ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta elektrotechnická

Katedra telekomunikační techniky

EMULACE GSM SÍTĚ V OPEN-SOURCE PROSTŘEDÍ

Květen 2014

Bakalant: Dominik Prekschl

Vedoucí práce: Ing. Pavel Bezpalec Ph.D

Čestné prohlášení

Prohlašuji, že jsem zadanou bakalářskou práci zpracoval sám s přispěním vedoucího práce a používal jsem pouze zdroje v práci uvedené. Dále prohlašuji, že nemám námitek proti půjčování nebo zveřejňování mé bakalářské práce nebo její části se souhlasem katedry.

Datum: 23.5.2014

……

podpis bakalanta

sem vložit originál zadání

Anotace

Tato bakalářská práce se zabývá GSM sítí a prostředky k její emulaci, konkrétně softwarem OpenBTS, LabView a Asterisk, z hardwarové části pak zapůjčenou jednotkou USRP, která však k tomuto účelu není zcela vhodná a slouží tak pouze jako ukázka. V teoretické části práce je popsána síť GSM, tedy to jak je realizován přenos signálu, z čeho se celá síť skládá a jak je celý systém zabezpečen. Praktická část práce se pak zabývá výše uvedeným softwarem a ukázkou programovaní USRP jednotky pomocí LabVIEW.

Klíčová slova

GSM síť, OpenBTS, Asterisk, USRP NI PCI-5640R, LabView

Annotation

This thesis concerns with GSM network and with resources needed for its emulation, especially with software like OpenBTS, LabView and Asterisk. From the hardware part it is USRP device, which was lent to me and which is not so much suitable for GSM emulation and is used just for the example. In the theoretical part of the thesis I describe how does whole GSM system work - how signal is transmitted, from which parts is network composed of or how is whole system secured. In the practical part I describe how to program USRP device via LabView.

Keywords

GSM network, OpenBTS, Asterisk, USRP NI PCI-5640R, LabView

Obsah

Seznam obrázků

Seznam tabulek

Kapitola 1

Úvod

GSM, Globální systém pro mobilní komunikaci (Global System for Mobile Communication), je mezinárodním standardem pro mobilní komunikaci. Uživatelé se tak mohou do této sítě připojit, ať jsou kdekoliv na světě. Nabízí mnoho služeb, jako je SMS (Short Message System), fax, hlasová schránka. Dalšími menšími poskytovanými službami, které zvyšují komfort uživatele, je přesměrování hovorů, či zobrazení čísla volajícího. V současnosti je využíváno několik frekvenčních pásem. Nejběžnější frekvence jsou 450 MHz, 850 MHz, 900 MHz, 1800 MHz a 1900 MHz. GSM využívá metody sdílení kanálu FDMA a TDMA.

První zmínky o GSM jsou již z roku 1982, kdy byla založena pracovní skupina Groupe Spécial Mobile, později ETSI, která navrhla první verzi stejnojmenného standardu. Tehdy se však ještě nepředpokládalo, že mobilní telefony budou tak používané, jako je tomu dnes. První telefony nebyly zcela přenosné, kvůli svým rozměrům, hmotnosti a spotřebě byly převážně instalovány do osobních automobilů. Dalo by se říci, že se jednalo o luxusní zboží, a to i pro obyvatele vyspělých zemí, ať už kvůli ceně samotných terminálů nebo z důvodu vysokých cen za hovory. Problémem byla rovněž neexistence roamingových smluv mezi operátory, což zapříčinilo to, že nebylo možné realizovat mezistátní hovory. Technické základy GSM byly definovány v roce 1987, v roce 1989 převzala kontrolu organizace ETSI.

V roce 1990 tak vznikla první specifika GSM, samotný provoz byl zahájen v polovině roku 1991 a v roce 1993 bylo již v provozu 36 GSM sítí ve 22 zemích. Systém GSM nezůstal jen evropským standardem, ale rozšířil se po celém světě. Ve všech zemích funguje na stejném principu, ale může pracovat na různých frekvencích, což ještě v nedávné době způsobovalo, že telefony určené pro evropský trh nefungovali například v USA a naopak. Dnes už je většina nových telefonů vybavena „multi-band“ anténami, což znamená, že mohou pracovat na různých frekvencích, které jsou po světě pro GSM vyhrazeny.[1]

1.1 Organizace podílející se na vývoji a provozu GSM

ETSI (Evropský ústav pro telekomunikační normy) je dle [2] nezávislá, nezisková organizace která se zabývá standardizací v telekomunikačním průmyslu v Evropě. Sídlí ve Francii a odpovídá za standardizaci i pro televizní a rozhlasové vysílání, inteligentní dopravu nebo lékařskou elektroniku. ETSI má 750 členů v 63 zemích Evropy i mimo ni, a to z řad výrobců, síťových operátorů, správců, poskytovatelů telekomunikačních služeb nebo výzkumných organizací. Z České republiky je to například České vysoké učení technické, Český telekomunikační úřad nebo Správa železniční dopravy.

GSMA [3] je organizací, která spojuje přes 800 mobilních operátorů plus dalších 250 společností z celého světa které mají se systémem GSM nějakou souvislost. Typicky tedy výrobci mobilních zařízení, softwaru nebo příslušenství. Mimo jiné organizace pořádá Mobile World Congress, který je jedním z největších světových veletrhů na kterém jsou představovány novinky ze světa mobilních technologií. Typicky se pořádá v Barceloně, letos se konal již šestý ročník.

3GPP, dle [4], můžeme označit za sdružení několika telekomunikačních společností. Toto sdružení mělo za cíl vytvořit standard pro sítě třetí generace (3G) na základech GSM, později však převzalo kontrolu i nad původním GSM. Standardy, které skupina 3GPP vydává, se označují jako Releases. Za zmínku stojí Realease 99 (rok vydání 1999), který prvně definoval 3G síť, dále pak Release 8 (rok vydání 2008), který definuje LTE.

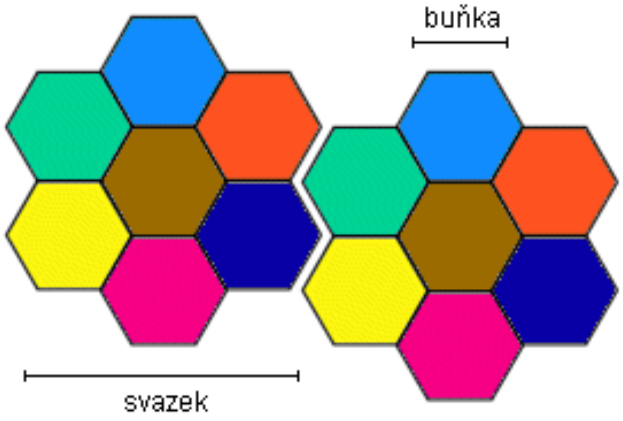
Kapitola 2

Prvky a principy GSM sítě

V následujících odstavcích bude vysvětleno jak se v GSM síti realizují hovory, z čeho se celá síť skládá, jak se registrují jednotliví účastníci do sítě a jak je celá síť zabezpečena.

2.1 Základní metody přenosu signálu a uspořádání sítě

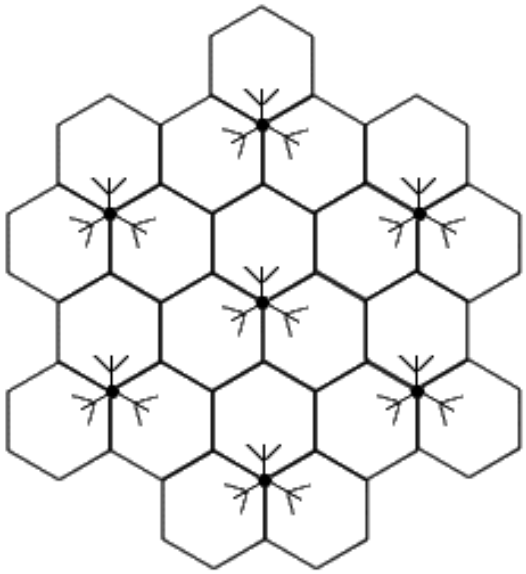
Celá síť je uspořádána do takzvaného buňkového systému což vede k efektivnímu hospodaření s frekvenčním spektrem díky přidělování stejných frekvencí v oblastech, které spolu nesousedí. Každý svazek (cluster) je tvořen sedmi buňkami, které představují určitou geografickou oblast, a v každé z těchto buněk je signál vysílán na jiné frekvenci. Pokud však k jednomu svazku připojíme druhý, není potřeba rezervovat další frekvence, ale můžeme použít ty stejné ze svazku původního. Takto lze tedy pokrýt neomezeně velké území. Princip buňkového systému je znázorněn na následujícím obrázku.



