitu SmartRF Transceiver Evaluation Board od firmy Texas Instruments a dále prakticky, kdy byl použit systém dálkového ovládání.

5.1 Ověření pomocí vývojového kitu

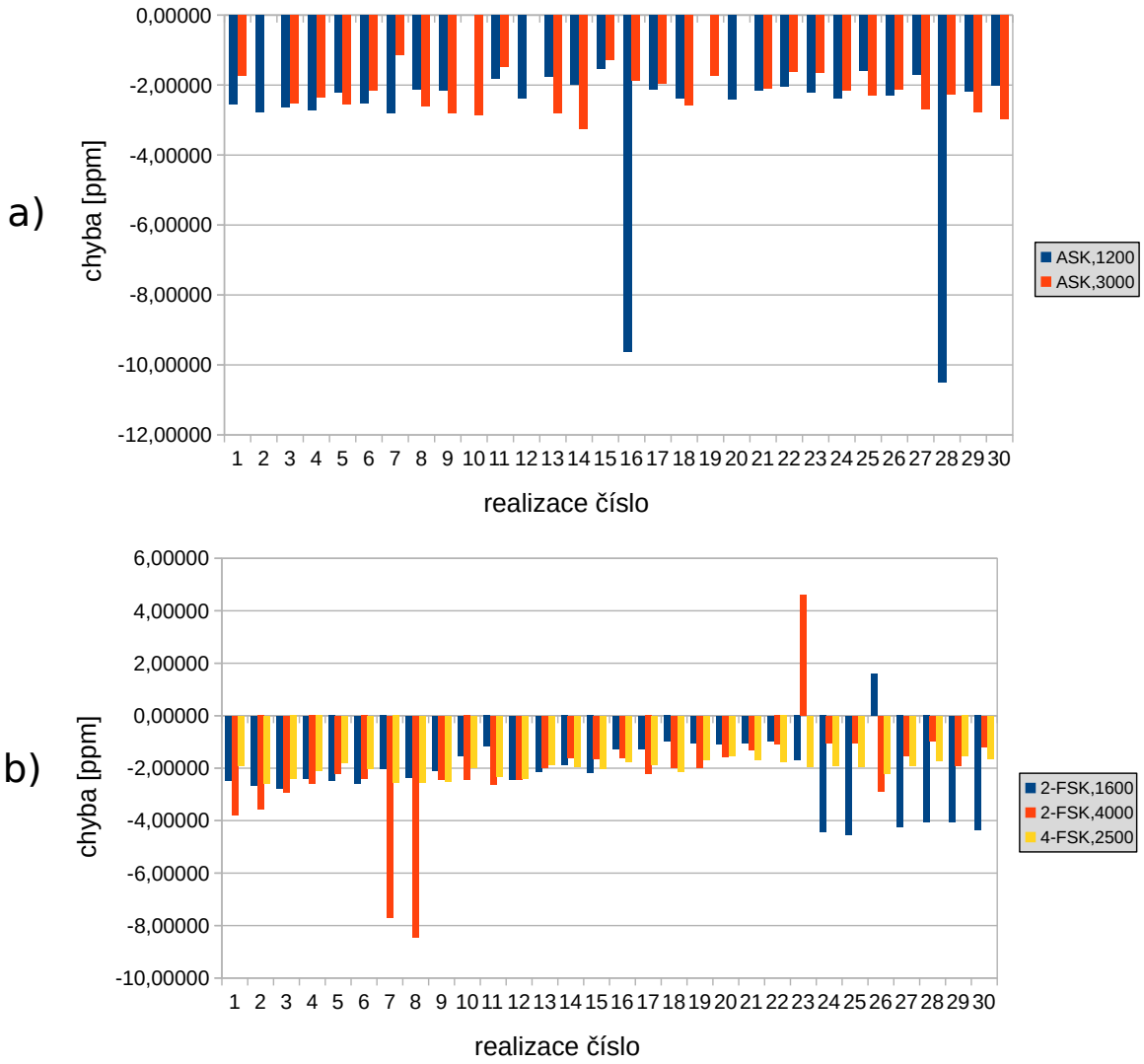
Vývojový kit je osazen modulem s integrovaným obvodem CC1120, který zajišťuje příjem i vysílání na nosných frekvencích do 1 GHz, podporuje základní typy modulací a disponuje symbolovou rychlosti do 100 000 symbolů za sekundu. Dále byla funkčnost otestována systémem dálkového ovládání vrat/brány. Výhodou vývojového kitu SmartRF je možnost přesně definovat veškeré parametry. Můžeme tedy vyhodnotit přesnost navrženého algoritmu. Vzhledem k tomu, ze máme možnost měnit frekvenci, typ modulace i přenosovou rychlost, provedl jsem vyhodnocení napříč různými konfiguracemi.

