Realizace rušičky mobilního telefonu s chaotickým oscilátorem

Realization of mobile phone jammer with chaotic oscillator

Bc. Petr Zikmund

Diplomová práce
2008

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektrotechniky a měření
akademický rok: 2007/2008

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Petr ZIKMUND**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Realizace rušičky mobilního telefonu s chaotickým oscilátorem**

Zásady pro vypracování:

1. **Nastudujte uspořádání rušičky mobilního telefonu s pilově rozmítaným generátorem.**
2. **Prakticky realizujte rušičku z bodu 1 a změřte její vlastnosti (kmitočtové spektrum a výstupní výkon). Zdroj rozmítacího pilového signálu a výstupní výkonový zesilovač realizujte vlastním návrhem v Eagle a výrobou příslušné DPS. Jako vlastní rozmítaný oscilátor použijte ZOS-1025 od fy. Minicircuits.**
3. **Navrhněte chaotický oscilátor s syntetickým členem se záporným diferenciálním odporem. Obvod vytvořte pomocí vhodných operačních zesilovačů. Proveďte simulaci chování oscilátoru v programu PSpice.**
4. **Chaotický oscilátor realizujte a změřte jeho vlastnosti (časový průběh výstupního napětí, spektrum)**
5. **Integrujte navržený chaotický oscilátor do rušičky z bodu 2 a porovnejte možnosti zarušení kmitočtového spektra s konstrukcí z bodu 2.**
6. **Na základě výsledků z bodu 5 diskutujte otázku rušení kmitočtového spektra s malým výkonem, cca. Desetiny wattu při zachování stejného dosahu jako u klasické rušičky z bodu 2.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

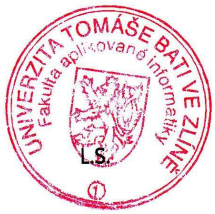
1. **Součástky pro elektrotechniku. Praha: GM electronic, 2004.**
2. **PSpice tutorials. URL:**
3. **Portable GSM900 Cellular Phone Jammer . URL:**
4. **RAUSCHER, C. Fundamentals of scpectrum analysi basics: 5th printing, Rohde-Schwarz. Munich. 2007. 219 s. ISBN 973-3-939837-01-5.**
5. **ELWAKIL A. S., KENNEDY M. P. Improved implementation of Chua's Chaotic Oscillator Using Current Feedback OP Amp. IEEE Trans.on.Circuits and Systems. Part I. Jan 2000, vol. 47, no. 1, s. 7679.**

Vedoucí diplomové práce: **Ing. Stanislav Goňa, Ph.D.**
Ústav elektrotechniky a měření

Datum zadání diplomové práce: **22. února 2008**

Termín odevzdání diplomové práce: **4. června 2008**

Ve Zlíně dne 22. února 2008



prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Tato práce seznámí čtenáře s problematikou rušení signálu pro mobilní telefony. Teoretická část se zabývá základním popisem struktury GSM sítě. Jejím úkolem není podrobný popis, ale pouze uvedení do tématu. Druhá kapitola teoretické části popisuje rušivé signály a jejich účinek na signály v základním pásmu a na modulované signály. V praktické části je popsána realizace samotné rušičky, její návrh, výroba, oživení a jednotlivá měření. Jsou přitom srovnány 2 případy, a to klasická GSM rušička s lineárním kmitočtovým rozmítáním a GSM rušička s rychlým kmitočtovým rozmítáním s využitím chaotického oscilátoru. Diskutuje se přitom možnost rušení s menším celkovým vyzářeným výkonem při stejném dosahu jaký má klasická rušička.

Klíčová slova: modulace GMSK, pomalé kmitočtové rozmítání, bílý šum, úzkopásmové rušení, rychlé kmitočtové přelaďování, chaotický signál.

ABSTRACT

This work introduces reader with problems of jamming signal of mobile phones. Theoretical part deals with basic description of a structure of a GSM network. Its purpose is not to give the detail, but make an introduction into the topic instead. Next subchapter mathematically describes jamming signals and their effect on base band and modulated signals. In practical parts, realization of a GSM jammer is described, specifically design, manufacture and several measurements are described. Two cases of GSM jammers are compared, namely classical GSM jammer with a linear frequency sweep and GSM jammer with a fast frequency sweep with utilizing a chaotic oscillator. A possibility of jamming with lower power if using jammer with chaotic oscillator is discussed and compared to a classical GSM jammer design.

Keywords: modulation GMSK, slow frequency sweep, white noise, narrowband jamming, fast frequency sweep, chaotic signal.

Děkuji svému vedoucímu bakalářské práce Ing. Stanislavu Goňovi, Ph. D. za ochotu, cenné rady a věcné připomínky, které mi během zpracování práce poskytl.

Prohlašuji, že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků, je-li to uvolněno na základě licenční smlouvy, budu uveden jako spoluautor.

Ve Zlíně …….

Podpis diplomanta

OBSAH

ÚVOD

Legislativa v České republice a zároveň i v Evropské Unii povoluje vysílání v pásmech GSM pouze provozovatelům mobilních sítí. V rozporu se zákonem je také vysílání v pásmech GSM za účelem zabránění komunikace. Rušičky GSM signálu lze použít pouze ve zvláštních případech, jako například rušení při policejních akcích nebo ve věznicích.

Princip rušení GSM signálu spočívá ve vysílání rušivých vln na stejných kmitočtech, jaké používají mobilní telefony. Signál pochází z generátoru sinusového průběhu, v našem případě trojúhelníkového, je smíchán se signálem šumovým. Tímto a přiváděným stejnosměrným napětím je naladěn VCO – napětím řízený oscilátor na požadované kmitočty. V našem případě pro pásmo 900 MHz se jedná o kmitočty v rozsahu 935 až 960 MHz, které jsou využívány pro vysílání základnových stanic.

Šumový signál způsobuje chyby v datovém toku a narušuje tak signál digitální, po rozkmitání digitálního signálu dochází k chybám při rozpoznávání úrovní napětí a tedy i k neurčitosti mezi hodnotami pro logickou nulu nebo jedničku.

Sítě GSM používají pro přenos dat speciální modulaci signálu – GMSK (gaussian minimum shift keying) . Jedná se o druh digitální fázové modulace, která je velmi odolná proti rušení ve srovnání s ostatníma.

Dosah rušičky se může lišit, záleží na výkonu základové stanice sítě GSM. Pokud je signál vysílaný stanicí slabý, dosah rušičky se zvyšuje.

Úkolem diplomové práce je vytvořit rušičku s co nejmenším vyzářeným výkonem. Denně jsme totiž vystaveni různým rádiovým signálům napříč kmitočtovým spektrem. Jak je známo, o účincích vln šířených hlavně v kmitočtech používaných mobilními telefony se vedou neustálé diskuze.

I. TEORETICKÁ ČÁST

1 GSM SÍŤ

1.1 Historie GSM

Začátkem osmdesátých let svět zaznamenal rychlý růst analogových celulárních (buňkových) systémů v Evropě, především pak ve Skandinávii, Velké Británii, Francii a Německu. Každá země měla vyvinutý svůj systém, který však byl neslučitelný s jakýmkoliv jiným systémem celulární komunikace. Tato situace byla neudržitelná nejenom z důvodu nepoužitelnosti zařízení za hranicemi země, které ve sjednocující se Evropě ztrácely na významu, ale také z důvodu velmi omezeného trhu pro jednotlivé typy zařízení, což s sebou přinášelo ekonomické problémy. Proto Konference evropských správ a pošt CEPT vytvořila v roce 1982 novou standardizační skupinu GSM (Groupe Spécial Mobile), která měla za úkol vytvořit standardy pro nový digitální systém, který by byl kompatibilní v zemích celé Evropy (světa).

Navrhnutý systém musel splňovat určitá kritéria :

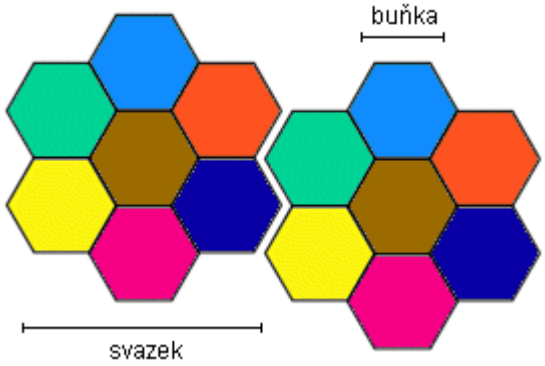
- Perfektní subjektivní kvalita přenášené řeči
- Nízká cena vybavení a služeb
- Podpora mezinárodního roamingu
- Frekvenční hospodárnost
- ISDN slučitelnost
- Efektivitu v budoucnosti

V roce 1989 byla odpovědnost za standardizaci tohoto systému přesunuta na Evropský telekomunikační normalizační institut (ETSI) a v roce 1990 byla specifikace fáze 1 sítě GSM prohlášena standardem.

Komerční provoz první GSM sítě byl zahájen v polovině roku 1991 a již v roce 1993 existovalo 36 GSM sítí v 22 zemích. Ačkoliv byl standardizován v Evropě, GSM není jen evropský standard, ale například i Jižní Afrika, Austrálie a mnoho dalších zemí středního a dálného východu zvolily z hlediska kompatibility tento systém. S jistým zpožděním použili tuto technologii i v USA, kde pod názvem PCS 1900 pracuje na odlišných frekvencích. Systém GSM tak existuje na všech kontinentech a zkratka GSM je interpretována jako "Global System for Mobile Communication", tedy "Globální systém pro mobilní komunikaci". Analogové buňkové systémy jako například AMPS v USA nebo TACS ve Velké Británii začaly pomalu upadat a v současné době je systém GSM velice rozšířeným mobilním komunikačním prostředkem. V České republice byl systém GSM spuštěn v roce 1996 společností Eurotel a dále následován společnostmi Radiomobil a Český mobil. [1]

1.2 Buňková struktura sítě GSM

Jak již bylo zmíněno, princip GSM sítě spočívá v rozdělení území na jednotlivé buňky které jsou pokrývány signálem. Následující obrázek znázorňuje právě princip buňkové struktury.



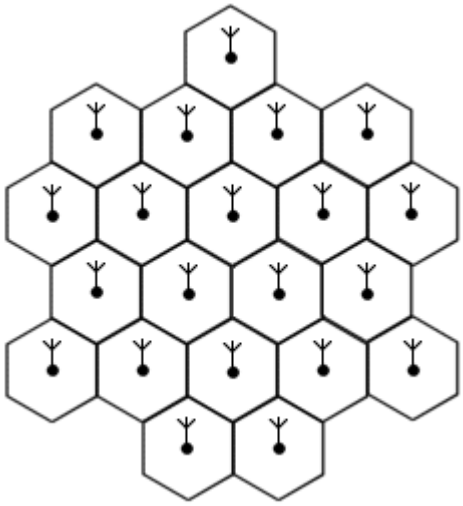
Obr. 1. Buňková struktura [1]

Území které je třeba pokrýt signálem je rozděleno na 14 šestiúhelníkových buněk, které tvoří dva svazky (clusters) po sedmi buňkách. Dalším přidáváním svazků je potom možno pokrýt neomezeně velké území. Uvnitř každé buňky je jedna základnová stanice s určitou

přidělenou skupinou kanálů a komunikující s mobilními účastníky, kteří se nacházejí pouze v této buňce. Zbývajících šest buněk příslušejících jednomu svazku má přiděleny své skupiny kanálů.

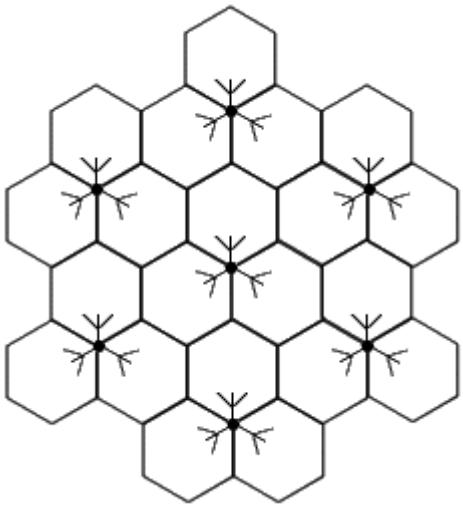
Výhody tohoto systému jsou zejména efektivní hospodaření s přiděleným radiovým spektrem a tzv. handover, tj. automatické přelaďování stanic při přechodu mezi jednotlivými buňkami.

Pro vytvoření sítě s lepšími provozními vlastnostmi (např. nižší vysílací výkony a zvětšení počtu současně obsluhovaných mobilních stanic) je možno použít princip tzv. sektorizace. Jeden svazek je rozdělen na 21 menších buněk.



Obr. 2. Sektorizace buněk [1]

Nezmění se tím počet potřebných kanálů, ale stoupne počet základnových stanic ze 7 na 21. Jejich počet však lze sektorizací redukovat na sedm umístěním tří samostatných směrových antén do společných bodů tří sousedních buněk. [1]



Obr. 3. Sektorizace buněk se směrovými anténami [1]

To zvyšuje provozní kapacitu základnové stanice (každá frekvence může obsahovat osm hlasových kanálů) zatímco moc nezvýší rušení způsobené na sousední buňky (v každém směru se šíří jen malý počet frekvencí).