Obrázek 2.1: Buňkový systém, převzato z [5]

V hustě zastavěných oblastech můžeme využít princip sektorizace, kdy každý svazek rozdělíme na 21 menších buněk. Pro snížení počtu základnových stanic z 21 na 7 můžeme

každou z nich umístit na rozhraní tří sousedních buněk a použít sektorové antény tak, jak je naznačeno na obrázku 2.2. Sektorizace se používá z důvodu zvětšení kapacity sítě, respektive zvýšení počtu aktuálně obsluhovaných účastníků.



Obrázek 2.2: Princip sektorizace, převzato z [5]

Systém GSM využívá dvou metod sdílení přenosového média – FDMA a TDMA.

FDMA (Frequency Division Multiple Access) je metoda sdílení jednoho frekvenčního pásma více uživateli, každý uživatel, respektive skupina osmi uživatelů, tedy vysílá a přijímá svá data na specifických frekvencích, které jsou vyhrazeny pouze jim a jsou jim vyhrazeny po celou dobu spojení. Celé frekvenční pásmo je tedy rozděleno na konkrétní počet kanálů, které jsou přiřazovány účastníkům.

TDMA (Time Division Multiple Access) je druhou používanou metodou sdílení přenosového média při které jsou signály odděleny tím, že každý účastník, který v danou chvíli chce využívat daný kanál pro komunikaci, vysílá vždy v pevně daných, krátkých, časových úsecích či intervalech, které se označují jako časové sloty (Timeslot). Těchto timeslotů je typicky osm (0-7) a každý takto vzniklý interval představuje jednoho účastníka. Osm účastníků tedy může ve stejnou chvíli využívat stejnou frekvenci.

Metody jsou používány současně, a to tak, že je frekvenční pásmo rozděleno na kanály metodou FDMA a na jednotlivých kanálech se vysílá dle metody TDMA.

Jako optimální modulační metoda byla vybrána gaussovská modulace MSK, tedy GMSK.

2.2 Koeficient ARFCN

ARFCN (Absolute Radio Frequency Channel Number), dle [1], je číslo, které označuje každý pár frekvencí – jednu pro uplink, druhou pro downlink. Rozestup nosných frekvencí je vždy 200 kHz a jejich duplexní odstup (offset) se liší podle pásma, ve kterém GSM pracuje (u GSM 900 je to 45 MHz). S každým zvyšováním ARFCN se tedy zvýší obě frekvence o 200 kHz.

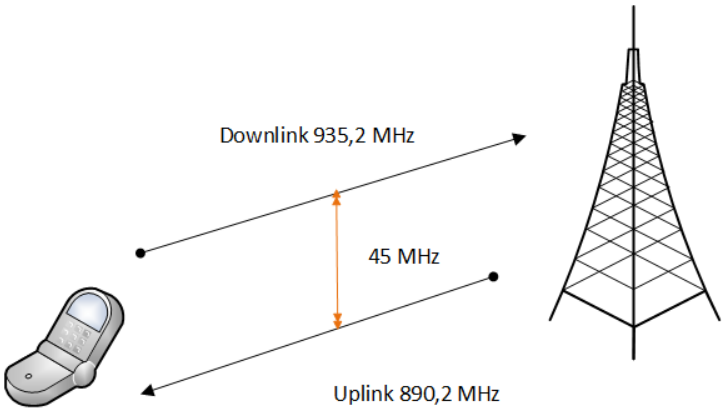
U systému GSM 900 lze tedy získat až 992 duplexních kanálů. Na každém kanálu je metodou TDMA vytvořeno 8 časových slotů, přičemž jeden slot představuje jednoho účastníka. ARFCN nabývá hodnot 1-124, tedy 8 x 124 = 992 kanálů.

	GSM 450	**GSM 850**	**GSM 900**	**GSM 1800**	**GSM 1900**
Rozsah uplink frekvence [MHz]	450 -458	824 - 849	890 – 915	1710 - 1785	1850 - 1910
Rozsah downlink frekvence [MHz]	460 -468	869 - 894	935 - 960	1805 - 1880	1930 - 1990
ARFCN	259 - 293	128 - 251	1 - 124	512 - 885	512 - 810
Offset [MHz]	10	45	45	95	80

Tabulka 2.1: Přehled používaných frekvencí a koeficientů ARFCN pro různé verze standardu GSM

Frekvence	**ARFCN**	**Frekvence Uplink, f_{UL} [Hz]**	**Frekvence Downlink [Hz]**
450 MHz	259-293	450,6 + 0,2(n-259)	$f_{UL}(n)+10$
850 MHz	128-251	824,2+0,2(n-128)	$f_{UL}(n)+45$
900 MHz	1-124	890+0,2n	$f_{UL}(n)+45$
1800 MHz	512-885	1710.2+0,2(n-512)	$f_{UL}(n)+95$
1900 MHz	512-810	1850.2+0,2(n-512)	$f_{UL}(n)+80$

Tabulka 2.2: Způsob výpočtů nosných downlink a uplink frekvencí



Obrázek 2.3: Konkrétní frekvence GSM 900 při ARFCN 1

2.3 Logické kanály

Díky použití výše zmíněných metod sdílení přenosového média vznikají na rádiovém rozhraní fyzické kanály, popsané v [6]. Jsou to tedy kombinace přiděleného rádiového kanálu o šířce 200 kHz, označeného pomocí ARFCN, a časového intervalu, timeslostu, o hodnotě 0-7. Do těchto fyzických kanálu pak může být procesem mapování vložen různý logický kanál. Logické kanály se dále dělí na kanály provozní a signalizační.

2.3.1 Provozní kanály

Provozní kanály zajišťují přenos digitalizovaných hovorů a datových signálů. Jsou dále rozděleny na kanály s plnou rychlostí TCH/F (Full Rate Traffic Channels) a kanály s poloviční rychlostí TCH/H (Half Rate Traffic Channels).

2.3.2 Signalizační (řídící) kanály

Jak již název napovídá, tyto kanály zajišťují signalizaci. Dále je dělíme do tří následujících skupin.

- Rozhlasové kanály BCH (Broadcast Channels)
- Kanály všeobecného řízení CCCH (Common Control Channel)

- Vyhrazené řídicí kanály DCCH (Dedicated Control Channel)

První skupinou jsou rozhlasové kanály (BCH). Těmi hlavními jsou kanály určené pro korekci kmitočtu FCCH (Frequencu Correction Channel) které nesou informaci umožňující korekci naladění mobilní stanice a identifikaci kmitočtu nesoucího signalizační kanály. Dále pak kanál synchronizace SCH (Synchronization Channel), který nese informace pro rámcovou signalizaci mobilní stanice a identifikaci základnové stanice. Posledním rozhlasovým kanálem je všeobecný kanál BCCH (Broadcast Common Channel). Ten nese informaci o aktuálním způsobu mapování signalizačních kanálů, o lokalizační oblasti nebo o výzvách k mobilní stanici. Sleduje ho každá mobilní stanice.

Druhou skupinou jsou kanály všeobecného řízení CCCH. Prvním z těchto kanálu je návěstní - PCH (Paginig Channel). Je sledován každou mobilní stanicí ve stavu pohotovosti a slouží k předání informace o příchozím hovoru. Druhým z kanálů této podkategorie je kanál náhodného přístupu RACH (Random Access Channel). Jedná se o vzestupný kanál, který slouží pro vyžádání samostatného řídícího kanálu pro další signalizaci. Třetím je řídící kanál potvrzení přístupu AGCH (Access Grant Control Channel) který je využíván pro přidělené samostatného řídícího kanálu mobilní stanici, která o to požádala.

V poslední kategorii nalezneme takzvaný pomalý přidružený řídící kanál SACCH (Slow Associated Control Channel). Ten zajišťuje přenos signalizace k existujícímu spojení. Naproti tomu rychlý přidružený řídící kanál FACCH (Fasr Associated Control Channel) vzniká a zaniká podle potřeby, ale jinak slouží ke stejnému účelu. Posledním ve skupině je samostatný přidělený řídící kanál SDCCH (Stand Alone Dedicated Control Channel), který slouží pro obousměrnou komunikaci mezi základnovou a mobilní stanicí před přidělením provozního kanálu.

2.4 Mobilní stanice – MS

Mobilní stanice je tvořena dvojicí mobilního zařízení a SIM karty.

Mobilním zařízením se rozumí přístroj jako takový. Každé mobilní zařízení je jednoznačně identifikováno číslem IMEI (International Mobile Equipment Identity), které je danému

zařízení přiřazeno již během procesu výroby a lze jej tedy označit za sériové číslo daného zařízení.

SIM (Subscriber Identity Module) je plastová karta malých rozměrů, která se vkládá do mobilních telefonů a obsahuje data, která jsou pro daného účastníka specifická a tedy neměnná – například IMSI, TMSI, MSISDN, autentikační klíč Ki, šifrovací klíč Kc, SPN nebo LAI. O těchto údajích bude psáno dále v práci. SIM karta dále obsahuje data, která již uživatel měnit a ovlivňovat může, typicky to bývají kontakty nebo seznam volaný a přijatých číslel. Větší podrobnosti můžeme nalézt v [7].