Celkem bylo provedeno 5 testovacích konfigurací. U každé konfigurace bylo provedeno 30 realizací a bylo otestováno stanovení frekvence nosné vlny, symbolové rychlosti a typu modulace. Lze předpokládat, že s dostatečně přesně detekovanou symbolovou rychlostí lze dekódování provést úspěšně. Testovací sada je popsána tabulkou 5.1:

frekvence nosné vlny [Hz]	symbolová rychlost [Symbol/s]	modulace
868 000 000	1200	ASK
868 000 000	3000	ASK
868 000 000	1600	2-FSK
868 000 000	4000	2-FSK
868 000 000	2500	4-FSK

Tabulka 5.1: Konfigurace vysílače použité pro vyhodnocení přesnosti navrženého řešení.

Obrázek 5.1a) zobrazuje chybu výpočtu nosné vlny ze všech testů amplitudové modulace, 5.1b) chybu výpočtu nosné vlny ze všech testů frekvenční modulace. Protože jsou chyby nosné frekvence malé budeme používat pojem ppm (anglicky *parts per milion*), kde 1 % = 10 000 ppm, který značí jednu miliontinu celku. Je vidět, že všechny výpočty nosné



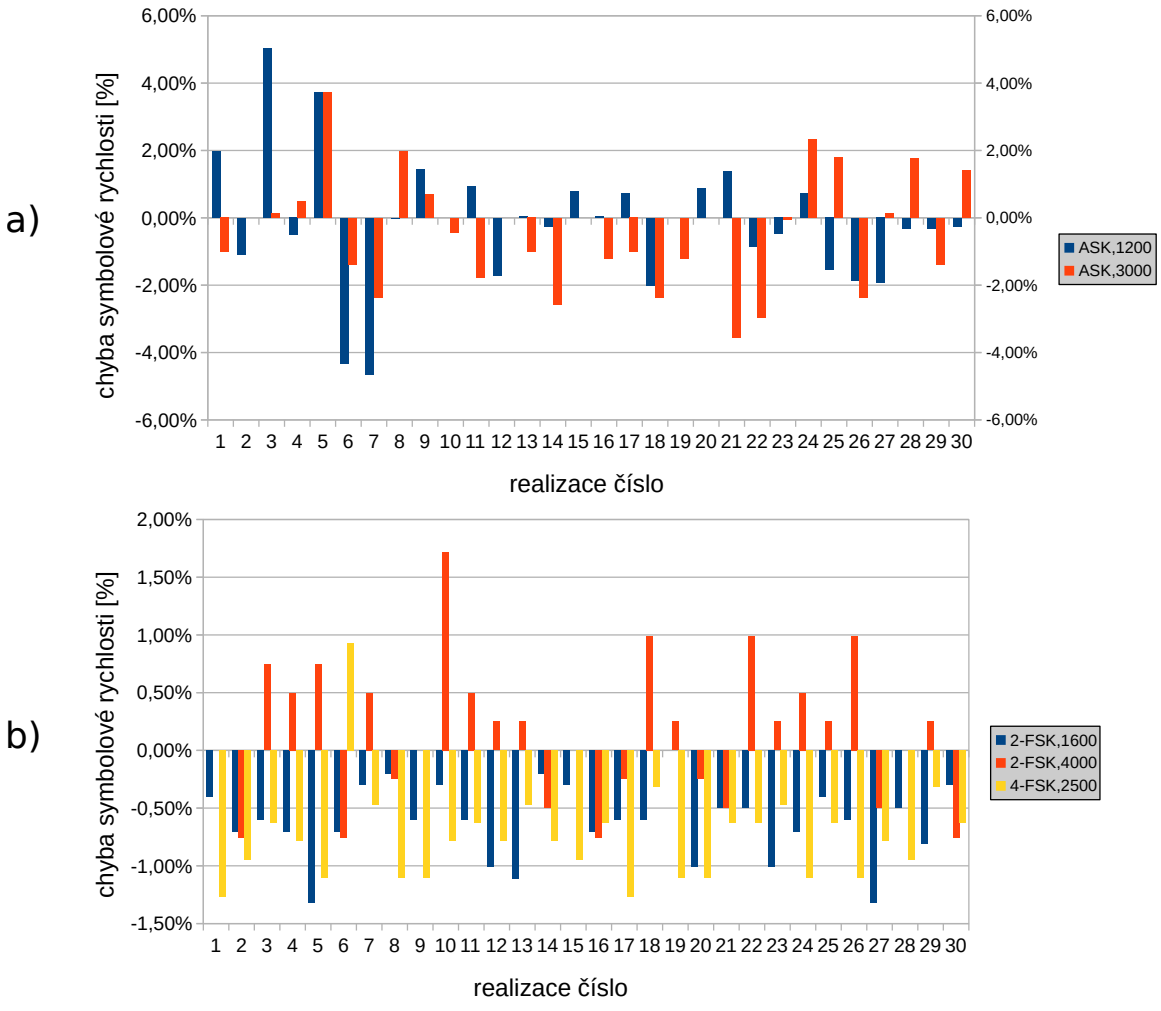
Obrázek 5.1: Detekce frekvence nosné vlny.