Buňky jsou dále rozdělovány podle dosahu i možnosti umístění:

- Makrobuňka je klasickým příkladem standardní základnové stanice. Má dosah až 35 km. Dříve se na stožár základnové stanice dával pouze jeden vysílač, nyní kvůli zvýšení kapacity obsahuje stožár vysílače makrocell až tři vysílače, které mají vysílací úhel 120°. Pokud je použito na stožáru tří směrových vysílačů, obsahuje jeden stožár tři makrocelly (a podobně u dvou či jedné);

- Mikrobuňka je vysílač mnohem menší jak rozměrově, tak svým dosahem. Obecně se používá jedné antény s vyzařovacím úhlem 360°, která má ovšem dosah pouze 27 km. Mikrobuňky se používají na vykrytí „problematických“ částí. (vnitřek budov, nebo například metro);

- Deštníková buňka je kombinací předchozích dvou typů. Jelikož mikrobuňky nemohou zajistit úplné pokrytí určitého prostoru, používá se na překrytí „hluchých

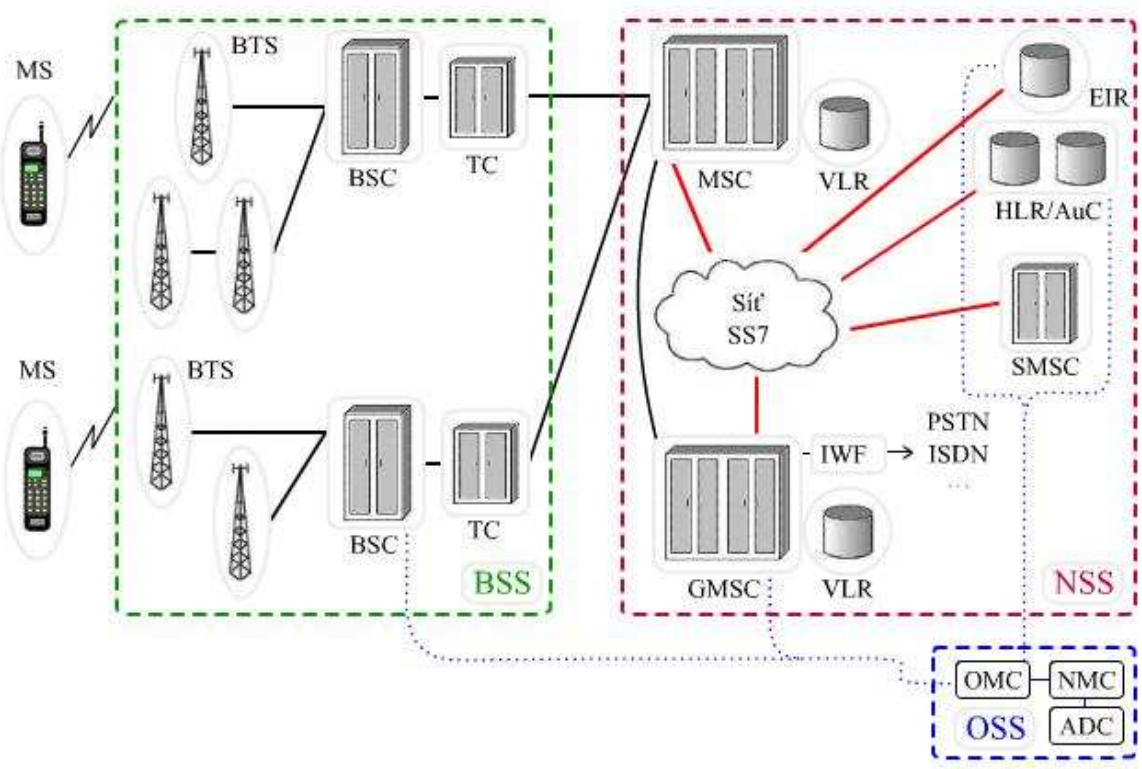
míst“ obvykle jeden vysílač typu makro cell (s dosahem max. 35 km) a vyzařovacím úhlem 360°. [2]

- Pikobuňka se používá uvnitř budov a v místech s vysokou koncentrací osob. Její dosah bývá zpravidla několik desítek metrů.

1.3 Subsystémy GSM

Celkový systém GSM je rozdělen na 3 subsystémy:

- subsystém základových stanic BSS (Base Station Sub-System);
- síťový přepojovací (spínací) subsystém NSS (Network Switching Subsystem);
- operační podpůrný subsystém OSS (Operation Support Subsystem).



Obr. 4. Systém GSM [1]

1.3.1 Subsystém základových stanic BSS

Základními stavebními prvky subsystému BBS jsou následující zařízení:

- Základnové stanice BTS (Base Transceiver Station)
- Základnová řídicí jednotka BSC (Base Station Controller)
- Transkodér TC (TransCoder)

V systému GSM obvykle obsahuje jeden svazek 9 buněk, používají se však i svazky s menším počtem buněk. Uvnitř každé buňky je umístěna základnová stanice (není-li využito principu sektorizace), která zajišťuje komunikaci s mobilní stanicí. Tato komunikace probíhá přes rádiové rozhraní (Air interface), označované jako rozhraní Um nebo I/F. Několik základnových stanic je společně řízeno jedinou základnovou řídicí jednotkou BSC. Jednotlivé BTS mohou spolu s BSC vytvářet hvězdicovou, kaskádní, stromovou i jinou topologii. Základnové stanice se dělí do osmi výkonových tříd s výkony 2,5; 5; 10; 20; 40; 80;1 60; 320 Wattů a komunikace s BSC je často realizována radioreléovými spoji. Stejně jako v případě komunikace BSC - MSC však může být použito optického nebo metalického vedení. Základnové řídicí jednotky BSC výrazně odlehčují ústředně MSC tím, že vykonávají funkce handoveru (v systému GSM typu MAHO), přidělování kanálů (dynamické) a částečně také plní funkce přepojovací. Mezi BTS a BSC se nachází rozhraní Abis. Na rádiovém rozhraní (Um) má telefonní kanál přenosovou rychlost 13 kbit/s, na rozhraní Abis již 16kbit/s. Rozhraní mezi základnovou řídicí jednotkou a ústřednou MSC se nazývá rozhraní A. Mobilní ústředna však z důvodu kompatibility s externími sítěmi používá telefonní kanály s rychlostmi 64 kbit/s. Proto je nutností zařadit mezi BSC a MSC transkódovací jednotku TC (TransCoder), která má na starost přizpůsobení rychlostí. Tato jednotka může být umístěna jednak na straně BSC nebo na straně MSC, což je z ekonomických důvodů výhodnější. [1]

1.3.2 Síťový spojovací subsystém - NSS

Základními stavebními prvky subsystému NSS jsou následující zařízení:

- Mobilní radiotelefonní ústředna MSC (Mobile Switching Centre)
- Domovský lokační registr HLR (Home Location Register)
- Návštěvnický lokační registr VLR (Visitor Location Register)
- Centrum autentičnosti AuC (Authentication Centre)
- Identifikační registr mobilních stanic EIR (Equipment Identity Register)
- Jednotkou spolupráce s externími sítěmi IWF (Inter-Working Functionality)
- SMS Centrum

Síťový spojovací subsystém plní v systému GSM především spojovací funkce, obdobně jako je uskutečňuje klasická telefonní ústředna. Tuto funkci plní v subsystému NSS mobilní radiotelefonní ústředna MSC. Jde zde o běžný typ telefonní ústředny, která je však doplněna o další funkce plynoucí z mobility přepojovaných účastnických stanic. Tato ústředna je nadřazena nad systémem řadičů BSC a jedna nebo více z nich plní funkci tzv. Gateway MSC a umožňuje propojení mobilní sítě GSM s externími telekomunikačními sítěmi, fixními nebo mobilními. Za tímto účelem je potřeba ústřednu vybavit jednotkou spolupráce s externími sítěmi IWF (Inter-Working Functionality)

Subsystém NSS dále realizuje celou řadu specifických úloh, spojených s mobilitou účastníků. Součástí každé sítě GSM je domovský lokační registr HLR, což je v podstatě hlavní databáze, ve které jsou uložena veškerá důležitá data o uživatelích sítě. Obsahuje důležitá čísla IMSI (International Mobile Subscriber Identity), MSISDN (Mobile Subscriber ISDN Number), zpřístupněné služby a dále například údaje týkající se polohy uživatele. V síti jednoho operátora je vždy minimálně jeden HLR, může jich být i více. Součástí registru HLR je i centrum autentičnosti AuC (Authentication Centre), což je chráněná databáze, obsahující klíče pro ověřování totožnosti účastníků. 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.

Na registr je dále napojen identifikační registr mobilních stanic EIR. V této databázi jsou uložena čísla IMEI (International Mobile Equipment Identity) mobilních stanic, které jsou autorizovány k použití v dané síti, dále čísla ukradených MS a je zde i seznam stanic, které jsou označeny jako porouchané, případně nesplňující určitá požadovaná specifika. Velmi důležitou roli hraje také návštěvnický lokační registr VLR, který přechodně uchovává a obnovuje data o uživatelích, v dané chvíli se nacházejících v oblasti příslušné MSC. Obsahuje podobné informace jako HLR , ale pouze dočasně, tzn. že jakmile účastník opustí oblast, data jsou vymazána.

K přenosu signalizace mezi jednotlivými zařízeními je použita signalizační síť SS7 a jsou definovány následující rozhraní:

- B mezi MSC a VLR
- C mezi MCS a HLR
- D mezi registry VLR A HLR
- E mezi dvěma ústřednami MSC
- F mezi MSC a EIR
- G mezi HLR a AuC [1]

1.3.3 Operační a podpůrný subsystém - OSS

Základními stavebními prvky subsystému OSS jsou následující zařízení:

- Provozní a servisní centrum OMC (Operational and Maintenance Centre)
- Centrum pro řízení sítě NMC (Network Management Centre)
- Administrativní centrum ADC (Administrative Centre)

Tento subsystém provádí zejména následující základní funkce:

- Podílí se na managementu mobilních stanic, tyto stanice monitoruje a eviduje porouchané

- Dohled a konfigurace sítě
- Provádí kontrolu a údržbu systému GSM
- Podílí se na administrativním managementu účastníků GSM, konkrétně jejich registraci, tarifikaci [1]

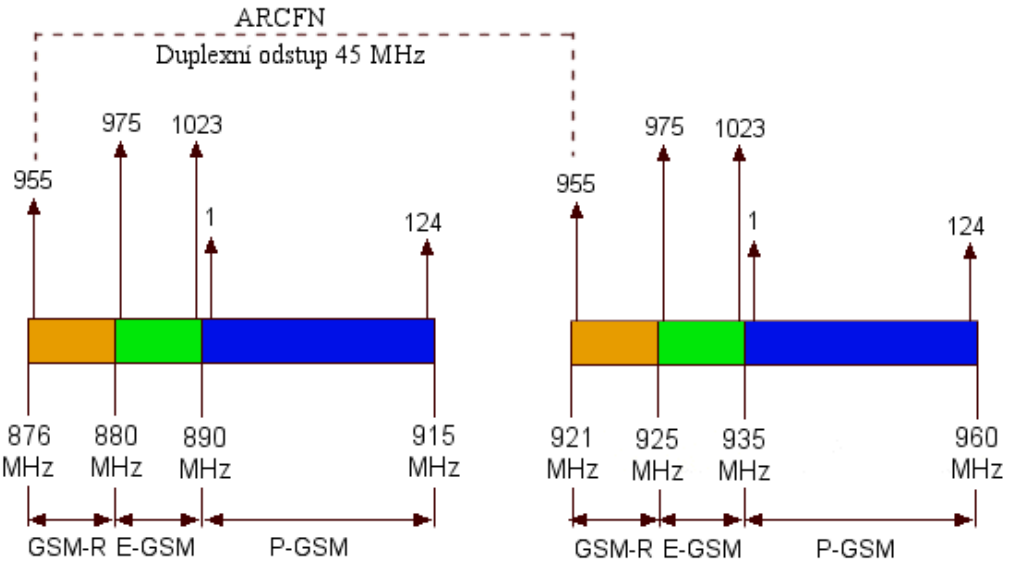
1.3.4 Mobilní stanice MS

Samostatnou skupinu tvoří mobilní stanice. Většinou se do jednotlivých subsystémů neuvádí. Podle specifikací GSM se mobilní stanicí rozumí jednak vlastní přijímač/vysílač (označovaný také jako mobilní uživatelská či účastnická stanice, nebo terminál resp. transceiver) a také předplatitelský identifikační modul resp. karta SIM (Subscriber Identification Module), pomocí kterého je účastník identifikován v síti. Každá mobilní stanice je identifikována číslem IMEI (International Mobile Equipment). Každá SIM karta má jedinečné identifikační číslo IMSI (International Mobile Subscriber Identity).

1.4 Radiové rozhraní systému GSM

Systém GSM má vyhrazena dvě rádiová pásma o šířce 2x25 MHz. Pro vzestupnou trasu (vysílají mobilní stanice) je to 890-915 MHz a pro trasu sestupnou (vysílaji základnové stanice) je to 935-960 MHz. Systém poskytuje plně duplexní provoz ve formě frekvenčního duplexu FDD s duplexním odstupem 45 MHz. Nosné vlny mají vzájemný odstup 200 kHz, takže v pásmu 25 MHz je jich celkem 125. Kanál č. 0 je oddělovací a nepoužívá se pro přenos hovorů, využitelných je tedy 124 duplexních kanálů. Každá dvojice uplink/downlink je potom označena absolutním číslem rádiového frekvenčního kanálu ARFCN (Absolute Radio Frequency Channel Number). U systému GSM nabývá ARFCN hodnot 1-124. Kapacita frekvenčního pásma v oblasti 900 MHz se ukázala nedostačující a proto bylo rozhodnuto o použití dalších kmitočtových pásem. Vznikl tak systém nazývaný

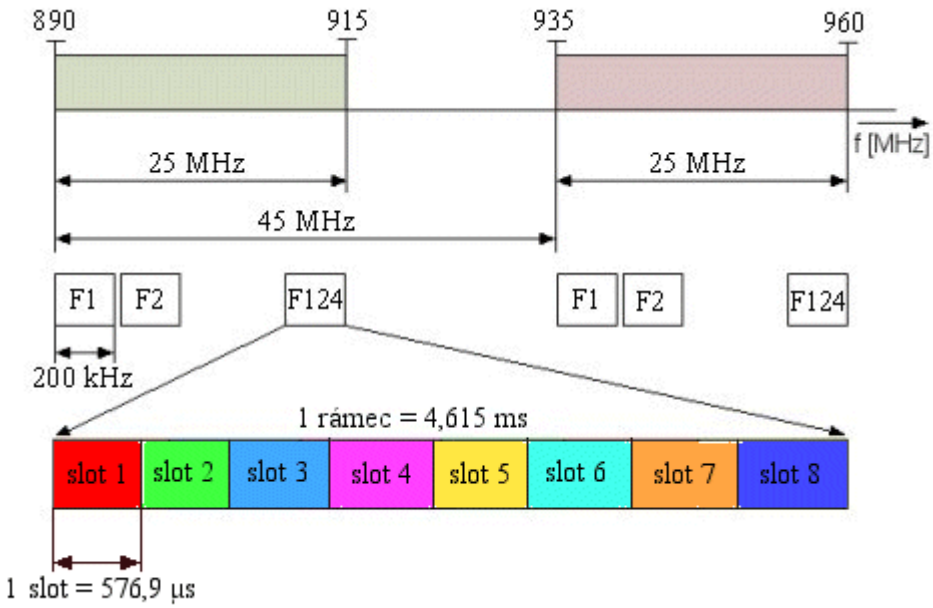
GSM 1800 (DCS 1800), který je založen na standardech GSM a je koncipován pro nasazení v buňkách malých rozměrů. Liší se především v použitém kmitočtovém pásmu (1710-1785/1805-1880), které poskytuje kapacitu 375 rádiových kanálů (ARCFN 512-885). Šířka přiděleného pásma je tedy 75 MHz a duplexní odstup 95 MHz. V USA je systému PCS 1900 (DCS 1900, GSM 1900) přiděleno pásmo 1850-1910/1930-1990, což znamená že šířka pásma je 60 MHz a odstup 80 MHz. Použít lze 300 rádiových (ARFCN 512 -810) a 2400 uživatelských kanálů. Dále vznikla novější varianta GSM, označená E-GSM (Extended-GSM), kde je rozšířeno frekvenční pásmo standardní P-GSM (Primary-GSM) na 880-915/925-960 MHz (ARFCN jako u P-GSM a navíc 975-1023) a zmínit je třeba i variantu GSM-R (Railway GSM), kterou odsouhlasili provozovatelé železnic jako jednotný komunikační systém pro použití v železniční dopravě. Pro tuto službu ETSI vymezila pásmo 876-880/921-925 MHz (odpovídá ARCFN 955-974).