Každá karta je chráněna čtyřmístným PIN (Personal Identification Number) kódem, který slouží k odblokování karty. Pokud je tento kód zadán špatně třikrát, musí být karta odblokována kódem PUK (Personal Unblocking Key), který je tak jako kód PIN uchováván na SIM kartě.

Hlavním účelem SIM karty je ověření a identifikace uživatele.

2.5 IMSI

IMSI (International Mobile Subscriber Identity), dle [1], je unikátní číslo, většinou patnáctimístné, které je operátorem přiděleno každé SIM kartě. První tři číslice představují kód země (MCC – Mobile Country Code), pro Českou republiku je to 230. Další dvě až tři číslice kód operátora (MNC – Mobile Network Code) a zbylá čísla identifikují konkrétního uživatele (MSIN – Mobile Subscriber Identification Number) v domácí GSM síti.

¨

MNC	**Podnikatel**
01	T-Mobile
02	O2
03	Vodafone
04	Air Telecom
05	TRAVEL TELEKOMMUNIKATION, s.r.o.
07	ASTELNET s.r.o
08	Compatel s.r.o.
98	Správa železniční dopravní cesty, státní organizace

Tabulka 2.3: Přidělené MNC v České republice dle ČTÚ [8]

Identifikátor IMSI slouží k autorizaci účastníka, celý proces je popsán v kapitole 2.11.1.

2.6 MSISDN

MSISDN (Mobile Subscriber Integrated Services Digital Network Number), také popsáno v [1], je z pohledu účastníka jeho telefonní číslo. Přidělování MSISDN čísel se řídí plánem E. 164 definovaným Mezinárodní telekomunikační unií (ITU-T). Podle tohoto plánu může mít MSISDN maximální délku patnáct číslic a skládá se ze tří částí. První částí je kód země - CC (Country Code), pro Českou republiku to je 420, následuje národní směrové číslo - NDC (National Destination Code), které určuje mobilní síť v příslušné zemi a poslední částí je účastnické číslo – SN (Subscriber Number), které definuje konkrétního uživatele.

Přenositelnost telefonních čísel je zajištěna tím, že číslo MSISDN je v podstatě softwarově přiřazené k IMSI v Domovském registru, účastník si tak může ponechat své telefonní číslo při výměně SIM karty, respektive je možná změna telefonního čísla při zachování stejné SIM karty. Z toho tedy vyplívá, že telefonní číslo není pevně vázané se SIM kartou, jak si mnozí myslí.

2.7 Stanice BTS, systém BSC, BSS

BTS (Base transceiver station), popsáno v [1], je přístupový bod pro mobilní stanice do GSM sítě. Odpovídá tak za přenos dat mezi mobilní stanicí a GSM sítí. To zahrnuje kódování řeči, zabezpečení, multiplexování a modulování / demodulování rádiových signálů. Jedna BTS stanice má obvykle vyzařovací úhel 120°, proto můžeme na stožárech obvykle vidět tři BTS stanice vedle sebe – pokrývají tak celých 360° kolem sebe.

Dříve pro spojení jednotlivých BTS sloužily radioreléové spoje, v současnosti s příchodem nových technologií a s nárůstem požadavků na rychlost a množství přenesených dat bývají BTS připojené do optické sítě, která má několikanásobně vyšší přenosové rychlosti a větší kapacitu než radioreléové spoje.

Tyto stanice jsou ovládány systémem BSC (Base Station Controller), který alokuje rádiové kanály, spravuje používané frekvence, měří a zpracovává signály od mobilních stanic a vykonává takzvané handovery. K handoveru dochází ve chvíli, kdy se mobilní stanice vzdaluje od jedné BTS a přibližuje se ke druhé s lepším signálem. Pokud handover proběhne korektně, účastník ani nepozná, že byl přepojený z jedné BTS na druhou. Pokud systém BSC spravuje handovery, tak pouze mezi vlastními BTS.

Fyzicky může být BSC zcela na odlišném místě než BTS.

Rozhraní mezi BTS a BSC se nazývá Abis Interface.

Stanice BTS spolu se systémem BSC tvoří takzvaný Systém základnových stanic (BSS – Base Station System).

2.8 Síťový spojovací subsystém NSS

Subsystém NSS (Network Switching Subsystem), dle [9], tvoří následující zařízení:

- Ústředna MSC
- Domovský registr HLR
- Návštěvnický registr VLR
- Registr mobilních zařízení EIR
- Centrum autorizace AuC
- SMS centrum
- Jednotka spolupráce s externími sítěmi IWF

2.8.1 Ústředna MSC

MSC (Mobile Switching Center) je nejdůležitější částí celé GSM sítě. Dochází tu zejména k sestavování spojení a směrování hovorů. Jedna ústředna MSC může ovládat mnoho BSC a zároveň komunikuje s ostatními MSC. Většinou je celá síť vybavena více MSC ať už z důvodu rozložení zatížení celé sítě tak i z důvodu lepšího vypořádání se s možným výpadkem celé ústředny MSC.

Rozhraní mezi BSC a MSC se nazývá A interface, rozhraní mezi ústřednami MSC se označuje jako E interface.

2.8.2 Brána ústředny GMSC

GMSC (Gateway Mobile Switching Center) plní funkci brány mezi dvěma sítěmi. Pokud chce mobilní účastník volat do sítě jiného operátora nebo do pevné sítě, musí jeho hovor projít přes GMSC, kde je navázán do klasické veřejné telefonní sítě PSTN (Public Switched Telephone Network). Ta je tvořena sítěmi jednotlivých telefonních operátorů, které se skládají z telefonních linek, optických kabelů, mikrovlnných spojů, mobilních sítí, komunikačních satelitů a podmořských telefonních kabelů vzájemně propojených telefonními ústřednami.

2.8.3 Domovský registr HLR

Domovský registr (Home Location Register) je databáze, která permanentně uchovává data o účastnících, jako je IMSI, současná lokace mobilní stanice, MSISDN a jiné. Těchto databází bývá fyzicky více, jsou rozmístěny po celé oblasti, ve které daný operátor působí, všechny ale obsahují stejná data, aby nedocházelo ke zbytečnému vytěžování sítě.

2.8.4 Návštěvnický registr VLR

Návštěvnický registr je rovněž databáze, obsahuje však pouze informace o těch účastnících, kteří jsou připojeni v dané lokaci, kterou tento registr spravuje. VLR tak snižuje celkový počet dotazů na HLR a tím i zatížení celé sítě. Registry VLR jsou identifikované kódem, který reprezentuje danou geografickou oblast, v níž pracují.

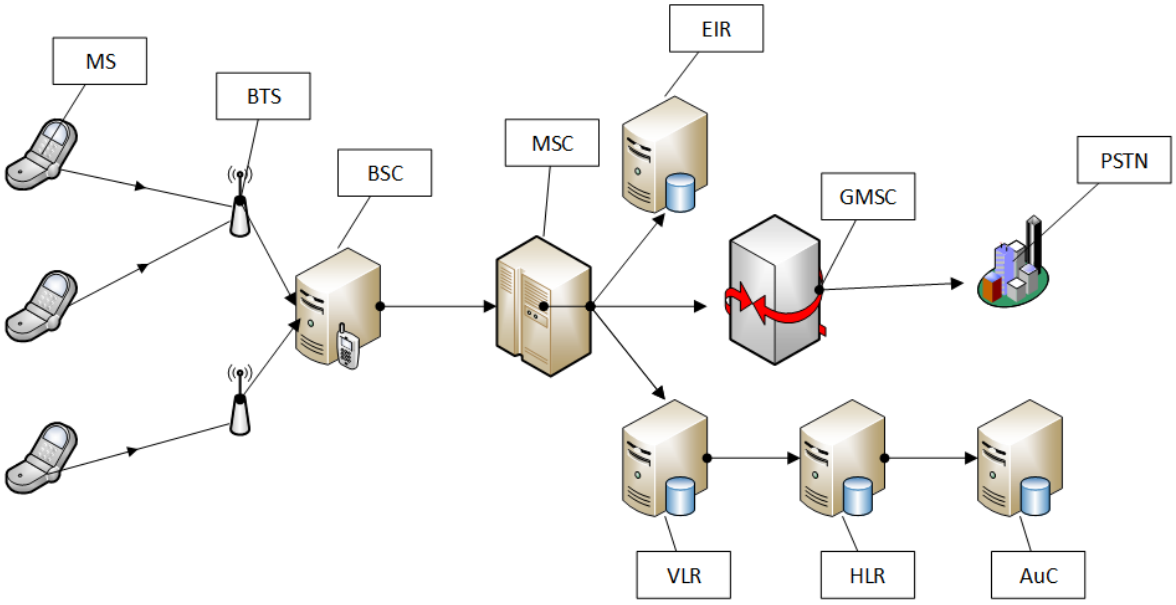
2.8.5 Registr mobilních zařízení EIR

Jedná se o databázi připojených, ale také odpojených (vypnutých) mobilních zařízení. Jednotlivé mobilní stanice jsou zde ukládány dle svých IMEI. Registr EIR je tedy databázi konkrétních přístrojů. Celá databáze bývá obvykle rozdělena do tří kategorií. Do první kategorie řadíme zařízení, která nevykazují podezřelé chování a jsou tedy plně oprávněná k provozu – takzvaný whitelist. Druhou kategorií jsou zařízení, která nefungují tak, jak síť očekává a jsou částečně monitorována – takzvaný greylist. Do třetí kategorie spadají zařízení, která mají například naklonované IMEI nebo taková, která jsou nahlášena jako zcizená, ta se většinou do sítě už nepřipojí – takzvaný blacklist.