vlny se drží okolo chyby -2 ppm. Tato chyba je dána nepřesnou výrobou oscilátoru přijímače. Vyskytují se však případy, kde měla detekce nosné frekvence větší chybu - okolo 10 ppm. To mohlo být způsobeno právě některým z rušivých elementů, např.: cizí komunikací nebo nesprávnou diskretizací spektra. Tabulka 5.2 ukazuje výsledky automatické analýzy každé konfigurace. Hodnoty jsou průměrem všech realizací každé konfigurace.

Graf uveden na obrázku 5.2a) zobrazuje chyby automatického výpočtu symbolové rychlosti amplitudové modulace, 5.2b) chyby při výpočtu symbolové rychlosti frekvenční modulace. Vidíme, že signál modulovaný metodou FSK, dosahuje velmi dobrých výsledků i ve formě 4-FSK. Chyby způsobené během měření byly průměrně 0.5%. U jednotlivých realizací byla maximální chyba realizace č.4 u signálu modulovaný metodou ASK, při rychlosti 1200 symbolů/s, což by znamenalo chybu při dekódování na 10. stejném symbolu v pořadí.

frekvence nosné vlny [Hz]	symbolová rychlost [Symbol/s]	modulace
867 997 592	1201.91	ASK
867 998 038	3014.95	ASK
867 998 073	1609.94	2-FSK
868 998 077	3994.16	2-FSK
867 998 258	2518.8	4-FSK

Tabulka 5.2: Tabulka výsledků automatické analýzy parametrů jednotlivých konfigurací.



Obrázek 5.2: Detekce symbolové rychlosti.

5.2 Ověření v praxi

U neznámého systému (dálkové ovládání vrat) je detekce parametrů ověřena tak, že se provede včetně dekódování a pokud výsledek dekódování vykazuje datovou komunikaci (zaslání synchronizační preambule, přítomnost stejných datových sekvencí v datových rámcích) uznám, že se detekce parametrů provedla úspěšně. Tabulka 5.3 zobrazuje výsledek automatické analýzy parametrů.

frekvence nosné vlny [Hz]	symbolová rychlost [Symbol/s]	modulace
868 303 614	2344.87	2-FSK

Tabulka 5.3: Tabulka výsledků automatické analýzy parametrů neznámého systému.

Tento systém byl navíc stanoven rozptyl frekvenční modulace, který byl stanoven na hodnotu přibližně 23 kHz. Rozptyl byl ověřen pomocí aplikace HDSDR, která vyobrazuje spektrum přijatého signálu a z něj bylo možné frekvenční rozptyl odečíst.