Obr. 5. Radiové rozhraní GSM [1]

Na každém rádiovém kanálu je metodou TDMA vytvořeno 8 časových slotů, přičemž každý interval představuje 1 uživatelský kanál. Celkem je tedy u standardního systému GSM 900 k dispozici 8 x 124 = 992 duplexních kanálů (3000 u varianty GSM 1800). To ovšem platí při zdrojovém kódování "plnou rychlostí", tzv. full rate. Zavedením dokonalejšího a účinnějšího zdrojového kódování half rate je potom možno docílit přenosu

16 hovorových kanálů na jedné nosné vlně. Uvedený způsob přenosu s kombinovaným frekvenčním a časovým multiplexem se pak označuje zkratkou FDMA/TDMA.



Obr. 6. Metoda TDMA [1]

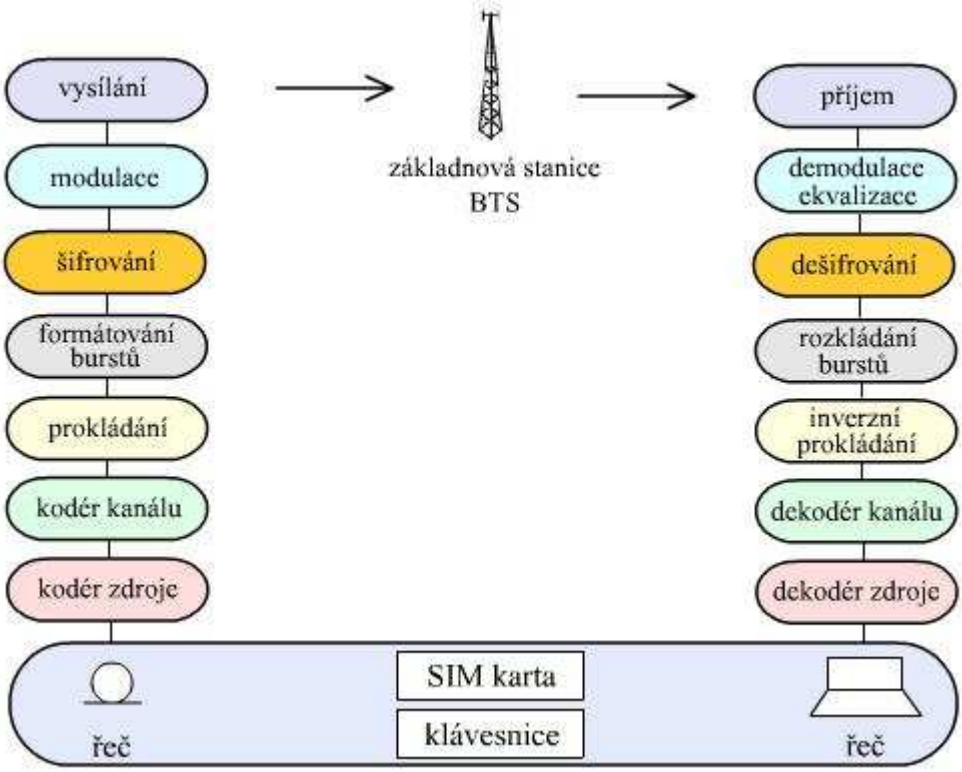
Každý digitalizovaný hovorový kanál má po zakódování v kodéru zdroje přenosovou rychlost 13 kbit/s. Ta se dále po přidání ochranných bitů, prováděném při kanálovém kódování, zvýší na 22,8 kbit/s. Sdružením takových osmi kanálů a přidáním dalších pomocných a signalizačních bitů dojdeme k celkové přenosové rychlosti signálu připadajícího na jednu frekvenci o hodnotě 270,883 kbit/s. Odpovídající perioda jednoho bitu je potom 3,692 µs a efektivní přenosová rychlost na jeden kanál 33,854 kbit/s. Jako optimální modulační metoda byla vybrána pro systém GSM gaussovská modulace MSK, tj. GMSK s normovanou šířkou pásma předmodulační gaussovské dolní propusti B x T = 0,3.

Odolnost proti selektivnímu úniku je zajištěna tzv. ekvalizací. Při ekvalizaci je do přenosového řetězce na straně přijímače zařazen filtr, který kompenzuje vlastnosti přenosového kanálu na přijímací straně. Proto je v každém slotu vysílána tréninková posloupnost (známá posloupnost bitů) a v přijímači se deformovaný signál porovná se správným signálem a podle výsledku se nastaví parametry ekvalizačního filtru. Ekvalizace je málo účinná v prostředích, kde vznikají dlouhé výpadky signálu a proto základnová

stanice v každém časovém slotu mění kmitočet komunikace (mobilní stanice se jí přizpůsobují). Použitá ekvalizace spolu se strukturou rámců umožňuje používat mobilní stanice až do rychlosti 250 km/h, což je i maximální rychlost pro úspěšný handover. Mobilní stanice neustále sleduje kvalitu rádiových kanálů nejen z hlediska intenzity signálu ale také z hlediska bitové chybovosti BER. Měří se až 6 sousedních základnových stanic a na základě těchto údajů BSC nebo MSC rozhoduje o handoveru.

1.5 Zpracování signálu

Na následujícím obrázku jsou schematicky znázorněny funkce uskutečňující se ve vysílači a v přijímači mobilní stanice. Princip zde použitý je v podstatě shodný s principem použitým v jakýmkoliv jiném digitálním rádiovém komunikačním systému.

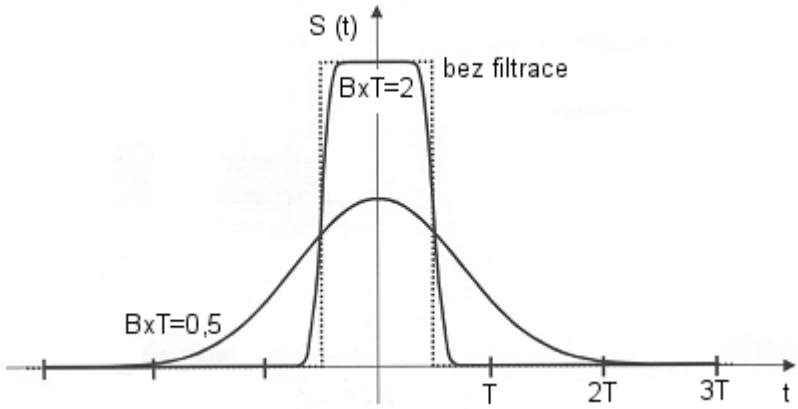


Obr. 7. Blokové schéma zpracování signálu [1]

Na vstup vysílací části mobilní stanice přichází z mikrofonu analogový elektroakustický (hovorový) signál. Ten je nejprve v kodéru zdroje signálu digitalizován a zbavován redundance, čímž se výrazně snižuje jeho bitová rychlost. V následujícím kodéru je zvětšována jeho imunita vůči rušivým vlivům, působícím v pozemském rádiovém kanálu. Zakódovaný signál je poté podroben prokládání (interleaving) a dále se uskutečňuje formátování burstů. Následuje proces šifrování a takto upraveným signálem se poté v modulátoru moduluje nosná vlna. Modulovaný signál je po frekvenční transpozici a výkonovém zesílení vysílán. Na přijímací straně probíhá tentýž proces v obráceném pořadí, navíc je do řetězce zapojen proces ekvalizace. [1]

1.5.1 Modulace a demodulace

Zakódovaný digitální modulační signál se přivádí do modulátoru vysílače, kde se jím moduluje nosná vlna. Pro radiotelefonní systém GSM byla jako nejvhodnější modulační metoda vybrána gaussovská modulace s minimálním zdvihem, značená zkratkou GMSK (Gaussian Minimum Shift Keying). Jedná se o upravenou variantu modulace MSK. Signál modulovaný metodou MSK zaujímá relativně malé kmitočtové pásmo, zůstává však nepříjemné vyzařování do sousedních pásem, které lze odstranit filtrací. Provádí se tedy předfiltrace datového signálu pomocí gaussovské dolní propusti, odtud pochází název této modulace. Protože časový průběh filtrovaného signálu neobsahuje skokové změny, nemění se skokově ani vysílaný kmitočet. U této modulace je důležitý modulační index (B x T), což je součin šířky pásma gaussovské propusti a doby trvání bitu. Pro malé hodnoty modulačního indexu klesají postranní laloky ale roste mezisymbolová interference, pro velké hodnoty je tomu naopak.



Obr. 8. Průběh GMSK [1]

Dvě sousední nosné vlny mají v systému GSM odstup 200 kHz, přičemž každá z nich přenáší 8 nezávislých účastnických kanálů sdružených metodou TDMA. Jeden kanál však nevyužívá v průběhu hovoru jednu a tutéž frekvenci, ale v určitých časových intervalech "přeskakuje" mezi více nosnými frekvencemi. Systém GSM tedy používá pomalé frekvenční skoky SFH (Slow Frequency Hopping). Pomalé frekvenční skoky tak přinášejí dvě hlavní výhody.

- Frekvenční diverzita: Pomáhá redukovat ztráty rádiového spojení v oblastech s rychlým Rayleighovým únikem.
- Interferenční diverzita: Zvyšuje účinnost metody opětovného využití frekvencí rádiových kanálů.

Pro správné fungování multiplexu TDMA je nutné, aby jednotlivé bursty používající sousední časové intervaly dospěly k základnové stanici ve správném čase a nedocházelo tak k překrývání, které vede k nárůstu chybovosti. Závažnost tohoto problému narůstá v okamžiku, kdy je mobilní stanice vzdálena od základnové stanice natolik, že nelze zanedbat dobu šíření rádiových vln. V klidovém stavu je mobilním stanice na příjmu, sleduje návěstní kanál (příchozí hovory) a její časování je oproti časování základnové stanice posunuto. V případě komunikace (odchozí nebo příchozí hovor) požádá pomocí přístupového burstu o přidělení řídicího kanálu. Přístupový burst má prodlouženou

ochrannou dobu (252 ms) a umožňuje komunikaci na 37,8 km. Základnová stanice změří zpoždění příchozího signálu a spočítá parametr TA (Timing Advance, "předstih"), který pošle mobilní stanici. Mobilní stanic tento parametr používá tak, že signál vysílá v předstihu, daném právě tímto parametrem, který může nabývat hodnot 0 bitů (mobilní stanice velmi blízko u základnové stanice) až 63 bitů. Mobilní stanice tedy nevysílá přesně po uplynutí 3 časových intervalů od příjmu (3 x 165,25 bitů), ale po době kratší (3 x 165,25 - TA bitů). Z tohoto plyne i dosah systému GSM 35 km. Tohoto parametru lze využít i pro lokalizaci mobilní stanice, kdy je pomocí TA určena přibližná vzdálenost mobilní stanice od základnové a v případě porovnání výsledků od více základnových stanic lze dojí k poměrně kvalitnímu určení polohy mobilní stanice. [1]

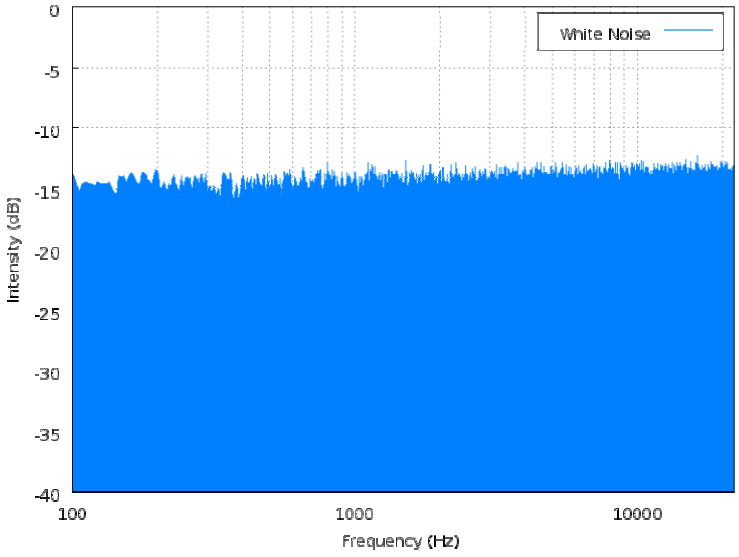
2 RUŠENÍ A RUŠIVÉ SIGNÁLY

2.1 Obdélníkový signál rušený Gaussovým šumem

Gaussův šum je nazýván také jako bílý šum. Bílý šum je náhodný signál s rovnoměrnou výkonovou spektrální hustotou. Signál má stejný výkon v jakémkoli pásmu shodné šířky. Například pásmo široké 20 Hz mezi 40 a 60 Hz má stejný výkon jako pásmo mezi 4000 a 4020 Hz. Bílý šum je tak nazýván jako analogie s bílým světlem, které obsahuje všechny frekvence. Nekonečný frekvenční rozsah signálu bílého šumu je pouze teoretický. Kdyby byl nenulový výkon na všech frekvencích, celkový výkon takového signálu by byl nekonečný. V praxi je signál „bílý“ pokud má ploché spektrum v definovaném rozsahu frekvencí. [3] Pro popis jednotlivých šumů se používá teorie pravděpodobnosti. Bílý šum je šum, jehož pravděpodobnost výskytu je stejná pro všechny frekvence. Pravděpodobnost výskytu Gaussova šumu se určuje dle vztahu

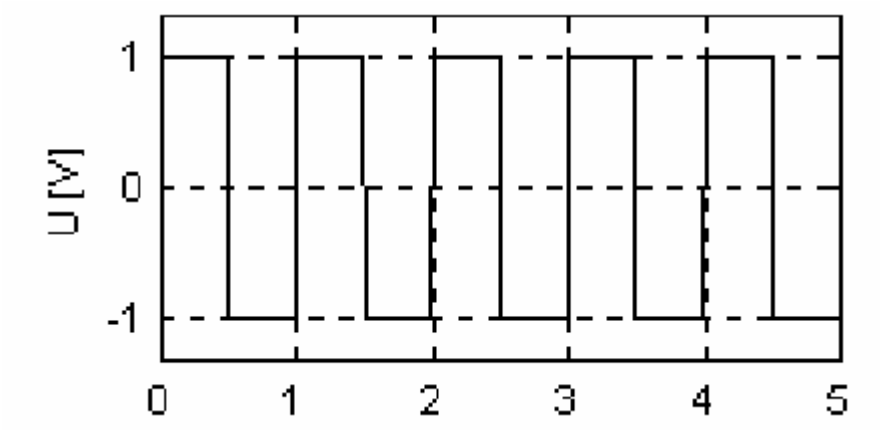
$$G_\sigma(x) = \frac{1}{2\pi\sigma^2} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

Kde μ je střední hodnota a σ je střední kvadratická odchylka. Znázornění spektra bílého šumu je na následujícím obrázku.