Rozhraní mezi MSC a EIR se nazývá F interface.

2.8.6 Centrum autorizace AuC

AuC zpracovává ověřování a šifrování zpráv ve vlastní síťi. Obsahuje Ki pro každé IMSI v dané síti, tedy i pro ty SIM karty, které se ještě nikdy do sítě nepřihlásily, nebo ani neprodaly u operátora, ale jsou připraveny k použití. Toto centrum má dále na starost šifrovací klíč, podle kterého se šifruje každý účastnický signál přenášený rádiovým rozhraním. Tento klíč je unikátní pro každého účastníka a je proměnný v čase, nazývá se Kc.



Obrázek 2.4: Schéma GSM sítě

2.9 Operační a podpůrný systém OSS

Tento systém zajišťuje chod a údržbu celé GSM sítě. To znamená, že monitoruje mobilní stanice, zajišťuje jejich registraci do sítě a eviduje ty, které jsou porouchané, dále také konfiguruje síť nebo spravuje tarifikaci služeb. Skládá se z administrativního centra (ADC), centra pro řízení sítě (NMC), provozního a servisního centra (OMC).

2.10 Signalizace v GSM síti

Signalizace je zajištěna sítí, která spojuje všechny výše uvedené části a je na ni využito signalizačního systému číslo 7 SS7 (Signaling System Number 7). Jedná se v podstatě o soubor protokolů využívaných v moderních telefonních sítích. Hlavním úkolem tohoto systému je předávání informací k uskutečnění a ukončení hovorů, překládání telefonních čísel, zasílání textových zpráv a účtování služeb. Detailněji popsáno v [10].

OSI vrstva	SS7 protokoly
Aplikační	TCAP, MAP, IS-41, INAP, CAP,TUP, ISUP
Síťová	SCCP, SIGTRAN (IP7), MTP Level 3
Linková	MTP Level 2
Fyzická	MTP Level 1

Tabulka 2.4: Příklady používaných protokolů SS7

Signalizační okruhy jsou v sítích používajících SS7 odděleny od okruhů hlasových a to z toho důvodu, že v signalizačních okruzích je využito takzvaného přepojování paketů a telefonní okruhy využívají přepojování okruhů. V paketově orientovaných sítích se data odesílají po menších částech – paketech, kdy každý paket obsahuje ve své hlavičce cíl své cesty a jednotlivé části dat tak mohou putovat sítí různými cestami. Vyslaná data se tak skládají až v cíli, kdy dorazí, při úspěšném přenosu, všechny pakety. V okruhově orientovaných sítích dochází před začátkem komunikace k sestavení celé trasy (okruhu), po které bude spojení probíhat. Po ukončení spojení se okruh zruší. Pro telefonování to tedy představuje jistou výhodu oproti paketově orientovaným sítím – v paketově

orientovaných sítích dochází na každém uzlu k určitému zpoždění, kdy se směrovač musí rozhodnout, kterou další cestu v síti zvolí. K tomu v okruhově orientovaných sítích nedochází. Dnes se díky rychle se rozvíjejícím technologiím již pro komunikaci v reálném čase dají bez problémů využít sítě s přepínáním paketů. Před pár lety však využití přepínání okruhů bylo jistě výhodnější.

Uzly v signalizační síti nazýváme signalizačními body SP (signaling Points), které lze rozdělit do tří skupin:

- SSP - Service Switching Point
- SCP - Service Control Point
- STP - Signal Transfer Point

SSP plní funkci ústředny – propojují hlasové linky a je to jediné místo, kde je propojena signalizační a hlasová část sítě. V GSM síti tento bod můžeme označit jako MSC (Mobile Switching Center). Za tímto bodem už by teoreticky mohly být připojeny telefonní přístroje. V GSM síti je však ústředna MSC napojena na systém BSC, kam jsou napojeny stanice BTS a až na ně mobilní stanice.

SCP jsou místa, které v GSM poskytují databáze potřebné pro směrování volání a zpráv. Konkrétně tedy registry HLR, VLR a EIR.

STP označuje přepínače v signalizační síti a umožňuje tak například komunikaci mezi SCP a SSP, které nejsou přímo propojeny.

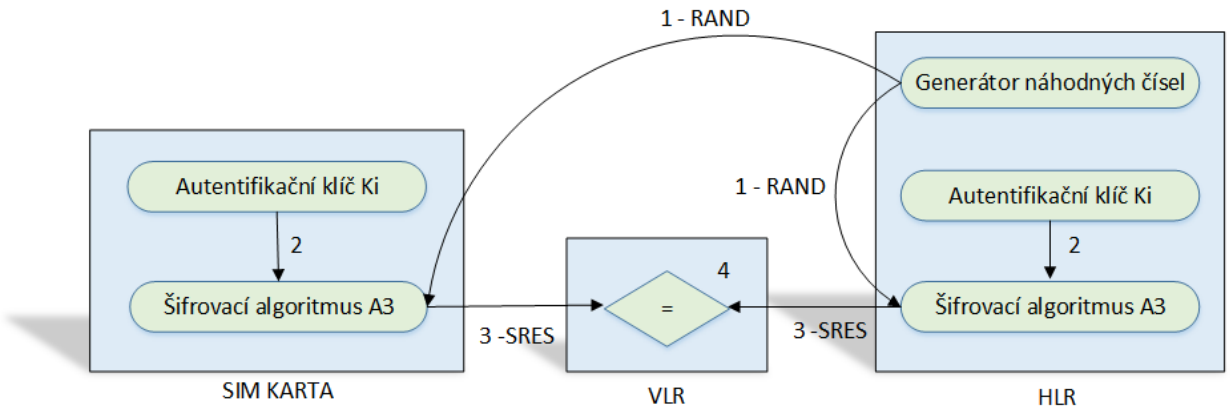
Všechny tři výše uvedené prvky jsou v síti vždy zdvojeny a umístěny na odlišných místech. Tím je zajištěna vyšší spolehlivost a tedy zachování funkčnosti celé sítě při výpadku některého z uzlů.

2.11 Bezpečnost v GSM

Tak jako v ostatních telefonních systémech je třeba dbát na bezpečnost a to nejen z důvodu zabránění odposlechu hovorů, tak i z důvodu možného zneužití ztraceného telefonu. Otázku bezpečnosti tak můžeme rozdělit do dvou kategorií. První z nich využívá registr EIR a již zmíněný systém „listů“ - whitelist, greylist a blacklist. Jedná se tedy o ověření účastníka, respektive jeho mobilní stanice a jeho SIM karty, při registraci do sítě. Druhou kategorií je pak samotné šifrování hovorů. V následujících podkapitolách bude vysvětleno jakým způsobem je zajištěna anonymita účastníka při komunikaci jeho mobilní stanice s GSM sítí dle [11].

2.11.1 Proces registrace účastníka do sítě GSM

Po zapnutí mobilní stanice je do sítě vyslán požadavek na registraci. Mobilní stanice v první fázi ověření zašle své IMSI do návštěvnického registru VLR. Z důvodu anonymity je IMSI okamžitě nahrazeno číslem TMSI (Temporary Mobile Subscriber Identity), které se uloží na SIM kartu a do registru VLR. Následuje vygenerování náhodného čísla RAND v registru HLR, na které je spočítána odezva podle algoritmu A3 pomocí autentifikačního klíče Ki, která se nazývá SRES (Signed Response) (SRES=A3(RAND,Ki)). Klíč Ki byl již zmiňován v kapitole zabývající se obsahem SIM karty, jedná se tedy o uživatelsky nepřístupnou hodnotu. Zároveň je pomocí algoritmu A8 vygenerován šifrovací klíč Kc z klíče Ki (Kc=A8(Ki)). Trojice čísel RAND (128 bitů), SRES (32 bitů) a Kc (64 bitů) je dále předána do registru VLR, kde je po dobu autentifikace uchovávána. Stejné číslo RAND, vygenerované v HLR, je odesláno mobilní stanici, která v SIM kartě na základě znalosti klíče Ki, který je v ní uložen, a šifrovacího algoritmu A3 dopočítá odpověď SRES. Ta je odeslána zpět do návštěvnického registru VLR, kde je porovnávána s tou, kterou návštěvnický registr obdržel od registru domovského. Pokud jsou odpovědi SRES stejné, má stanice garantovaný přístup do sítě. Lze tedy pozorovat, že při komunikaci přes rádiové rozhraní je přenášeno pouze náhodné číslo RAND a odpověď SRES, které jsou bez znalosti šifrovacího algoritmu a autentifikačního klíče nepoužitelné pro získání přístupu do sítě pod cizí identitou. Pro lepší představu jsem tento odstavec přenesl do obrázku 2.5.