Dekódování dat dálkové ovládání vrat vykazoval stejné bitové posloupnosti pouze v rámci jednoho stisknutí tlačítka a při novém stisku tlačítka se posílá jiná bitová posloupnost. Ovladač totiž disponuje ochranným mechanizmem typu plovoucí kód (anglicky *rolling code*). Po demontáži byl na desce plošných spojů nalezen integrovaný obvod HCS301 firmy Microchip implementující tento ochranný mechanizmus, přesněji se jednalo o KeeLoq. Dle [4] lze na tento ochranný mechanizmus provést útok, který nakonec dešifruje komunikaci. Je ale zapotřebí získat více než hodinový záznam komunikace, který následně lze na 64 procesorovém systému dešifrovat přibližně 8 dní.

Kapitola 6

Závěr

Cílem této bakalářské práce byl návrh softwaru využívající konceptu SDR, který automaticky stanoví parametry bezdrátové komunikace. Ty jsou získány výpočtem z dat nasbírané při vzorkování spektra. Návrh uvažuje základní typy modulace, které se používají pro komunikaci v bezlicenčním frekvenčním pásmu.

Experimentálně byla vyhodnocena přesnost navrženého řešení vůči referenčnímu vysílači SmartRF. Ukázalo se, že automatické stanovení parametrů komunikačního systému dosahuje překvapivě vysoké přesnosti. Např. při detekci frekvence nosné vlny byla chyba menší než 10 ppm a při stanovení symbolové rychlosti menší než 5%. Vezmeme-li v potaz fakt, že data získaná v PC jsou již zatížena různým druhem nepřesností a za účelem zvýšení robustnosti využívá navržené řešení pravděpodobnostního modelu, což může samo o sobě způsobit ztrátu dat (např. krátkých paketů) či vnést další nepřesnost (vícenásobné chybné stanovení některého komunikačního parametru), jedná se o poměrně dobrý výsledek.

Z výsledků lze konstatovat, že bezpečnost bezdrátových systému je s nástupem konceptu SDR nepochybně v ohrožení. Jako příklad uvedeme analýzu bezdrátového ovládání vrat. U tohoto systému se podařilo poměrně rychle stanovit parametry přenosového kanálu a určit, že se jedná o protokol KeeLoq. Pokud bychom nasbírali dostatečné množství dat, jsme schopni dokonce provést útok a tento systém nabourat. To vše lze provést tak, aniž bychom museli odcizit bezdrátové ovládání. Nebezpečí spojené s používáním bezdrátových systému umocňuje fakt, že útok lze provést za použití velmi nízkých finančních prostředků.

Ačkoliv dosahuje řešení dobrých výsledků, nejedná se o konečný produkt. Jako jedno z možných rozšíření je implementace méně časté modulační metody PSK. Dále by bylo vhodné použít některou z kvalitnějších hardwarových platforem jako je např.: systém Agilesdr, HackRF, které podporují i vysílání.

Literatura

[1] Al-Haddad, M.; Abdullah, S.; Ismail, Q.: Spectral technique for baud time estimation. http://www.iasj.net.

[2] Chan, T.; Plews, J.; HO, K.: Symbol rate estimation by the wavelet transform. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=608654, 2008-12.

[3] Hosking, R.: Software defined radio handbook. http://www.pentek.com/pildocs/8363/techother/DGTLRCVRHBK43.PDF.

[4] Indesteege, S.; Keller, N.; Dunkelman, O.; aj.: A practical attack on KeeLoq. http://www.cosic.esat.kuleuven.be/keeloq/.

[5] Lyons, R.: Quadrature Signals: Complex, But Not Complicated. http://www.ieee.li/pdf/essay/quadrature_signals.pdf.

[6] Prokeš, A.: Softwarově definované rádio [online]. http://www.urel.feec.vutbr.cz/web_pages/projekty/clanky/Prokes_SW_radio.pdf, 2008-12.

[7] Sklar, B.: *Digital communication: fundamentals and applications*. Prentice Hall, 2001, iSBN 978-0130847881.

[8] Song, M.: Characterizing cyclostationary features of digital modulated signals with empirical measurements using spectral correlation function. http://www.dtic.mil/dtic/tr/fulltext/u2/a544634.pdf, 2011-06.

[9] Tang, S.; Yu, Y.: Fast algorithm for symbol rate estimation. http://www.acr.atr.jp/ shtang/publication/05-IEICE-SymRate.pdf.