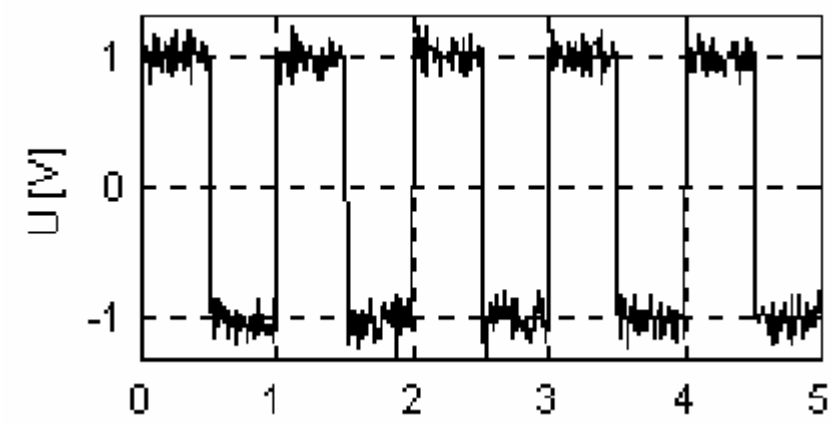


Obr. 9. Spektrum bílého šumu [4]

Na prvním obrázku je znázorněn signál obdélníkového průběhu, na dalším signál stejný, ale po vlivu šumu.



Obr. 10. Obdélníkový signál [5]

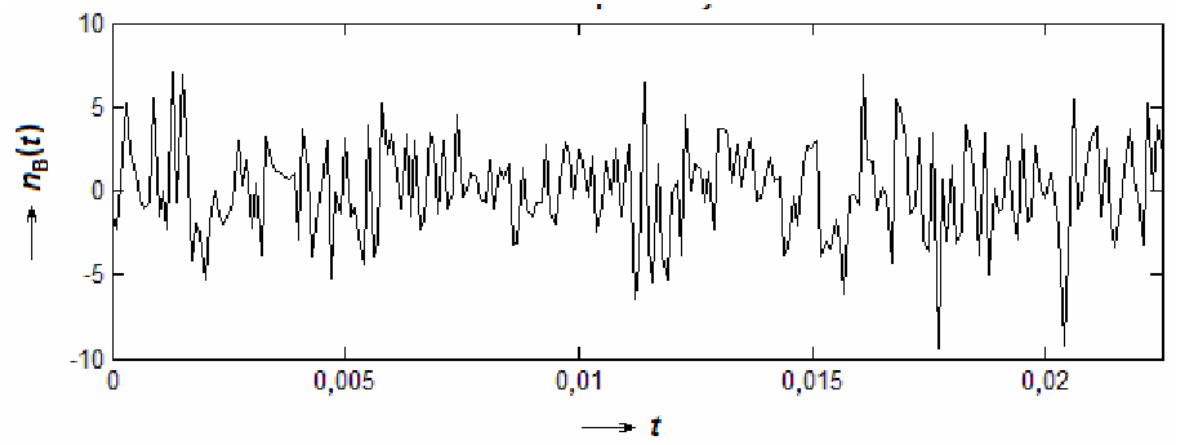


Obr. 11. Obdélníkový signál po zašumění [5]

Šumivý signál narušuje harmonický průběh signálu obdélníkového. V našem případě znázorňuje digitální průběh signál GSM. Šum narušuje datový tok. Pokud se pohybuje v rozmezích napětí stanovených pro logické 0 i 1, není potom jasné o jakou hodnotu se jedná a dochází k chybám v přenosu, tudíž i k rušení signálu.

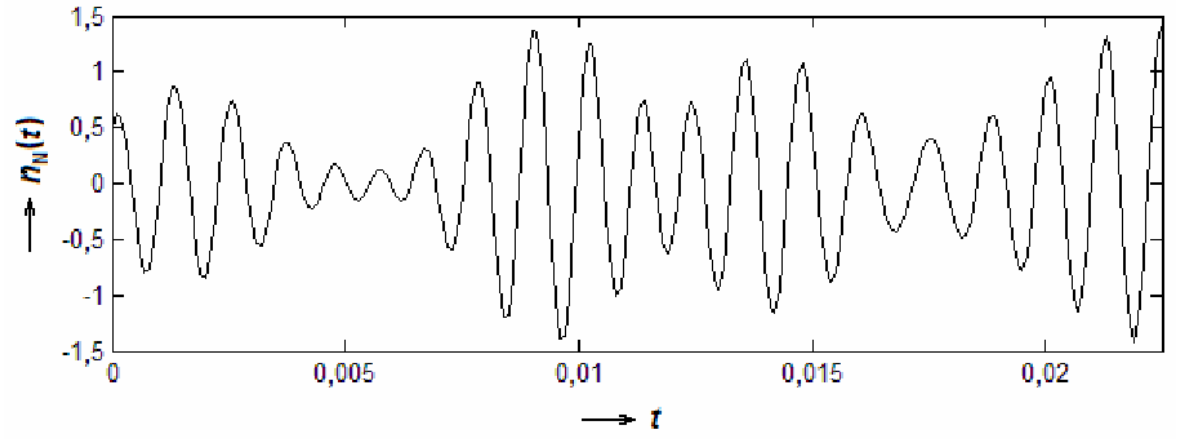
2.2 Úzkopásmový šum

Úzkopásmový šum je ve své podstatě širokopásmový šum po průchodu pásmovou propustí. Signál, kde B je šířka pásma a f kmitočet, pro který platí, že $\frac{B}{f} << 1$, je považován za úzkopásmový.



Obr. 12. Širokopásmový šum [6]

Příklad úzkopásmového šumu.



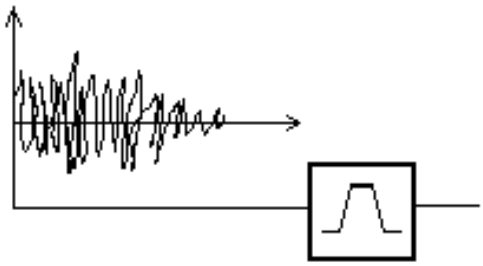
Obr. 13. Úzkopásmový šum [6]

Kvadraturní vyjádření úzkopásmového šumu:

$$v(t) = A_V(t)\cos[\varpi_C t + \varphi_V(t)] = A_V(t)\cos\varphi_V(t)\cos\varpi_C t - A_V(t)\sin\varphi_V(t)\sin\varpi_C t$$
$$v(t) = v_C(t)\cos\varpi_C t - v_S(t)\sin\varpi_C t$$

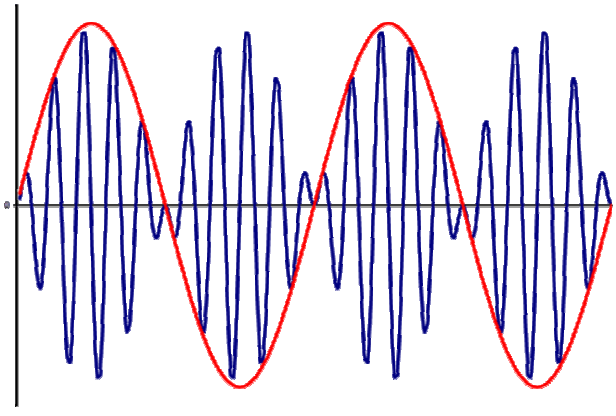
kde $A_V(t)$ je pomalu proměnná amplituda, jejíž okamžité hodnoty mají Rayleighovo rozdělení hustoty pravděpodobnosti a $\varphi_v(t)$ je pomalu proměnná počáteční fáze, jejíž okamžité hodnoty mají rovnoměrné rozdělení v intervalu od 0 do 2Л. [6]

Pásmová propust



Obr. 14. Pásmová propust

Pokud jsou mezní kmitočty blízké, dochází k záznějům. Příkladem je modulace DSB SC (Dual Side Band Suppressed Carrier), která obsahuje sice obě postranní pásma, ale nosná je zcela potlačena.

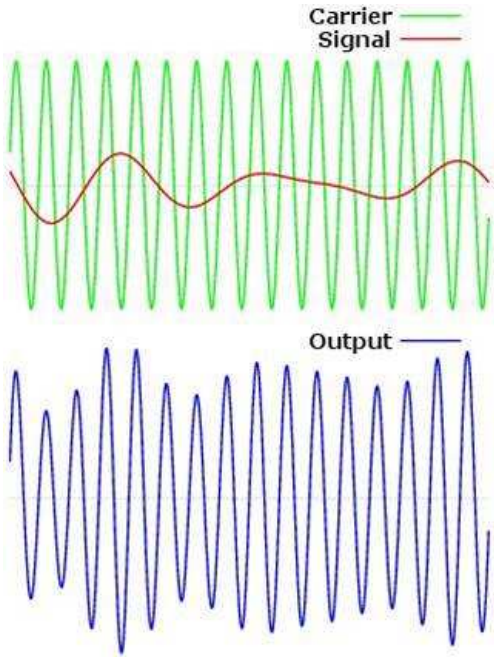


Obr. 15. Modulace DSB SC [7]

2.3 Účinky šumu na modulované signály

2.3.1 Amplitudová modulace (AM)

Jedním z nejpoužívanějších druhů modulace je amplitudová modulace. Patří mezi jednoduché spojité modulace. Amplituda nosného signálu se mění v závislosti na změně modulačního signálu. Frekvence ani fáze nosné se u této modulace nemění, zůstávají konstantní.

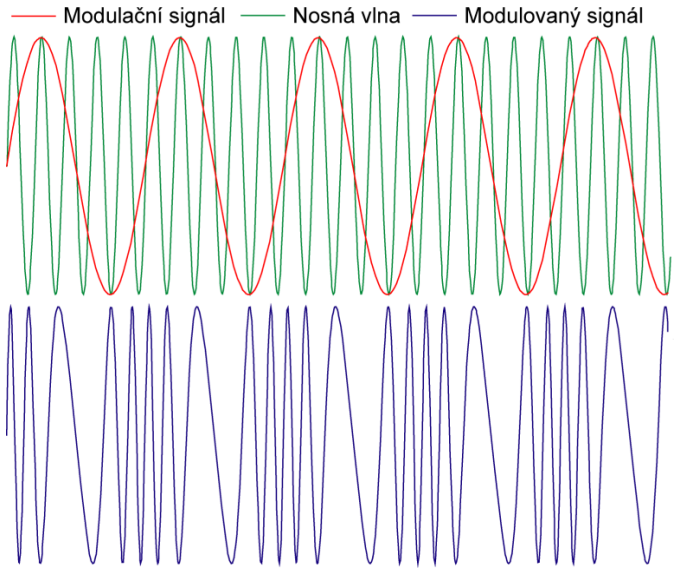


Obr. 16. Amplitudová modulace [8]

Amplitudová modulace je málo odolná a velmi citlivá na jakékoliv rušení amplitudového charakteru.

2.3.2 Frekvenční modulace (FM)

Amplituda nosné vlny zůstává při frekvenční modulaci konstantní. Kmitočet nosné vlny se mění působením nízkofrekvenčního modulačního signálu. Velikost změny kmitočtu, tzv. kmitočtový zdvih, závisí jen na velikosti amplitudy modulačního signálu.

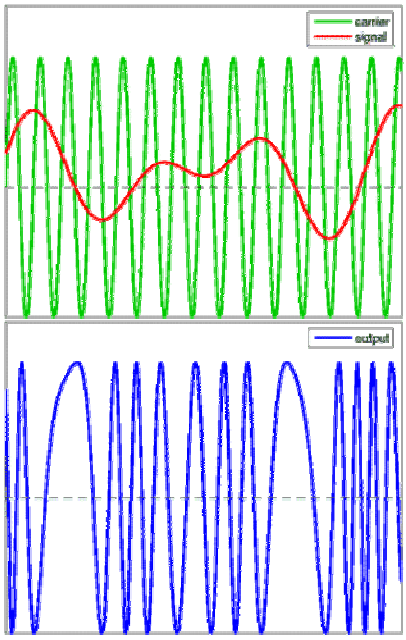


Obr. 17. Frekvenční modulace [9]

Frekvenční modulace je velmi odolná proti šumům a rušení. Proto byla v minulosti zvolena například pro jakostní přenos rozhlasu (FM rádio). Silným zesílením a následným omezením signálu na přijímací straně lze potlačit rušení amplitudového charakteru. Zkreslení, rušení parazitní fázovou modulací a šumy ovšem zůstávají.

2.3.3 Fázová modulace (PM)

Fázová modulace - PM (z anglického Phase Modulation) je druhem modulace u která mění fázi nosné vlny v rytmu modulačního signálu. Spojitá fázová modulace není příliš využívána, protože vyžaduje poměrně složitý demodulátor a v určitých situacích může být problematické rozeznat správně fázový posuv (například rozeznání 0 a 180°). Jedním z mála širších využití této modulace je nasazení v elektronických hudebních nástrojích, které ovšem bývá často nesprávně označováno jako FM (zkratka frekvenční modulace). V poslední době ovšem prudce narůstá využití varianty s diskrétním modulačním signálem nazvané PSK (Phase Shift Keying). [10]



Obr. 18. Fázová modulace [10]

V systému GSM se používá varianta digitální fázové modulace zvaná MSK (minimum shift keying). Jedná se přitom o vícestavové fázové klíčování, kdy se speciálním obvodem zajišťuje, aby nevznikaly výraznější fázové přeskoky v konstelačním diagramu klasické vícestavové PSK.

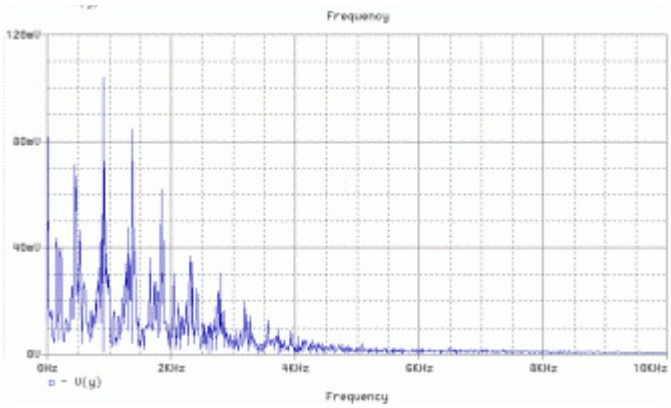
To vede k velmi efektivnímu využití kmitočtového spektra a minimálnímu rušení sousedních kanálů / účastníků.