Obrázek 2.5: Proces registrace účastníka do sítě

2.11.2 Šifrování hovorů v GSM síti

Při šifrování hovoru je využito další hodnoty – Kc. Proces vygenerování tohoto údaje je popsán v předcházejícím odstavci a je generován zvášť pro každé spojení. Pro šifrování hovorů se využívá algoritmus A5. Ten pracuje s klíčem Kc a číslem TDMA rámce (22 bitů, které se mění každých 4,615 ms) a je z důvodu nutné výpočetní kapacity implementován do mobilní stanice. Opět můžeme vidět, že se přes rádiové rozhraní nepřenášejí žádné citlivé údaje.

Algoritmy A3 a A8 nejsou pevně definovány v doporučení pro GSM, záleží zde tedy na dohodě/domluvě mezi výrobcem SIM karet a provozovatelem sítě.

Kapitola 3

Prvky potřebné k emulaci GSM sítě

Následující kapitola se bude zabývat hardwarovými a softwarovými částmi, které jsou potřeba k emulaci GSM sítě.

3.1 USRP

Obecně jsou USRP [12] jednotky softwarově řízená rádia (USRP – Universal Software Radio Peripheral), které jsou vyvíjeny společnostmi Ettus Research, LLS a její sesterskou společností National Instruments. Využití těchto jednotek je zejména v laboratořích a na univerzitních půdách. Bývají připojeny skrze rozhraní USB, ethernet nebo s vlastním procesorem na jinou sběrnici hostitelského počítače.

Všechny tyto jednotky musí být schopné generovat vlastní hodiny, být schopné synchronizace, mít FPGA modul, který uživateli umožňuje přístup a tedy i naprogramování celé jednotky a mít A/D, D/A převodníky, které umožní připojení antén, či jiných VF rozhraní.

Hlavní výhodou softwarově řízených rádií je, že jedna jednotka může zastat funkci několika rozdílných zařízení pouhým přeprogramováním. Konkrétním příkladem může být RFID čtečka, přijímač GPS signálu, dekodér digitálního pozemního televizního vysílání nebo demodulátor AM/FM signálu pro příjem rozhlasového vysílání. Mě však v této práci zajímalo využití USRP jednotky jako základnové GSM stanice.

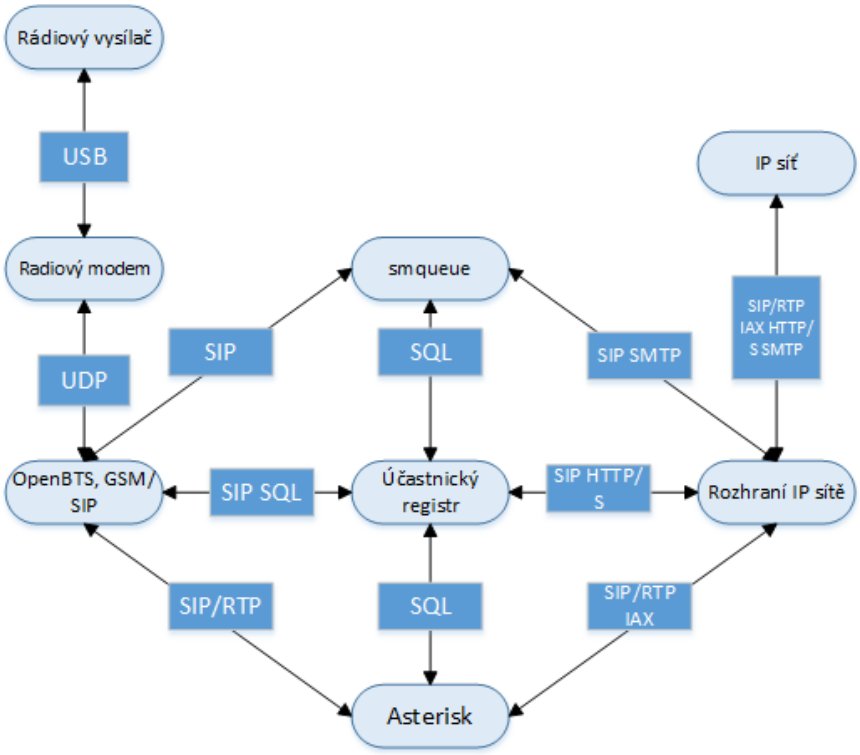
Z hlediska podpory operačními systémy zde moc omezení nenajdeme – podporovány jsou všechny tři nejčastější platformy – tedy Linux, MacOS a Windows, ale záleží však na konkrétním modelu, nicméně pro každý operační systém existuje několik alternativ USRP. Nutná je podpora ovladačů UHD (USRP hardware driver) pro daný software, skrze který je možné USRP kartu konfigurovat, nejčastěji LabVIEW, GNU Radio a Simulink.

3.2 OpenBTS

OpenBTS, dle oficiálních webových stránek [13], je open source software spravován společností Range Networks, který umožňuje definovat GSM přístupový bod, který umožní standartním GSM mobilním telefonům komunikovat skrze protokol SIP. K provozu je dále třeba pobočková ústredna, typicky Asterisk, který je od verze OpenBTS 4.0 součástí instalačního balíčku. Ústřednu pak může sdílet i více OpenBTS, z toho tedy vyplívá podpora handoverů a možnost pokrytí většího území.

Hlavními funkcemi, které OpenBTS zajišťuje je:

- Funkce časového dělení TDM
- Zjišťování a opravy chyb vzniklých při přenosu metodou FEC
- Spravuje LAPDm, což je protokol, který zajišťuje komunikaci mezi BTS a MS pracující na spojové vrstvě
- Spravuje GSM-SIP brána pro volání a SMS



Obrázek 3.1: Vnitřní uspořádání OpenBTS; Rozhraní IP sítě a Rádiový vysílač jsou dvě hardwarové součásti, vše ostatní je software; detailněji popsáno v [14]

3.3 LabVIEW

LabVIEW, dle [15], je vývojové prostředí pro grafický programovací jazyk společnosti National Instruments, který se jmenuje G.

LabVIEW je využíváno pro sběr reálných dat „ze světa“ a jejich následnou analýzu, ovládání různých zařízení, analýzu signálů, logické a numerické operace, průmyslovou automatizaci nebo simulaci všech jmenovaných možností. LabView svými rozsáhlými možnostmi dokáže jinak náročný projekt udělat snazším a méně náročným z hlediska potřebných osob, které by se na projektu měly podílet. LabView podporuje připojení a ovládání širokého spektra hardwaru, například zařízení pro sběr dat různého typu, senzory, kamery nebo motory.

Pro programování v rámci této práce je použito LabVIEW ve verzi 2009, které je spustitelné pouze na školní síti, odkud je licencováno. Podrobnější využití tohoto programu bude popsáno ve čtvrté kapitole.

3.4 Asterisk

Jedná se o pobočkovou ústřednu, která funguje na obyčejném počítači s operačním systémem Linux. Jde tedy o vcelku levné řešení pro spojení několika pevných telefonních zařízení například v menší firmě. Asterisk poskytuje plně VOIP řešení hovorů, tím odpadá nutnost tažení zvláštní kabeláže pro telefony a lze využít vybudovanou ethernetovou infrastrukturu pro počítačové sítě. Samozřejmostí je podpora hlasových schránek či konferenčních hovorů. Díky prefixům není problém volat na národní či mezinárodní linky, tedy mimo rozsah přímo připojených jednotek k dané ústředně.

3.5 GNU Radio

GNU Radio je dalším open-source softwarem, ve kterém můžeme tvořit bloková schémata pro softwarová rádia (USRP) a následně je do nich implementovat nebo je můžeme použít jen pro simulace. Můžeme říct, že se jedná o alternativu k LabView. Osobně jsem tedy

software nezkoušel instalovat ani s ním pracovat, protože jsem použil již výše zmíněné LabView. Nicméně podle recenzí a ohlasů na internetu je GNU Radio určitě vhodnou alternativou, zejména pak pokud pracujeme na unixovém operačním systému, a proto tento software stojí za to zmínit.

3.6 NI PCI-5640R

NI PCI-5640R je USRP jednotka použita v této práci, která je připojena přímo na PCI sběrnici hostitelského počítače. Ten je osazen procesorem Intel Pentium 4, 2,40 GHZ, 1GB paměti RAM a jako operační systém byl zvolen Windows XP. Tato konfigurace je však zvolena kvůli programu LabVIEW, ne z hlediska požadavků USRP karty. Díky velkým rozměrům samotné karty bylo složité najít počítačovou skříň, do které by se fyzicky vešla. K serveru se dá přistupovat skrze tunel a vzdálenou plochu odkudkoli z internetu. Pro přístup používám software Remmina, který byl součástí distribuce Ubuntu 12.04.