[10] Wegener, A.: Practical techniques for baud rate estimation. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=226306.

[11] Wolke, A.: What's your IQ - About Quadrature signals. http://www.tek.com/blog/what?s-your-iq-%E2%80%93-about-quadrature-signals%E2%80%A6.

[12] WWW stránky: Euler's formula. http://en.wikipedia.org/wiki/Euler%27s_formula/.

[13] WWW stránky: FFTW - Fast Fourier Transform in the West. http://www.fftw.org/.

Dodatek A

Obsah CD

SRC\tex Kompletní zdrojové kódy bakalářské práce pro sázecí systém LaTeX.

SRC\SDR_scpecral_analyser Kompletní zdrojové kódy aplikace pro vývojové prostředí QtCreator.

BIN Předkompilovaná aplikace ve statické podobě pro platformu Microsoft Windows, včetně potřebných knihoven.

DOC Text bakalářské práce ve formátu .pdf.

Dodatek B

Manual

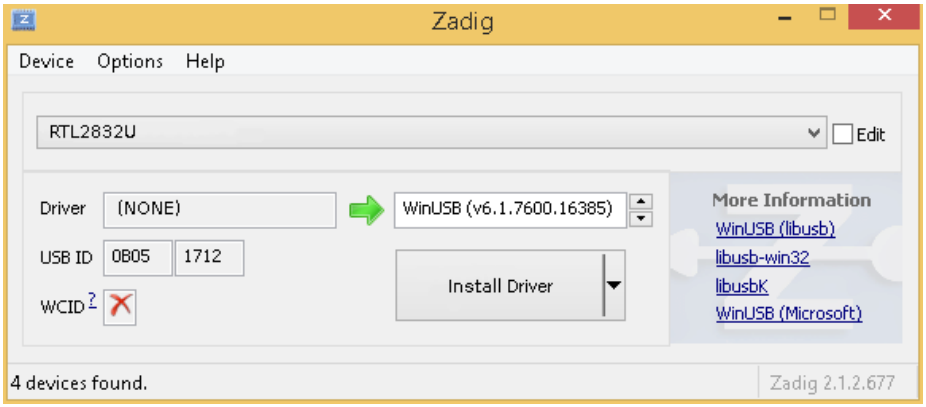
Pro správné fungování SDR na platformě Microsoft Windows je nutné nainstalovat speciální ovladač, který se nainstaluje pomocí programu Zadig [http://zadig.akeo.ie/]. Program vyžaduje administrátorské oprávnění a povolené instalace nepodepsaných ovladačů. Instalace ovladače probíhá následovně:

1. Spustit program Zadig.
2. Vložit SDR do portu USB počítače.
3. SDR se automaticky objeví v seznamu dostupných zařízení.
4. Vybereme ovladač WinUSB (v6.1.7600.16385).
5. Klikneme na Install Driver.
6. Pokud se SDR automaticky neobjeví v seznamu dostupných zařízení, pravděpodobně proběhla automatická instalace přidaného hardwaru systémem Windows. Ten ale nainstaluje ovladač k DVB-T tuneru. V tomto případě lze v programu Zadig v menu Options⟶ List All Devices zobrazit veškerá USB zařízení aktuálně připojená k PC.
7. Vybereme naše SDR.
8. Vybereme ovladač WinUSB (v6.1.7600.16385).
9. Klikneme na Reinstall Driver. Což přepíše ovladač nainstalovaný automaticky systémem Windows.

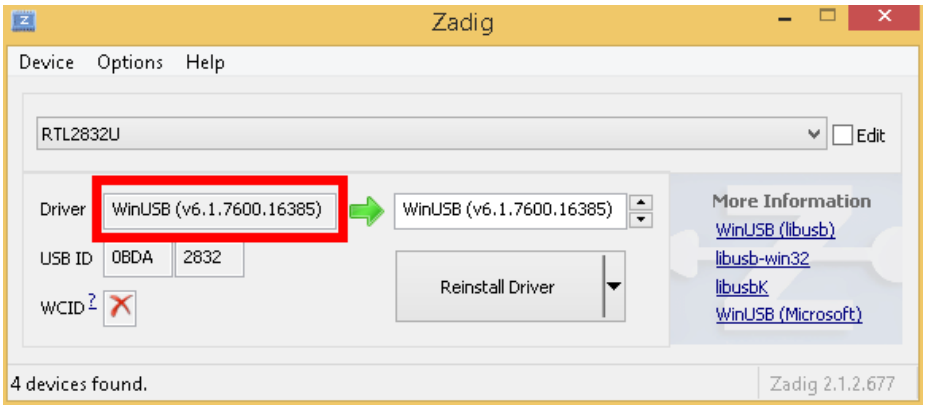
Obrázek B.1 zobrazuje rozhraní programu Zadig před instalací ovladače.