Varianta MSK použitá u mobilních telefonů pak ještě používá předfiltraci digitálního signálu pomocí analogového Gaussova filtru. Tím je pak ještě dále vylepšena mezisymbolová interference.

3 CHAOTICKÝ OSCILÁTOR

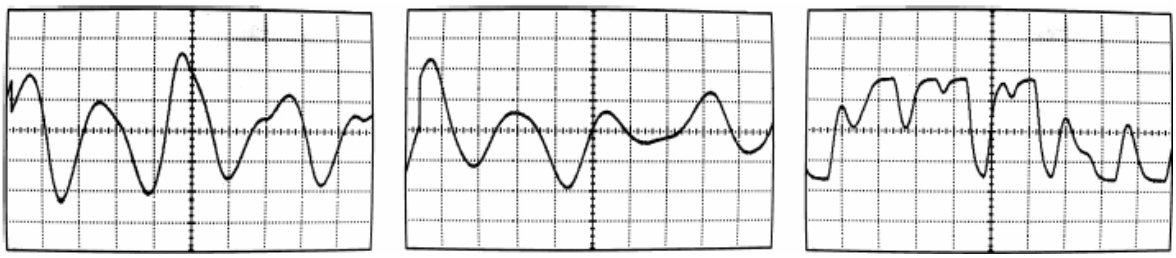
Chaotické oscilátory produkují periodické tlumené kmity. Periodické kmitání znamená, že se systém po určitém čase navrátí zpět do původního stavu, to vše při určitém časovém intervalu. Při tlumeném kmitání se část energie kmitů ztrácí, což ovlivňuje kmitání, nejčastěji postupným zmenšování amplitudy signálu.

Jak lze vidět, kmitočtové spektrum zobrazeného chaotického signálu je spojité.



Obr. 19. Spektrum chaotického signálu [13]

Pro ukázku uvádím také časové průběhy chaotických signálů.



Obr. 20. Časový průběh chaotických signálů [14]

II. PRAKTICKÁ ČÁST

4 REALIZACE RUŠIČKY MOBILNÍHO TELEFONU

4.1 Rušička lineárně rozmítaná s bílým šumem

Praktická část diplomové práce se již zabývá samotnou realizací rušičky mobilního telefonu dle zadání. Je zde popsáno její schéma a vysvětlen princip fungování. Naměřené veličiny a jejich průběhy jsou znázorněny v přehledných grafech.

Další část kapitoly se věnuje realizaci s chaotickým oscilátorem, jehož signál bude použit místo trojúhelníkového smíchaného s bílým šumem.

Při návrhu desky plošného spoje bude použit známý editor Eagle.

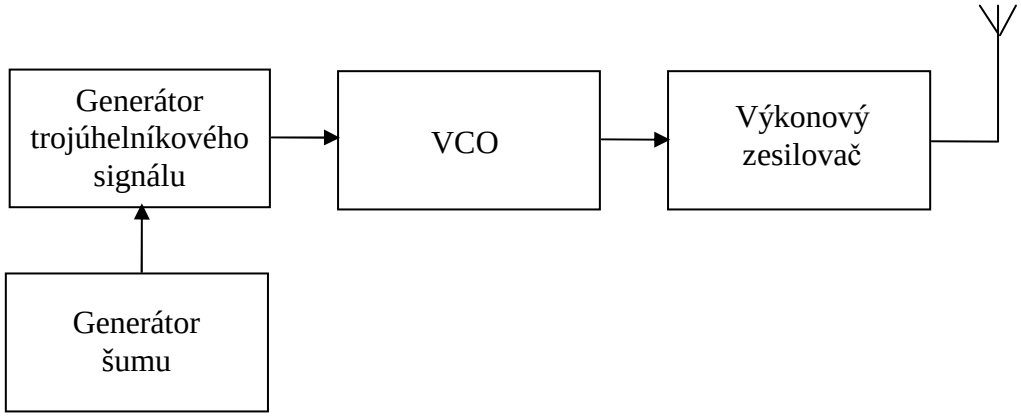
Úkolem práce také je sestavit rušičku s malým vysílaným výkonem, řádově v miliwattech, což by měl být výkon mnohem menší, než který vysílají rušičky které jsou k dostání v ČR. Je ovšem nutné dodat, že rušička realizovaná v diplomové práci bude zarušovat pouze pásmo 900 MHz.

Rušička samotná pracuje tak, že vysílá na stejných kmitočtech jako BTS rušící šumy. Mobilní telefon tyto šumy analyzuje a po překročení určité hranice těchto rušivých vln vyhlásí, že v dané lokalitě není dostupný signál.

Úkolem práce také je sestavit rušičku s malým vysílaným výkonem, řádově v miliwattech.

Princip rušení v našem případě spočívá v překrytí sestupné trasy signálu vysílaného základnovými stanicemi, tzv. downlink, o kmitočtech v rozmezí 935-960 MHz, rušivým signálem. Signál bude rozmítán trojúhelníkovým průběhem, smíchán s tzv. bílým šumem a bude naladěn na příslušné kmitočty pomocí napětím řízeného oscilátoru (VCO), konkrétně ZOS 1025 od firmy Mini-Circuits. Dále je nutné jej zesílit výkonovým zesilovačem a vysílat do okolí.

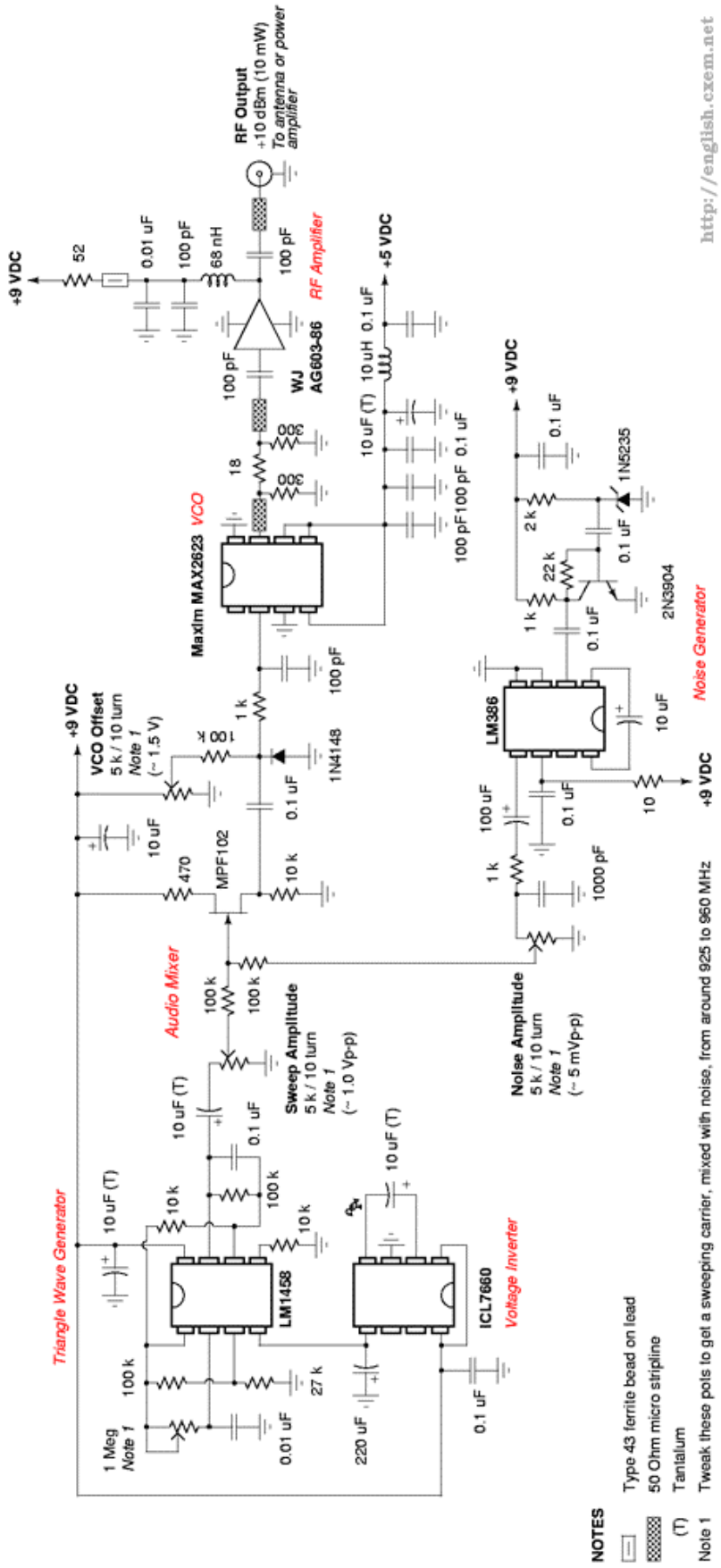
Následuje zjednodušené blokové schéma rušičky.



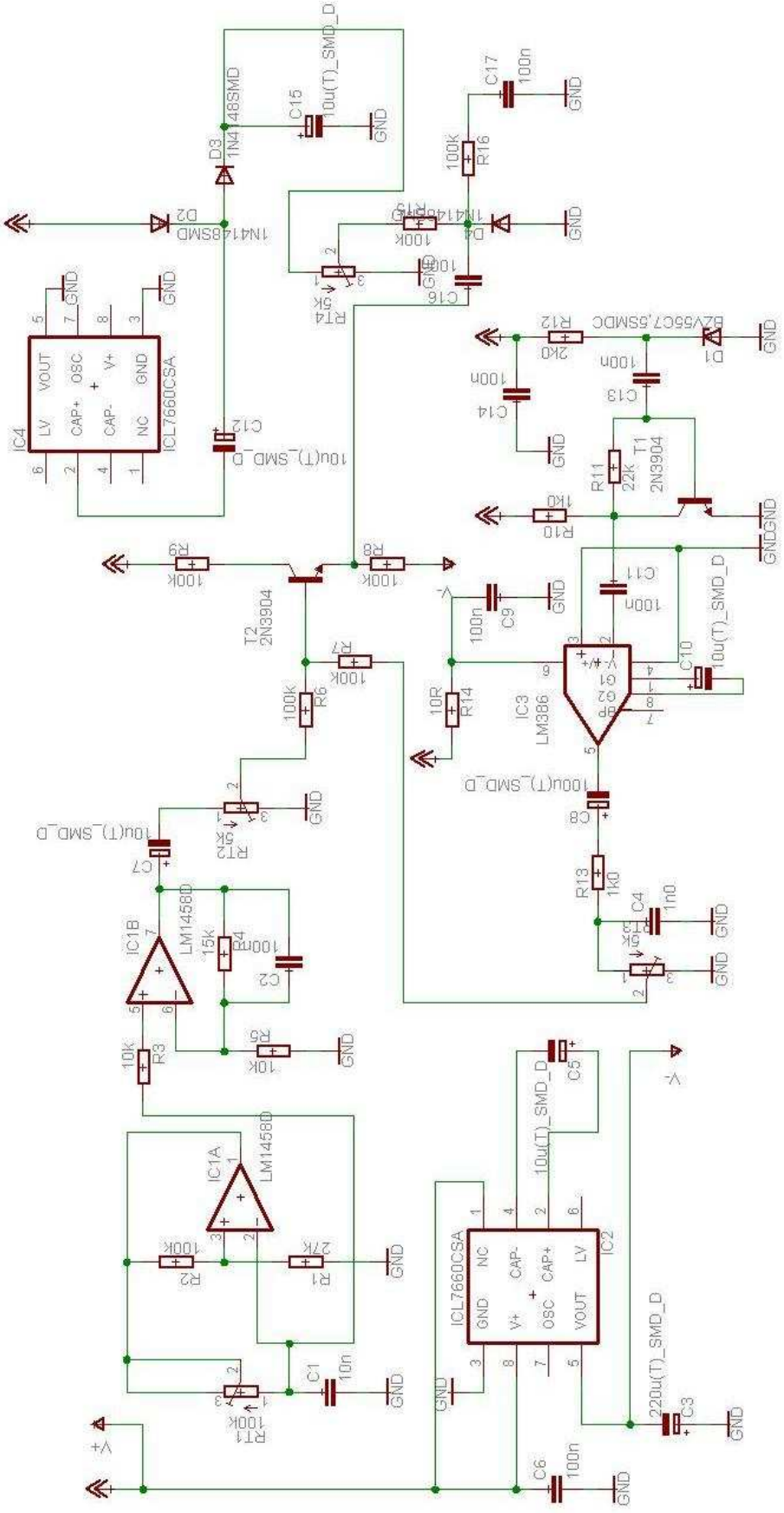
Obr. 21. Blokové schéma rušičky

4.1.1 Popis zapojení rušičky

Na následujících obrázcích jsou schémata zapojení rušičky mobilního telefonu, obr. 20. je schéma ze zadání, další obrázek, obr. 21., je už schéma nakreslené pomocí editoru plošných spojů Eagle, ve kterém je vytvořena i samotná deska plošného spoje.



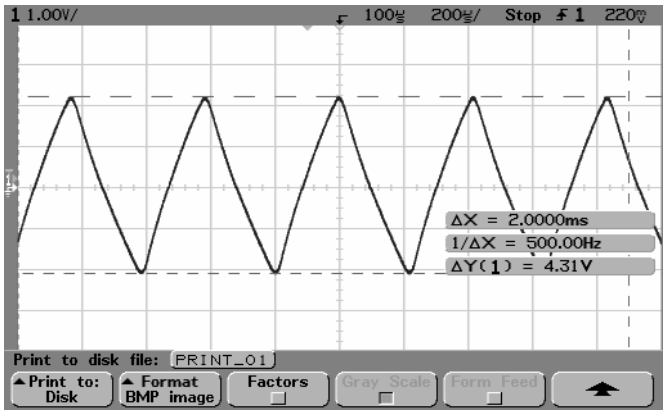
Obr. 22. Schéma zapojení rušičky [11]



Obr. 23. Schéma rušičky v programu Eagle

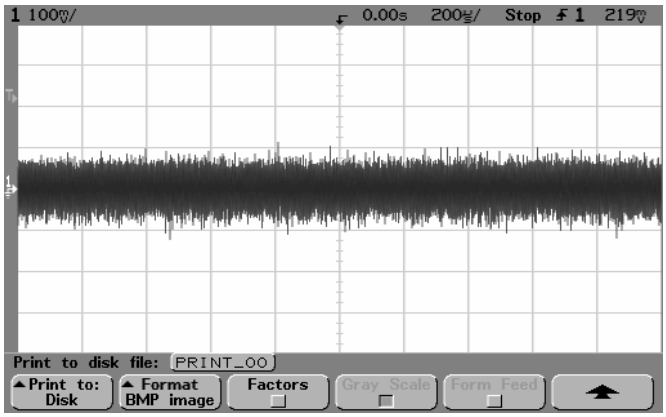
Samotná rušička se skládá z napěťového investoru, generátoru signálu trojúhelníkového průběhu, šumového generátoru a zdvojovače napětí.