Tato jednotka je od jiných USRP poměrně odlišná, a to jejím způsobem připojení. Ostatní USRP bývají připojené skrze USB či ethernet. To je určitým zjednodušením z hlediska podpory různým softwarem třetích stran, který s USRP pracuje. Protože se pravděpodobně jedná o jediné USRP připojené na PCI sběrnici, je podpora značně omezená a musel jsem si tak vystačit pouze s LabView.

3.6.1 Specifikace NI PCI-5640R

Následující stručná specifikace je platná při teplotách od 0 do 40°C a po uplynutí deseti minut pro ustálení všech parametrů a zahřátí na provozní teplotu. Čerpáno z datasheetu, viz [16].

Analogový vstup:

- Počet kanálů: 2, konektory SMA
- Maximální vzorkovací rychlost: 100 MS / s
- Maximální šířka pásma: 20 Mhz
- Vstupní impedance: 50 Ohm

Analogový výstup

- Počet kanálů: 2, konektory SMA
- Maximální vzorkovací rychlost: 200 MS / s
- Vstupní impedance: 50 Ohm

FPGA

- Model: Xilinx Virtex-II Pro P30 (XC2VP30)
- RAM: 2,448 Kb
- Logické buňky: 30 816

Obrázek 3.2: NI PCI-5640R, převzato z [17]

Kapitola 4

Praktické využití USRP

V následující kapitole budou ukázány způsoby, jak lze USRP využít v praxi a jakým způsobem ho můžeme programovat. Bude zde i vysvětleno, proč USRP použité v této práci, bohužel, není vhodné k emulaci GSM sítě.

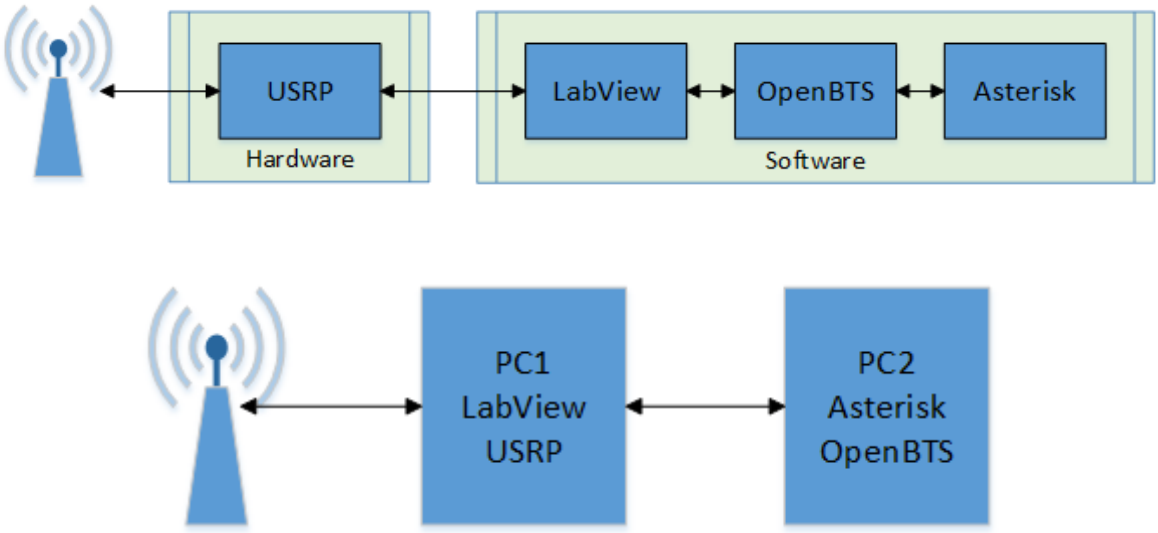
4.1 NI PCI-5640R a GSM

Po vytvoření programu pro vysílání, přijímání a směrování GSM signálu jsem zjistil, že USRP jednotka nedokáže vysílat vyšší frekvence než 100 MHz, viz Obrázek 9, a je tedy pro emulaci GSM sítě nepoužitelná. Původní program nebyl nijak složitý. Jeho funkcí bylo nasměrovat vysílaný a přijímaný signál na správné vstupy a výstupy USRP a definovat odkud a kam se má signál dále směrovat sítí k serveru.

Cílem a zároveň zdrojem GSM signálu měl být linuxový server, na kterém by byl nainstalovaný veškerý potřebný software, který by GSM signál generoval a zpracovával. Na výše zmíněné frekvenční omezení jsem narazil relativně pozdě, hlavě z toho důvodu, že jsem v LabView při vytváření programu frekvenci nijak nedefinoval, neměl jsem pro to důvod, frekvenci vysílání měl volit přislušný software na základě ARFCN. Až poté, kdy jsem ručně nastavil frekvenci na 800 MHz, a chtěl tak ověřit zda USRP vysílá, jsem zjistil, že je výstup daného zařízení omezen na již zmíněných 100 MHz. V tu chvíli mi tak bylo jasné, že s touto jednotkou nebude emulace GSM sítě možná. O tom, že dané rádio není pro GSM vhodné svědčí i fakt, že napříč celým internetem není jediná zmínka o použití NI PCI-5640R pro emulaci GSM sítě. To jsem však nebral jako důkaz toho, že realizace tohoto úkolu není možná a proto jsem i přes tento fakt v práci pokračoval. Bohužel ani v manuálu pro dané zařízení není o frekvenčním omezení žádná zmínka.

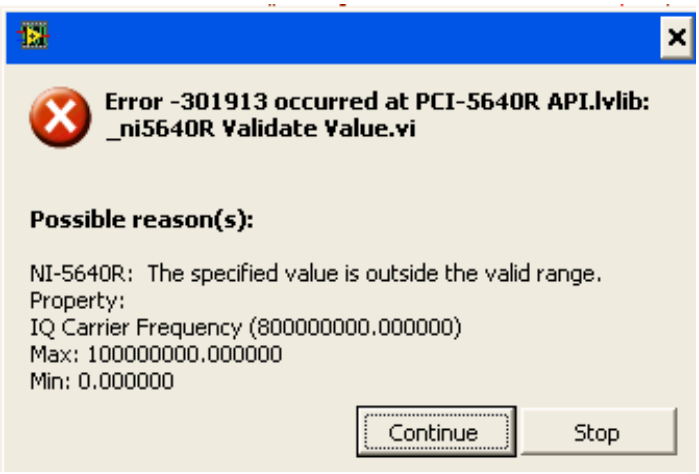
Díky tomuto omezení není USRP podporováno softwarem OpenBTS a není tak tedy možná ani instalace tohoto softwaru. Je potřeba ho instalovat na stroji, kde je USRP připojeno, protože s ním OpenBTS již při instalaci komunikuje, respektive je při instalaci nutné zadat parametr definující použité USRP.

Dvou počítačů na celou emulaci bylo potřeba, protože ovladače pro NI PCI-5640R jsou dostupné jen pro Windows. Musel jsem tak využít LabView jako mezičlánek pro definování IP adres potřebných pro komunikaci s linuxovým serverem. V LabView bych tak GSM signál vůbec nezpracovával a posílal ho pouze dál serveru pro zpracování.Pro lepší ilustraci uvádím následující obrázek.



Obrázek 4.1: Původně plánované zapojení všech komponent pro emulaci GSM sítě

USRP jednotku jsem nicméně využil jinak, abych ověřil její funkčnost a mohl ukázat její použití na jiném příkladu, i když sám vím, že jednodušším. Zvolil jsem spektrální analyzátor a následně FM demodulátor pro příjem veřejných rádiových stanic do frekvence 100 MHz. Vzhledem k frekvenčnímu omezení je to jedna z mála možností, jak toto USRP využít.



Obrázek 4.2: Chyba v LabView - nosná frekvence mimo povolený rozsah

4.2 Dostupné virtuální knihovny pro použitou kartu

Před ukázkou samotných programů považuji za vhodné krátce představit způsob programování v LabView a představit i knihovnu nástrojů, která je součástí ovladačů USRP.

Základní knihovnu pro PCI-5640R tvoří několik VI (Virtual Instrument). VI jsou jednotlivé funkční bloky, z kterých se skládá výsledný program. Každé VI se skládá z následujících komponent.

- Block Diagram
- Front Panel
- Connector Pane

Block Diagram je blokové schéma každého VI. Například u VI, které bude zesilovat signál, který přijde na vstup, bude blokové schéma tvořeno násobícím členem se vstupem pro signál a pro konstantu, která definuje, o kolik bude signál na výstupu zesílen.

Front Panel u výše popsaného VI může být tvořen posuvníkem, či textovým polem, které bude udávat velikost zesílení. Front Panel je tedy grafické rozhraní každého vytvořeného programu, po uložení projektu do spustitelného souboru je Front Pranel právě to, co se uživateli objeví na obrazovce po jeho spuštění.