Občas se může stát, že program Zadig vrátí chybovou hlášku i přes to, že instalace proběhla úspěšně. Pokud chceme mít jistotu, že je ovladač správně nainstalován spustíme Zadig znovu a v okénku ovladače (viz červený rámeček B.2 zjistíme nainstalovanou verzi.

Uživatelské rozhraní softwaru je minimalistické. Obsahuje výpis dostupných SDR aktuálně připojených k PC (seznam SDRs), seznam frekvenčních špiček (High peaks (Hz)), zjištěné parametry komunikace (Parameters). Dále je možno aplikaci nastavit zkoumané pásmo (Frequency band) případně zvolit manuální frekvenci nosné vlny a citlivost vůči energii signálu. Tlačítka Scan, Analyse, Decode, Stop umožňuje přepínání mezi stavy aplikace.



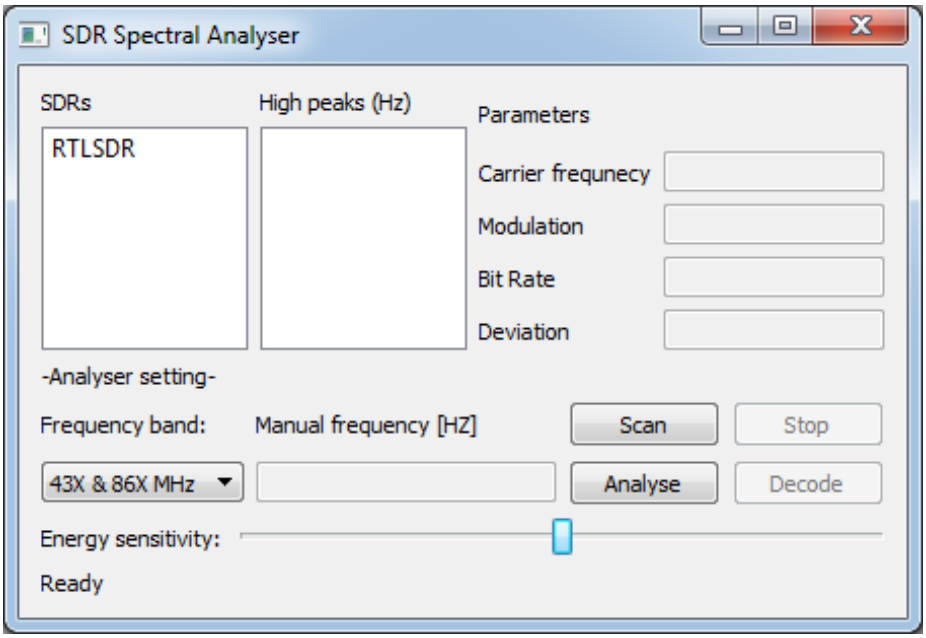
Obrázek B.1: Rozhraní programu Zadig.



Obrázek B.2: Ověření správnosti nainstalovaného ovladače SDR.

Postup analýzy bezdrátové komunikace:

1. Vybere SDR.
2. Zvolíme frekvenční pásmo a citlivost energie signálu.
3. Kliknutím na tlačítko Scan začne analýza spektra a špičky s vysokou energií budou vypsány do seznamu High peaks (Hz).
4. Po vybrání komunikace (špičky) klikneme na tlačítko Analyse, čímž začne analýza parametrů komunikace.
5. Až uzná uživatel za vhodné (typicky po naplnění statistických struktur, ale lze i dřív) klikne na tlačítko Decode, čímž se v místě uložení aplikace vytvoří soubor data.txt, do kterého se zapisují dekódované logické hodnoty.



Obrázek B.3: Uživatelské rozhraní aplikace.