Rušička je napájena stejnosměrným napětím o velikosti ± 9V a +18V. Obvod IC2, a to sice ICL7660CSA, slouží jako napěťový převodník. Operační zesilovač LM1458D je zapojen jako generátor signálu, IC1A obdélníkového průběhu, IC1B jako výsledného trojúhelníkového průběhu. Střídu tohoto signálu lze měnit trimrem RT1. Naměřený signál je znázorněn na následujícím obrázku, obr. 22.



Obr. 24. Signál trojúhelníkového průběhu

Signál z generátoru trojúhelníkového signálu je smícháván s tzv. bílým šumem. Ten pochází ze šumového generátoru, jehož základ tvoří známý nízkofrekvenční zesilovač LM386, mající ve schéma pozici IC3.

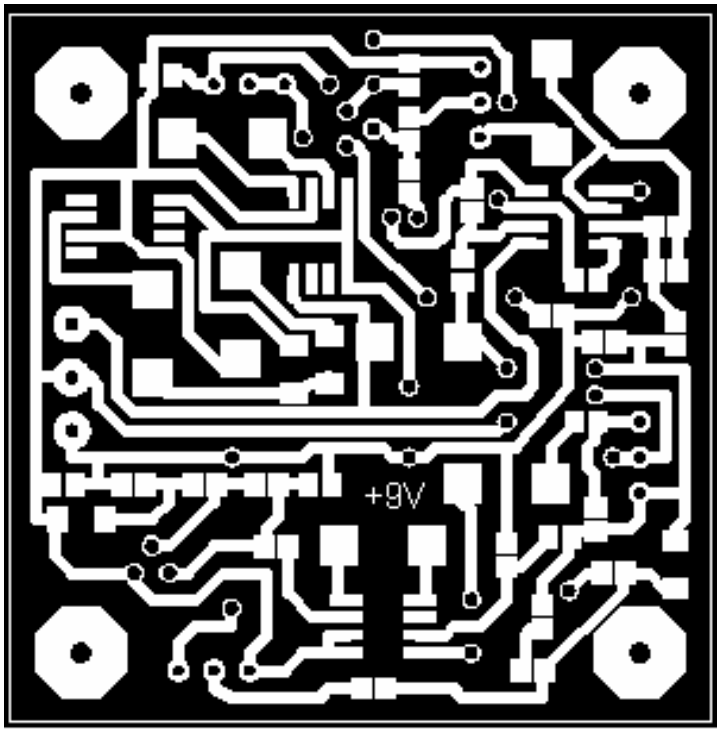


Obr. 25. Bílý šum

Šum je smíchán s trojúhelníkovým signálem před emitorovým sledovačem tvořeným tranzistorem T2, odporem R9, na který je přivedeno napájecí napětí + 9V a odporem R8 s napájecím napětím – 9V. Napětí za tímto sledovačem je pouze 0,7V, je tedy nutné jej zvednout na požadované (viz kapitola 3.2) hodnoty přivedením +18V ze zdvojovače napětí, jehož základ tvoří napěťový převodník ICL7660CSA.

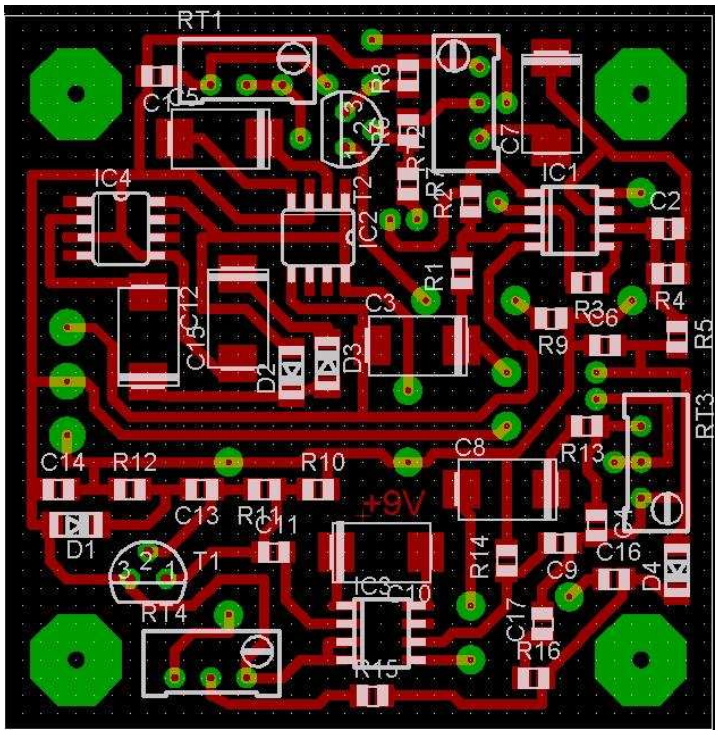
4.1.2 Deska plošného spoje

Jak již bylo zmíněno, návrh schématu a desky plošného spoje byl vytvořen v editoru Eagle. Protože editor neobsahoval knihovny pro všechny součástky, bylo nutné některé navrhnout. Na následujícím obrázku je deska plošného spoje z pohledu TOP.

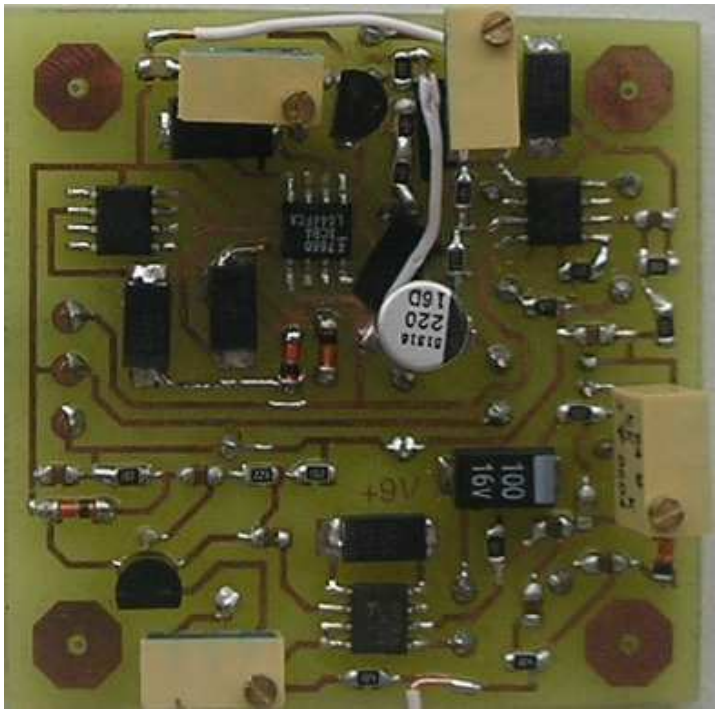


Obr. 26. DPS z pohledu TOP

V návrhu desky plošného spoje došlo k několika opravám. A to sice připojení napájení -9V na odpor R8 místo GND a přivedení zdvojeného napětí +18V na trimr RT4 místo napájení 9V. Vše je provedeno pomocí drátových propojek. Další obrázek je deska plošného spoje z pohledu TOP i s rozmístěním součástek, následuje už plošný spoj s osazenými součástkami.



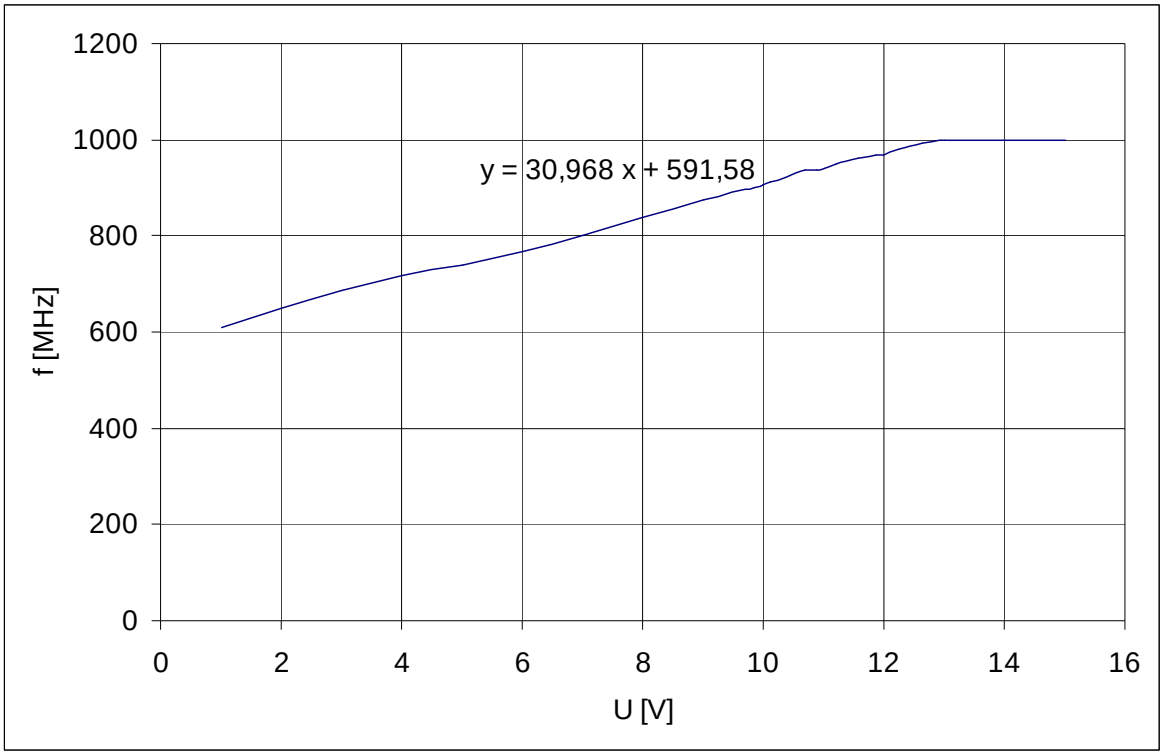
Obr. 27. DPS s rozmístěním součástek



Obr. 28. Osazená DPS

4.1.3 Praktická realizace rušičky

Jak již bylo zmíněno, rušivý element vzniká v generátoru trojúhelníkového průběhu a je smícháván s bílým šumem ze šumového generátoru. Napětím řízený oscilátor potřebuje takové hodnoty napětí, aby generoval požadované kmitočty a bylo možné překrývat požadované spektrum. Následující graf znázorňuje naměřenou charakteristiku VCO ZOS 1025, a to sice závislost kmitočtu na přiváděném napětí. Tato se prakticky neliší od charakteristiky uváděné výrobcem.



Obr. 29 Charakteristika VCO

VCO poskytuje kmitočty v rozmezí od 685 MHz do 1025 MHz, což je pro rušení požadovaného pásma plně dostačující.

Abychom dosáhli požadovaných kmitočtů z VCO, bylo nutné upravit napájecí napětí, protože jeho velikost nebyla dostatečná. Pomocí obvodu ICL7660CSA, ve schématu uvedeném jako IC4, zapojeného jako zdvojovače napětí, dochází ke zdvojení napájecího napětí, a to sice z +9V na +18V. Jeho velikost je upravována na potřebnou hodnotu na děliči napětí tvořeném odporovým trimrem RT4 a odporem R15.

Jelikož chceme zarušit pásmo od 935 MHz do 960 MHz, je nutné zvolit i odpovídající hodnoty napětí pro VCO. Křivka grafu má rovnici regrese:

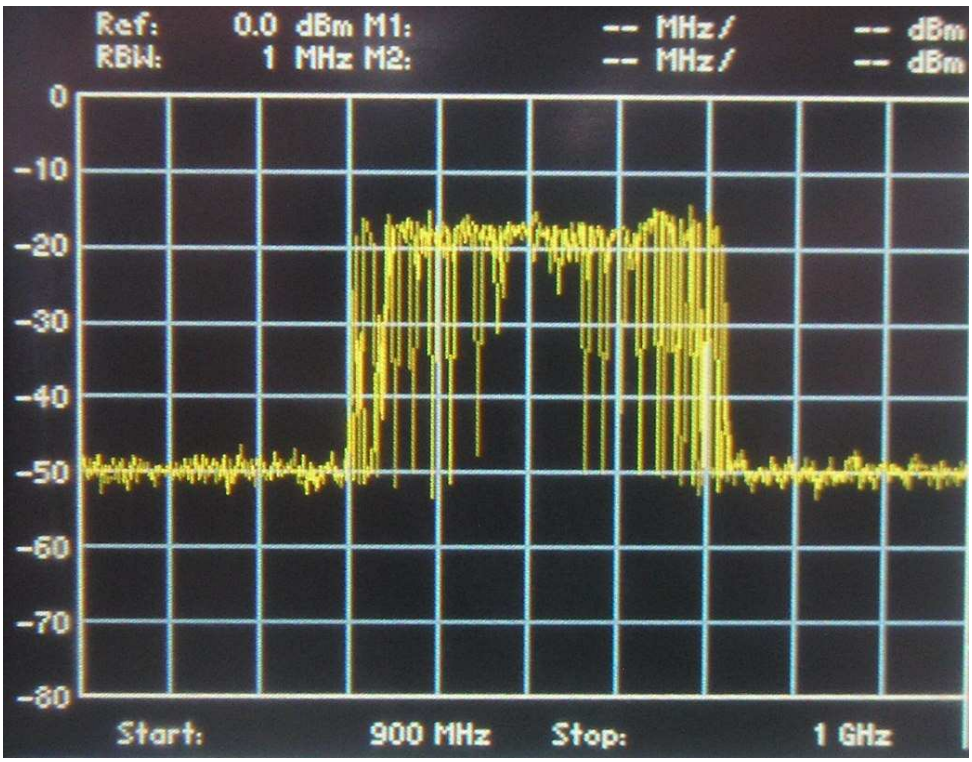
$$y = 30{,}968x + 591{,}58$$

Po úpravě:

$$x = \frac{y - 591{,}58}{30{,}968}$$

Z toho vyplývá, že pro kmitočty od 935 MHz do 960 MHz je třeba nastavit napětí od 11,01V do 11,97V.