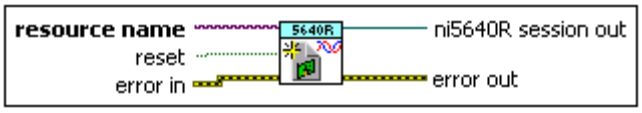
Connector Pane je schéma vstupů a výstupů každého VI. Výše popsaný program bude mít pouze jeden vstup (vstupní nezesílený signál), (eventuelně dva vstupy, druhý pro konstantu udávající zesílení) a jeden výstup (výstupní zesílený signál).

Poslední drobnou součástí každého VI je jeho ikona, kterou si uživatel může plně přizpůsobit.

Velmi často však mají VI více vstupů a výstupů, které přesně definují to, co daný blok dělá.

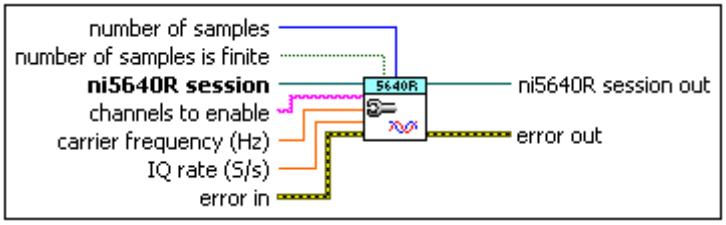
Následující výčet VI přímo určených pro použité USRP není kompletní, jedná se pouze o výběr tří nejdůležitějších součástí, které jsou potřeba znát před začátkem vytváření jakéhokoliv programu pro dané USRP.

- Ni5640R Init Acquistion Session



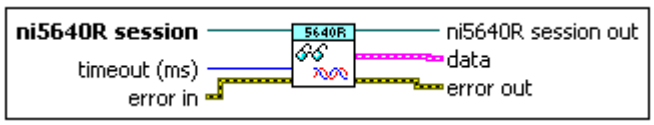
  - Jedná se o základní VI, které definuje, jaký fyzický vstup (resource name) bude USRP používat pro příjem. V mém případě používám jedinou možnou volbu – RIO0 (Reconfigurable I/O device). Existuje zároveň VI s opačnou funkcí, které definuje fyzický výstup pro vysílání signálu.

- Ni5640R Configure Acquisition VI



  - Toto VI nastavuje nutné parametry definující vlastnosti přijímaného signálu tak, jak potřebujeme. Základem je tedy nosná frekvence (Carrier frequency), používané kanály (channels to enable), obdoba vzorkovací frekvence IQ rate a počet vzorků, které chceme při spuštění přijmout. Po nastavení parametru number of sample is finite na hodnotu False probíhá příjem signálu nepřetržitě až do zastavení celého programu.

- Ni5640R Read IQ VI

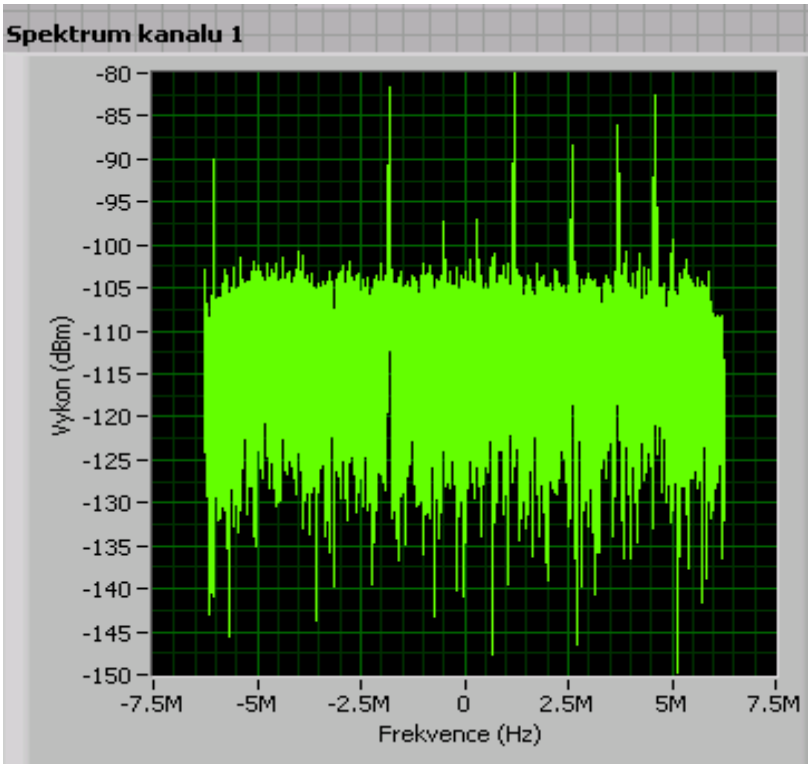


  - Důležité VI, bez kterého bychom nebyli schopni přijímat data k následnému zpracování. Na vstupu jsou údaje z výše uvedených VI, podle kterých toto VI zahájí sběr dat a na výstupu pak nalezneme pole prvků. To se skládá z prvku t0, tedy hodnoty kdy příjem signálu začal, prvku dt – časovým

rozestupem mezi jednotlivými vzorky signálu a prvku Y, který udává hodnotu (amplitudu) signálu v daném čase. Následnému zpracování se nekladou meze, v LabView je nespočetně možností jak a co s naměřeným signálem udělat.

4.3 USRP spektrální analyzátor

To, že USRP přijímá signál z okolí, jsem ověřil programem, kdy USRP funguje jako spektrální analyzátor. Z níže uvedeného obrázku je vidět, že jsou ve spektru výkonové špičky, které odpovídají jednotlivým rádiovým stanicím, nebo jiným systémům, které na frekvencích v okolí 90 MHz vysílají. Z hlediska rušení však můžeme předpokládat, že se skutečně jedná o rozhlasové stanice, tedy že toto frekvenční pásmo je vyhrazeno pro vysílání radiových stanic a ostatní tento fakt respektují. Dle plánu přidělení frekvenčních pásem, je pro rozhlasové vysílání přiděleno pásmo od 87,5 MHz do 108 MHz.

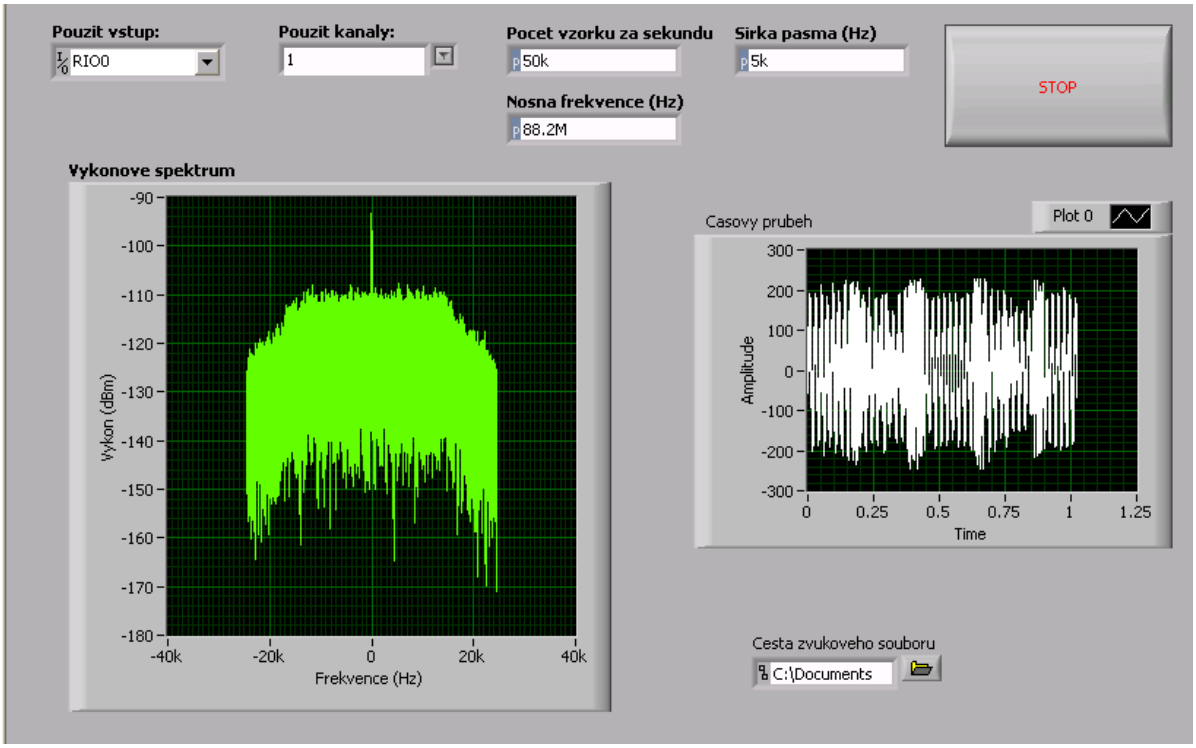


Obrázek 6: Získané spektrum; ve středu osy X je hodnota 90 MHz, spektrum je tedy pásma 82,5 MHz až 97,5 MHz