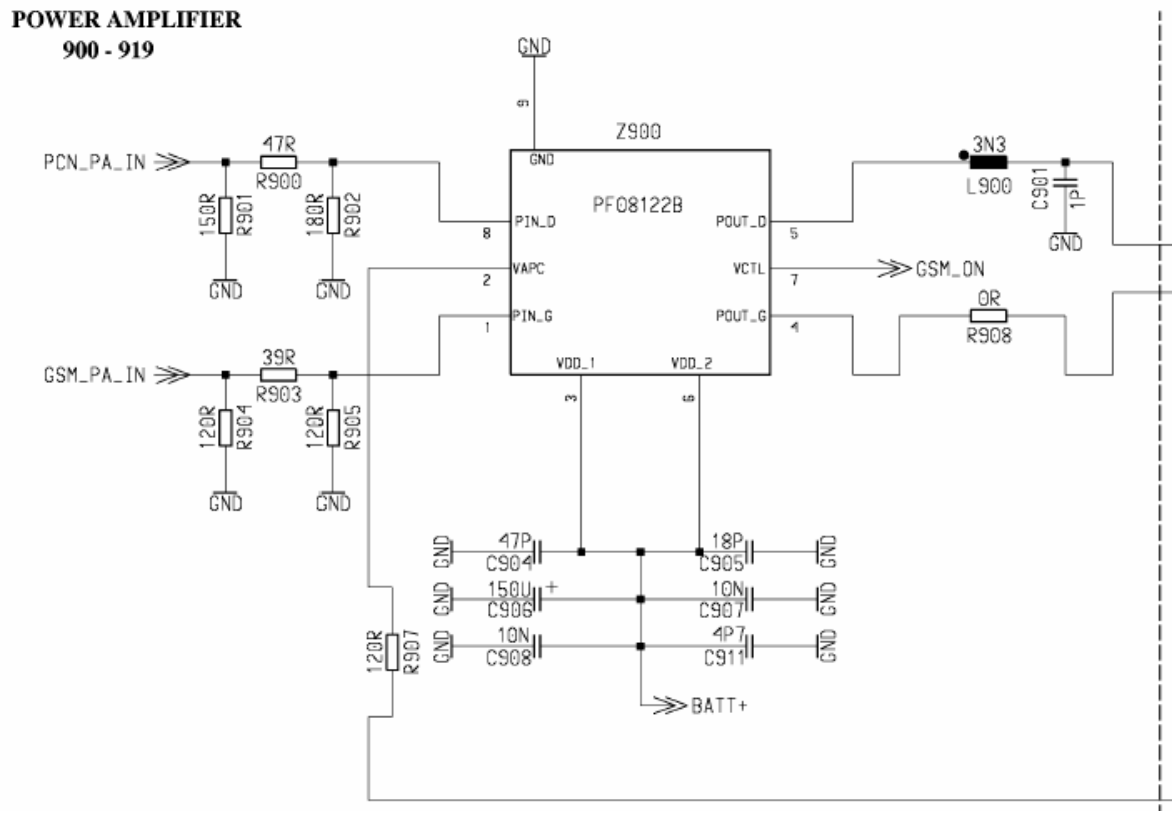
Rozsah požadovaného napětí nastavíme pomocí odporových trimrů RT2 a RT4. Aby bylo rušení spolehlivější, je nutné překrýt nejen celé pásmo, ale i kmitočty pod a nad uváděným rozmezím. Velikost napětí zvolíme tedy úměrně požadovaným hodnotám. Průběh rušivého signálu je názorně vidět na spektrálním analyzátoru.



Obr. 30. Průběh signálu ze spektrálního analyzátoru

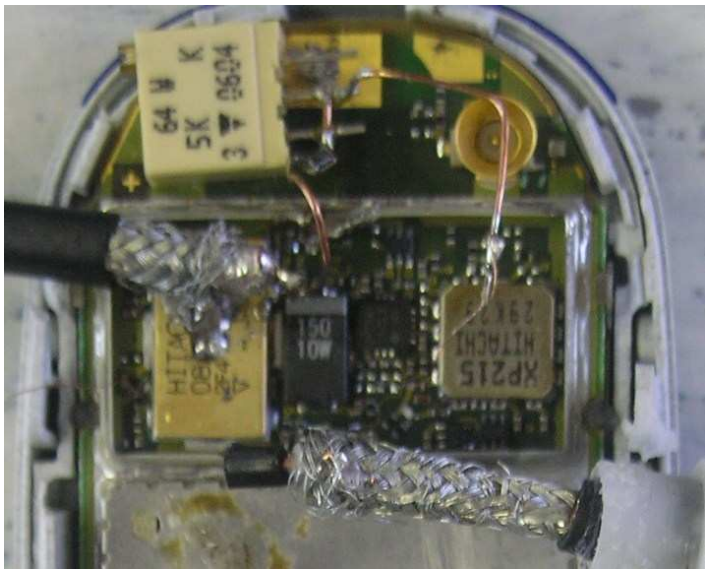
Po připojení antény na výstup VCO byla ověřena funkčnost rušičky, dosah rušivého signálu bude změřen v další části této kapitoly.

Jak již bylo zmíněno, signál je nutné zesílit výkonovým zesilovačem. Zvolen byl zesilovač z mobilního telefonu Siemens A50, konkrétně PF08122B. Nejprve je nutné změřit jeho zesílení. Na vstup VAPC , pin 2 , je přivedeno napětí z děliče, který je postaven přímo na desce plošného spoje telefonu. Dělič je napojen na kondenzátor C906 a upravuje napětí z baterie telefonu z hodnoty 9V na 1,2 V. Zesílené napětí by mělo být změřitelné na výstupu zesilovače POUT_G, pin 4. Výsledné napětí a tudíž i zesílení se přes velkou snahu změřit nepodařilo. Rušička bude tedy odzkoušena v provozu pouze s nezesíleným signálem. Na následujícím obrázku je schéma zapojení výkonového zesilovače.



Obr. 31. Zapojení výkonového zesilovače [12]

Pro ukázku uvádím na další straně i praktické zapojení děliče napětí a vodiče pro měření zesílení.

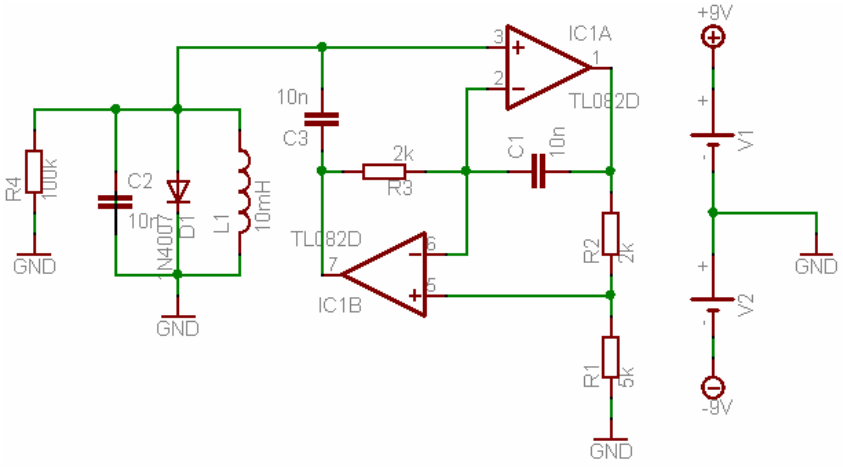


Obr. 32. Měření zesílení

Jak již bylo uvedeno, zesilovač se otestovat nepodařilo. Ovšem i tak bude rušička uvedena do provozu a změřen dosah rušivého signálu. Výsledky měření a srovnání s rušičkou s chaotickým oscilátorem jsou v další části kapitoly.

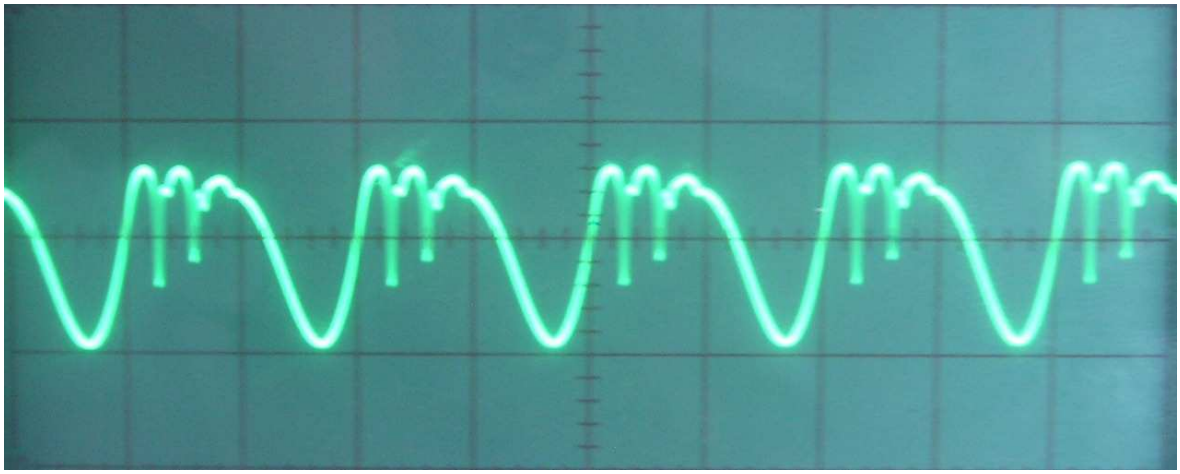
4.2 Rušička s rychlým přelaďováním pomocí chaotického oscilátoru

Dalším bodem je realizace rušičky s chaotickým oscilátorem. Ten byl navrhnutý se záporným diferenciálním odporem a operačním zesilovačem TL082 a rezonančním LC obvodem. Napájení je + - 9V. Následuje jeho schéma z programu Eagle.



Obr. 33. Chaotický oscilátor

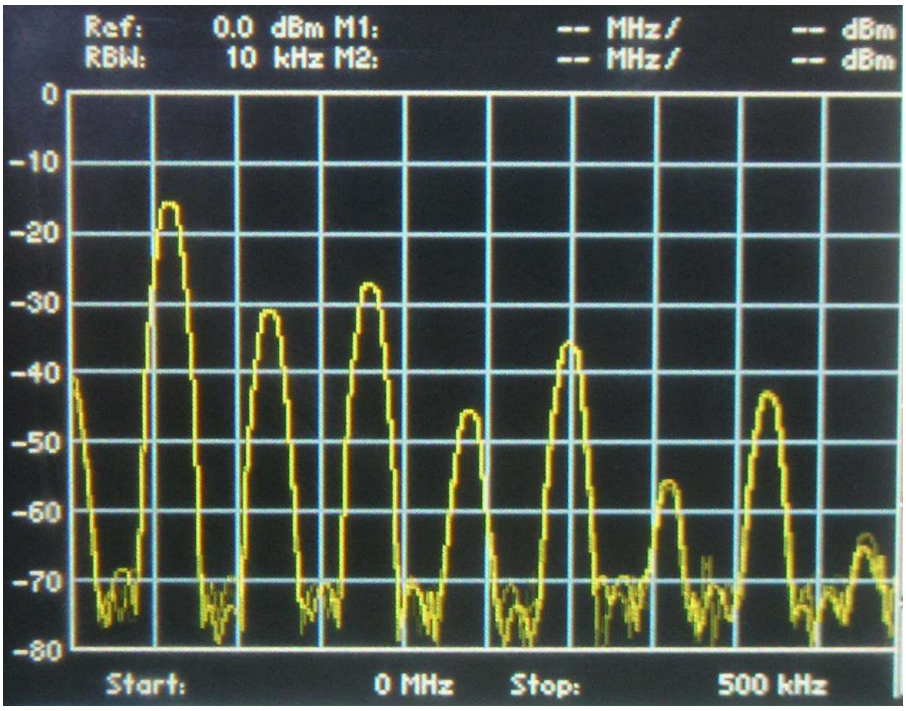
Průběh rozmítaného napětí chaotického oscilátoru změřený na osciloskopu:



Obr. 34. Průběh chaotického oscilátoru

Osciloskop je nastaven na hodnotu 1V/DIV, tudíž výsledné napětí kmitá v rozsahu od – 0,9V do + 0,6 V.

Průběh chaotického oscilátoru změřený spektrálním analyzátorem:



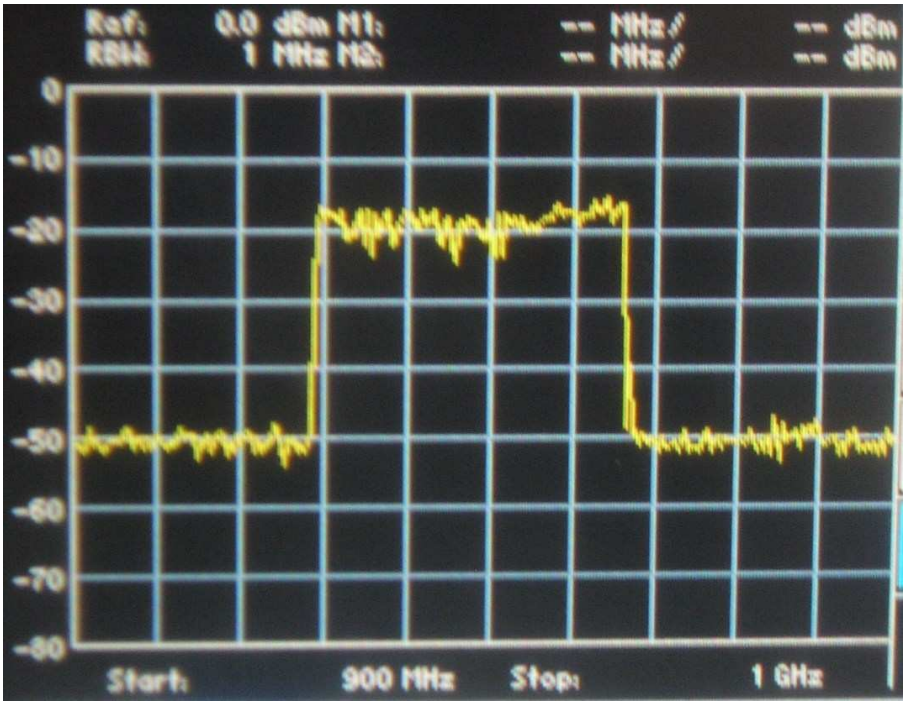
Obr. 35. Průběh chaot. oscilátoru ze spektrálního analyzátoru

Tento naměřený průběh však chaotické kmitání připomíná jen velmi vzdáleně. Jedna z možností, jak jej napravit, je změna hodnoty tlumícího odporu oscilátoru R4 ze 100kΩ na 200 až 500 kΩ. Tato možnost však ke zlepšení průběhu nevedla. Další způsob spočívá v přeměření cívky L1. Její indukčnost je skutečně 10 mH. Vhodné by bylo i zjištění činitele jakosti cívky Q či změna záporného diferenciálního odporu, ovšem to se mi již z časových důvodů nepodařilo.

Další postup je shodný jako u rušičky s lineárním rozmítáním s bílým šumem, tj. smíchání signálu s napětím nutným pro naladění VCO. Protože signál po smíchání s napětím zcela zanikl, bylo nutné jej zesílit na zesilovači LM1458.

Pak již byl VCO naladěn bez problémů na příslušné rozmezí kmitočtů potřebné pro zarušení pásma 900 MHz, tj. 935 až 960 MHz.