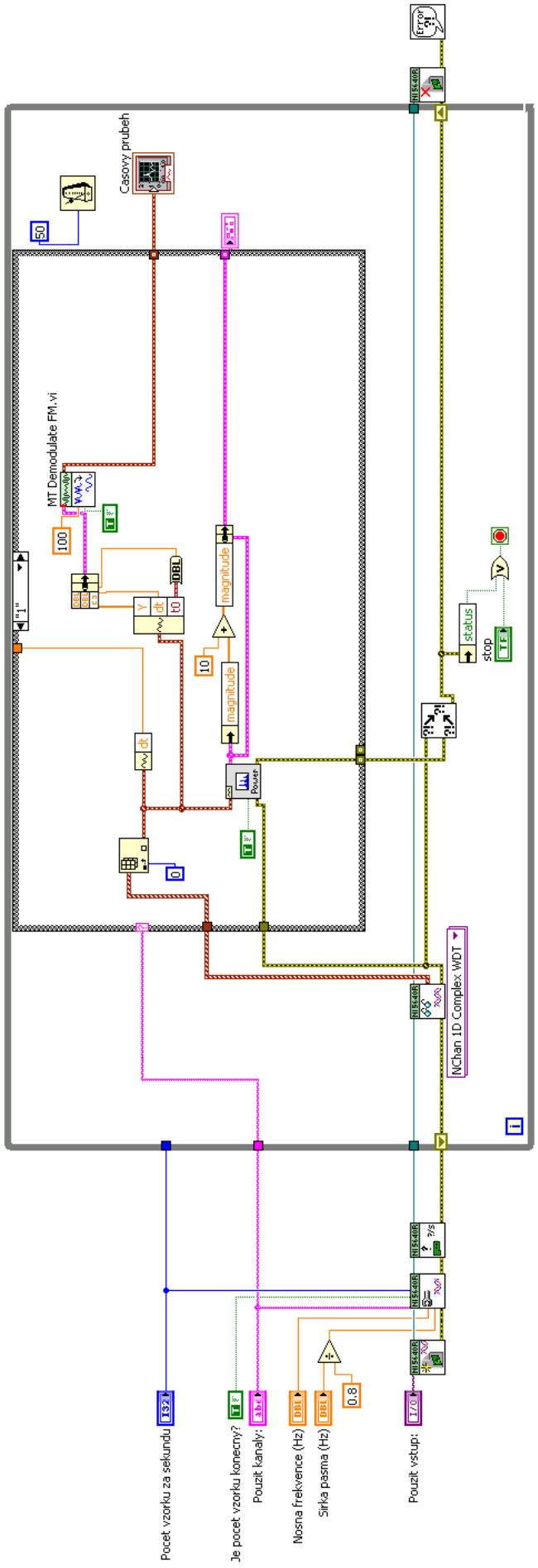
Důvodem relativně nízkého přijímaného výkonu bude pravděpodobně použitá anténa. Použil jsem obyčejnou anténu z WiFi routeru, s konektorem SMA a zanedbatelným ziskem, která je určena pro komunikaci v pásmu 2,4 GHz. Hodnoty RSSI dosahují hodnot v okolí -80 dBm, ale vzhledem k tomu, že FM signál má bitovou rychlost maximálně v řádu stovek kb/s, je i tato hodnota pro demodulaci, dle mého názoru, dostačující.

4.4 USRP FM přijímač

Pro demodulaci FM signálu již stačí použít VI *FM Demodulation*, které signál zpracuje a na jeho výstupu je poté časový průběh zvukového signálu. Ten jsem si však nemohl poslechnout, protože LabView nenašlo v počítači žádnou zvukovou kartu i po reinstalaci ovladačů. Nicméně z časového průběhu signálu, který je na obázku níže, bych odhadoval, že by se v něm nějaké zvuky nacházet měly, rozhodně průběh nevypadá jako šum. Blokové schéma tohoto programu je na následující straně.



Obrázek 4.4: Front Panel VI pro příjem FM signálu



Obrázek 4.5: Blokové schéma programu pro příjem a demodulaci FM signálu

Závěr

Je velká škoda, že USRP jednotka, která mi byla pro tuto práci zapůjčena, nepodporuje frekvenční pásmo, ve kterém pracuje systém GSM a nemohl jsem tak tedy celkovou emulaci sítě vyzkoušet prakticky. Bohužel jsem na začátku práce nepřemýšlel nad tím, zda je USRP pro GSM síť vhodné, bral jsem to totiž jako fakt a myslel jsem, že je tato funkčnost zaručena a že by jinak zadání této práce nevzniklo.

V práci jsem si tak mohl pouze vyzkoušet, jak se s těmito jednotkami pracuje, jak se programují a ovládají. Také jsem se seznámil s potřebným softwarem, který je pro emulaci GSM sítě potřebný. Dále jsem si v práci zopakoval a prohloubil znalosti o GSM sítích a v neposlední řadě se také naučil pracovat v prostředí LabView, které jsem doposud nikdy nepoužíval a viděl jsem ho jen na pár laboratorních cvičení v průběhu studia, kde sloužilo pro simulace.

Byl bych určitě rád, kdybych v budoucnu mohl v této práci pokračovat, ale s vhodným hardwarem, se kterým bych mohl realizovat vlastní GSM síť. Bohužel pro mě osobně USRP jednotky nejsou finančně dostupné, takže se s nimi budu moci setkat asi jedině v rámci dalších předmětů nebo diplomové práce.

Zdroje

[1] EBERSPÄCHER, J., H. VÖGEL, C. BETTSTETTER a C. HARTMANN. GSM: architecture, protocols and services [online]. 3rd ed., English lang. ed. Chichester, U.K.: Wiley, 2009, ix, 326 p. [cit. 2014-05-21]. ISBN 04-700-3070-4.

[2] ETSI. [online]. [cit. 2014-05-20]. Dostupné z: http://www.etsi.org/about

[3] GSMA. [online]. [cit. 2014-05-20]. Dostupné z: http://www.gsma.com/aboutus/

[4] About 3GPP. [online]. [cit. 2014-05-21]. Dostupné z: http://www.3gpp.org/about-3gpp

[5] Princip buňkového systému. *Technologie pro mobilní komunikaci* [online]. [cit. 2014-05-20]. Dostupné z: http://tomas.richtr.cz/mobil/bunk-princip.htm

[6] Logické kanály. *Technologie pro mobilní komunikaci* [online]. [cit. 2014-05-20]. Dostupné z: http://tomas.richtr.cz/mobil/gsm-log.htm

[7] . Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface. In: *ETSI - GSM 11.11* [online]. 1996 [cit. 2014-05-20]. Dostupné z:http://www.etsi.org/deliver/etsi_gts/11/1111/05.03.00_60/gsmts_1111v050300p.pdf

[8] Přidělená čísla a kódy - ČTÚ. [online]. [cit. 2014-05-21]. Dostupné z: http://www.ctu.cz/ctu-online/vyhledavaci-databaze/pridelena-cisla-a-kody.html?pageid=&order=&asc=&type=2&f_format_cisla=10&f_podnikatel=all&action=aktualni&date=31.12.2004

[9] Základní struktura sítě GSM. *Technologie pro mobilní komunikaci* [online]. [cit. 2014-05-20]. Dostupné z: http://tomas.richtr.cz/mobil/gsm-struktnss.htm

[10] Q.700 : Introduction to CCITT Signalling System No. 7. In: ITU [online]. [cit. 2014-05-21]. Dostupné z: http://www.itu.int/rec/T-REC-Q.700-199303-I/e

[11] Zabezpečení systému GSM proti zneužití. *Technologie pro mobilní komunikaci* [online]. [cit. 2014-05-20]. Dostupné z: http://tomas.richtr.cz/mobil/gsm-sec.htm

[12] What Is NI USRP?. [online]. [cit. 2014-05-21]. Dostupné z: http://www.ni.com/usrp/what-is/

[13] *OpenBTS* [online]. [cit. 2014-02-14]. Dostupné z: http://openbts.org/

[14] RANGE NETWORKS. *User Manual: OpenBTS Application Suite, Release 4.0* [online]. 2014 [cit. 2014-05-20]. Dostupné z: https://wush.net/trac/rangepublic/attachment/wiki/WikiStart/OpenBTS-4.0-Manual.pdf

[15] What Is LabView?. [online]. [cit. 2014-05-21]. Dostupné z: http://www.ni.com/newsletter/51141/en/

[16] NI PCI-5640R Specifications: Reconfigurable IF Transceiver. In: [online]. 2007 [cit. 2014-02-14]. Dostupné z: http://www.ni.com/pdf/manuals/371620c.pdf

[17] NI PCI-5640R: Software-Defined Radio IF Transceiver. In: [online]. [cit. 2014-02-14]. Dostupné z: http://sine.ni.com/nips/cds/view/p/lang/cs/nid/204022