Průběh signálu lze vidět na spektrálním analyzátoru:



Obr. 36. Signál z chaot. oscilátoru na spektrálním analyzátoru

Průběh signálu sice neodpovídá předpokladům, nicméně i tak ho lze použít k rušení sítě GSM. V následující kapitole je popsáno měření dosahu rušivého signálu.

4.3 Měření dosahu rušivého signálu

V této kapitole popisuji způsob měření a dosah rušivého signálu. Měření bylo provedeno v laboratoři, jejíž vybavení bylo ponecháno na původních místech aby byly co možná nejvěrohodněji zachovány podmínky a vlastnosti měřené místnosti, protože při praktickém použití rušičky jsou také kladeny signálu různé překážky.

Vysílaný signál není výkonově zesílen, je pouze odebírán z VCO a přiveden do antény. Pro měření byla použitá všesměrová anténa a mobilní telefon Nokia 3220. Během měření se VCO zahříval, výrobcem udávaná pracovní teplota je do 85°C, ovšem měření netrvalo tak dlouho, aby bylo nutné jeho chlazení. Obrázek ukazuje anténu a mobilní telefon již bez signálu.

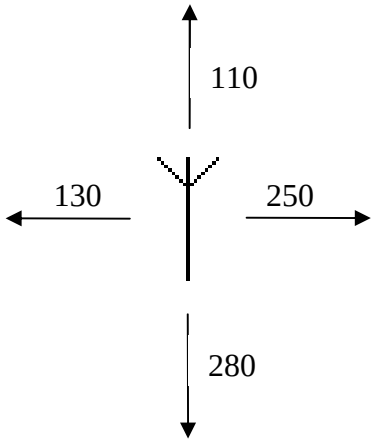
Obr. 37. Mobilní telefon bez signálu

Měření bylo prováděno několik ve směrech zobrazených na schématech níže. Výsledné hodnoty jsou potom průměrnou vzdáleností.

Uvedené průměrné vzdálenosti uvádějí místo, kde nebyl mobilním telefonem zaznamenán vůbec žádný signál, jehož intenzita je zobrazována na displeji pomocí jednotlivých dílků. Mobilní telefon tedy v daných místech nezobrazil ani jeden dílek.

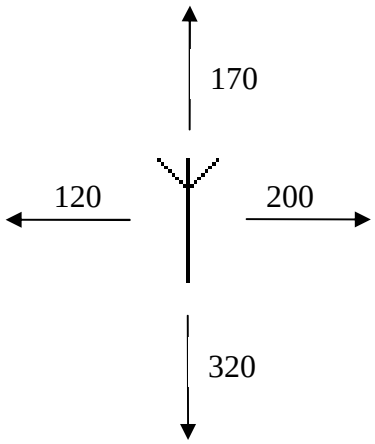
4.3.1 Dosah lineárně rozmítané rušičky s bílým šumem

Schéma znázorňuje vzdálenost místa od antény, kde ještě nebyl zaznamenán žádný signál, v centimetrech. Měření bylo prováděno ve vodorovných směrech, podle schématu by se mohlo zdát že se měřily místa pod a nad rušičkou. Měření má spíše informativní charakter, hodnoty jsou vzhledem ke způsobu měření pouze orientační.



Obr. 38. Dosah lineárně rozmítané rušičky

4.3.2 Dosah rušičky s rychlým přelaďováním pomocí chaotického oscilátoru



Obr. 39. Dosah rušičky s chaot. oscilátorem

4.3.3 Srovnání dosahů rušivých signálů

Při výpočtu zarušené plochy jsem vycházel z předpokladu, že anténa vysílá do všech směrů a zarušená plocha má obdélníkový tvar.

Signál z lineárně rozmítané rušičky zabírá plochu asi 14,8 m^2 a signál rušičky s chaotickým oscilátorem asi 15,7 m^2, což jsou prakticky srovnatelné hodnoty a odpovídají velikosti menší místnosti.

Skoro stejnou vzdálenost vysílání rušivého signálu lze vidět pouze ve směru za anténou, potom už se hodnoty liší. Lineárně rozmítaná rušička vysílá více před sebe, ale zase podstatně méně do obou stran. V těchto směrech vykazuje vyšší hodnoty rušička s chaotickým oscilátorem.

Z výsledků pořízených tímto způsobem bych nejspíš nevyzdvihoval ani jeden ze způsobů rušení, co se týká zarušené plochy, jsou výsledky téměř totožné. Relevantnější výsledky by přineslo měření se zesíleným signálem. Z důvodů uvedených v předchozí kapitole však takové měření není možné provést. Dosah rušivého signálu se také liší v závislosti na síle signálu vysílaného stanicemi BTS, v místech kde je silnější by byl dosah rušičky menší. A naopak v místech se signálem slabším se dosah rušičky zvyšuje.

ZÁVĚR

Rušení signálu GSM sítí je v ČR zakázáno, nicméně používá se například ve věznicích či bankách.

Systém GSM je řazen k tzv. buňkovým systémům, pracuje tedy na principu rozdělení území na jednotlivé buňky, které jsou pokrývány signálem pomocí základnových stanic BTS. Jeho první návrhy vznikly již počátkem osmdesátých let. Systém GSM má vyhrazena dvě rádiová pásma o šířce 2x25 MHz. Pro mobilní stanice je to 890-915 MHz, základnové stanice vysílají v rozmezí 935-960 MHz. A právě tento signál je zarušen.

GSM signál je modulován pomocí speciální fázové modulace, GMSK (Gaussian Minimum Shift Keying), která je velmi odolná proti rušení. Ostatní modulace, tedy amplitudová a frekvenční, již takovou odolnost neposkytují.

Teoretické předpoklady pro fungování lineárně rozmítané rušičky s bílým šumem se podařilo naplnit. Nepodařilo se však již daný signál zesílit. Vybraný zesilovač PF08122B byl měřen přímo na desce plošného spoje mobilního telefonu Siemens A50, zkušební napětí 1,2V přiváděno na vstup zesilovače, ovšem zesílení se změřit nepodařilo. Je možné, že zesilovač je řízen dalším signálem, který se mi však nepodařilo odhalit.

Průběh chaotického oscilátoru úplně neodpovídá teoretickým předpokladům, chaotické kmitání téměř nesplňuje. Jedna z možností, jak průběh napravit, byla změna tlumícího odporu. Tento způsob však k nápravě nevedl. Další možnost spočívá v přeměření cívky. Indukčnost je skutečně 10mH. Činitel jakosti cívky Q jsem z časových důvodů i z nedostatku teoretických znalostí nezměřil. Signál se neshoduje také proto, že vlastnosti použitých součástek nejsou shodné s těmi ideálními. Ovšem i s takovým signálem lze kmitočtové spektrum spolehlivě zarušit.

Samotné měření dosahu rušivého signálu má pouze informativní charakter, protože metoda měření pomocí mobilního telefonu není úplně ideální. Měřil se dosah nezesíleného signálu ve školní laboratoři. Oba způsoby rušení vykazují přibližně stejně velkou zarušenou plochu - signál z lineárně rozmítané rušičky zabírá plochu asi 14,8 m^2 a signál rušičky s chaotickým oscilátorem asi 15,7 m^2. Tímto způsobem nelze jednoznačně určit, který metoda rušení je spolehlivější a výkonově méně náročnější.

Zadání diplomové práce se podařilo naplnit pouze z části. A to hlavně z časových důvodů i kvůli nedostatkům teoretických znalostí potřebných pro naplnění některých úkolů v diplomové práci.

I přesto myslím, že práce a vynaložené úsilí nebyly zbytečné. Nabyté znalosti a zkušenosti budou určitě využity.

CONCLUSION

Jamming of a GSM network is in CR off limited, nevertheless are using for example in prison or banks.

GSM system is sorting to a cellular systems, he is working then on principle partition of area on component cells, which are overlaying signal by the help BTS station. His first suggestions originated yes early eightieth years. GSM system has stipulated two radio band widths 2x25 MHz. For mobile station it's 890-915 MHz, base station are broadcasting at intervals 935-960 MHz. And just this signal is jamming.

GSM signal is modulating by the help of special phases modulation, GMSK (Gaussian Minimum Shift Keying), which is very resistant to jamming. Others modulation, then amplitude and frequency, yet withheld such immunity.

Theoretical presumptions for function linear sweep jammer with white noise are managed complete. Signal indeed yet miscarried amplify. Choice amplifier PF08122B was metered right on card of printed circuits mobile phone Siemens A50, test voltage 1,2V was connected onto input of amplifier, indeed miscarried measure boost. Is possible, than amplifier is managing next signal, which I'm not detected.

Course of chaotic oscillator do not completely reply theoretical presumption, chaotic oscillating nearly fail to satisfy. One of possibilities, how repair course, was change of steadying resistance. That manner but isn't conducted to reparation. Next possibility is measuring of inductor. Inductivity is really 10mH. I 'm not measured Q-factor of inductor from time reasons and for lack of theoretic knowledge. Signal don't harmonize also hence, that characteristics of using parts aren't consistent with those ideal. But with such signal is possible jamming of frequency spectrum.

Metering of reach jamming signal has only informative character, because metering method by the help of mobile phone isn't completely ideal. Both manners of jamming are approximately embodying commensurate jamming area – signal from linear sweep jammer is occupying area about 14,8 m^2 and signal of jammer with chaotic oscillator about 15,7m^2. In this way it's impossible specify, which method of jamming is more reliable and fewer more exacting for power.

Graduation thesis managed complete only from a part. Largely from time reason, also on the score of absences theoretic knowledge needed for implementation some tasks in graduation thesis.

I thing yet, that work and take pains wasn't needless. Acquisition experience and experience will certainly be use.

SEZNAM POUŽITÉ LITERATURY

[1] RICHTR, Tomáš. Technologie pro mobilní komunikaci [online]. 2002 [cit. 2008-05-02]. Dostupný z WWW: <http://tomas.richtr.cz/mobil/bunk-gsm.htm>.

[2] Systém základnových stanic [online]. 2008 [cit. 2008-05-02]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Systém_základnových_stanic>.

[3] Bílý šum - Wikipedie, otevřená encyklopedie [online]. 2008 [cit. 2008-05-24]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Bílý_šum>.

[4] White noise - Wikipedia, the free encyclopedia [online]. 2008 [cit. 2008-05-24]. Dostupný z WWW: <http://en.wikipedia.org/wiki/White_noise>.

[5] EISENSTEINOVÁ, Gabriela, SEDLÁČEK, Miloš. Využití Matlabu k potlačování aditivního šumu pomocí filtrace a pomocí vlnové transformace. In Konference Matlab 2004. [s.l.] : [s.n.], 2004. s. 8. Dostupný z WWW: <dsp.vscht.cz/konference_matlab/matlab04/matejka.pdf>.

[6] ČÍŽ, Radim. Teorie sdělování [online]. 2008 [cit. 2008-05-24]. Dostupný z WWW: <http://www.utko.feec.vutbr.cz/~cizr/tsd/index.php>.

[7] Amplitudová modulace - Wikipedie, otevřená encyklopedie [online]. 2008 [cit. 2008-05-23]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Amplitudová_modulace>.

[8] KASÍK, Pavel. Technet.cz [online]. 2006 [cit. 2008-05-24]. Dostupný z WWW: <http://i.idnes.cz/06/123/nesd/DNO17e68b_Amplitude_modulation_wikipedia.jpg>.

[9] Frekvenční modulace - Wikipedie, otevřená encyklopedie [online]. 2008 [cit. 2008-05-24]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Frekvenční_modulace>.

[10] Fázová modulace - Wikipedie, otevřená encyklopedie [online]. 2008 [cit. 2008-05-24]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Fázová_modulace>.

[11] Cellular Phone Jammer [online]. 1999-2008 [cit. 2008-05-02]. Dostupný z WWW: <http://english.cxem.net/mobile/mobile209.php>.

[12] Servisní manuál Siemens A50. [cit. 2008-05-24]. Dostupný z WWW: http://www.siemensmania.cz/download.php?file=smanualy/diagram_set_a50.rar.

[13] PETRŽELA, Jiří. Obvodová realizace konzervativního chaotického oscilátoru. Elektrorevue [online]. 2004 [cit. 2008-05-24]. Dostupný z WWW: <http://www.elektrorevue.cz/clanky/04001/index.html>.

[14] HRUBOŠ, Zdeněk. Anlogový univerzální oscilátor. [s.l.], 2007. 46 s. Bakalářská práce. Dostupný z WWW: <www.ieee.cz/mtt/soutez07/Hrubos.pdf >.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ARFCN Absolute Radio Frequency Channel Number (absolutní číslo rádio frekvenčního kanálu)

ADC Administrative Centre (administrativní centrum)

AM Amplitude modulation (amplitudová modulace)

AuC Authentication Centre (autentizační centrum)

CEPT European Conference of Postal and Telecommunications Administrations (Konference evropských správ a pošt)

BSC Base Station Controller (základnová řídící jednotka)

BTS Base Transceiver Station (základnová stanice)

BSS Base Station Sub-System (subsystém základových stanic)

EIR Equipment Identity Register (identifikační registr mobilních stanic)

ETSI European Technical Standards Institute (Evropský telekomunikační normalizační institut)

FDD Frequency Division Duplex (frekvenční duplex)

FM Frequency Modulation (frekvenční modulace)

GMSK Gaussian Minimum Shift Keying (klíčování Gaussovým minimálním posuvem)

GND Ground (zem)

GSM Global System for Mobile Communication (globální systém pro mobilní komunikaci)

HLR Home Location Register (domovský lokační registr)

IMEI International Mobile Equipment Identity (výrobní číslo mobilního telefonu)

IMSI International Mobile Subscriber Identity (mezinárodní identifikační číslo)

ISDN Integrated Services Digital Network (digitální komunikační síť s integrovanými službami)

IWF Inter-Working Functionality (jednotka spolupráce)

MSC	Mobile Switching Centre (mobilní radiotelefonní ústředna)
MSK	Minimum Shift Keying (minimální klíčování)
NMC	Network Management Centre (centrum pro řízení sítě)
NSS	Network Switching Subsystem (síťový přepojovací systém)
OMC	Operational and Maintenance Centre (provozní a servisní centrum)
OSS	Operation Support Subsystem (operační podpůrný subsystém)
PM	Phase Modulation (fázová modulace)
PSK	Phase Shift Keying (fázové klíčování)
SFH	Slow Frequency Hopping (pomalé frekvenční kroky)
SMS	Short message service (systém krátkých zpráv)
TA	Timing Advance (předstih)
TC	Trans Coder (transkodér)
VCO	Voltage Control Oscillator (napětím řízený oscilátor)
VLR	Visitor Location Register (návštěvnický lokační registr)
TDMA	Time Division Multiple Access (vícenásobný přístup s časovým dělením)

SEZNAM OBRÁZKŮ