Vysoká škola báňská – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Bezpečnostní problémy GSM

GSM security issues

2014

Bc. Martin Prokeš

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání diplomové práce

Student: **Bc. Martin Prokeš**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2612T059 Mobilní technologie

Téma: Bezpečnostní problémy GSM
GSM Security Issues

Zásady pro vypracování:

1. Vlastnosti, principy a komponenty GSM/UMTS sítí
2. Zabezpečení komunikace v GSM/UMTS sítích, rizika a útoky
3. Praktická realizace odposlechu hovorů v GSM síti s využitím USRP
4. Zhodnocení dosažených výsledků

Seznam doporučené odborné literatury:

REDL S., WEBER, M., OLIPHANT M. *GSM and Personal Communications Handbook*. Artech House, 1998, ISBN 978-0-89006-957-8
NIEMI V., NYBERG, K. *UMTS Security*. Wiley, 1 edition, 2003, ISBN 978-0470847947
BURGESS D., HARVIND S. *Open BTS Project*. Kestrel Signal Processing, California, 2008
GUNNAR H. *GSM Networks, Protocols and Implementation*. Artech House, 1999, ISBN 0-89006-471-7

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **doc. Ing. Miroslav Vozňák, Ph.D.**

Datum zadání: 16.11.2012
Datum odevzdání: 07.05.2014

VYSOKÁ ŠKOLA BÁŇSKÁ-TECHNICKÁ UNIVERZITA Fakulta elektrotechniky a informatiky OSTRAVA

doc. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlášení studenta

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne: *4. května 2014*

podpis studenta

Poděkování

Rád bych poděkoval doc. Ing. Miroslavu Vozňákovi, Ph.D. za odbornou pomoc a konzultaci při vytváření této diplomové práce.

Tato práce byla vypracována v rámci projektu „Podpora vědy a výzkumu v Moravskoslezském kraji 2013 DT 2 – Podpora výzkumu a vývoje VŠB-TUO prostřednictvím investic“ (č. s. 02540/2013/RRC). Podpořeno z rozpočtu Moravskoslezského kraje.

Abstrakt

Globální systém pro mobilní komunikaci (GSM) je v současnosti celosvětově nejrozšířenějším telekomunikačním systémem s více než 7 miliardami uživatelů. Tato diplomová práce se zabývá problematikou zabezpečení komunikace na rádiovém rozhraní systému GSM. Práce nejprve analyzuje bezpečnostní rizika v systému GSM, a popisuje již realizované a publikované útoky vůči tomuto systému. Na základě těchto poznatků je následně prakticky provedena realizace útoků vůči autentizačním a šifrovacím mechanismům sítě GSM, za využití volně dostupného software a hardware v podobě softwarově programovatelného rádia USRP (Universal Software Radio Peripheral) a DVB-T (Digital Video Broadcasting-Terrestrial) přijímače.

Klíčová slova

Zabezpečení GSM; mobilní telefonní sítě; falešná BTS; IMSI catcher; odposlech komunikace; USRP; DVB-T přijímač; Airprobe

Abstract

Global System for Mobile communication (GSM) is actually the most wordldwide used telecommunication system serving over 7 billion users. This master thesis points out security weaknesses in the radio interface of GSM. These weaknesses are analyzed and afterwards already realized attacks against GSM are described. Using open-source software and available hardware – USRP (Universal Software Radio Peripheral), DVB-T (Digital Video Broadcasting – Terrestrial) receiver are realized several attacks against authentication and ciphering mechanisms in GSM

Key words

GSM security; mobile telecommunication networks; fake BTS; IMSI catcher; eavesdropping; USRP; DVB-T receiver; Airprobe

Seznam použitých zkratek

Zkratka	Význam
3GPP	3rd Generation Partnership Project
AMPS	Base Transceiver Station
BCH	Broadcast Channel
BCCH	Broadcast Control Channel
BTS	Base Transceiver Station
CCC	Chaos Computer Club
CCH	Control Channel
CEPT	European Conference of Postal and Telecommunications Administrations
DVB-T	Digital Video Broadcasting – Terrestrial
ETSI	European Telecommunications Standards Institute
FACCH	Fast Associated Control Channel
HSDPA	High-Speed Downlink Packet Access
IEEE	Institute of Electrical and Electronics Engineers
IMSI	International Mobile Subscriber Identity
ISDN	Integrated Services Digital Network
ITU	International Telecommunication Union
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
GSMA	GSM Association
LAPD	Link Access Procedures, D channel
LTE	Long Term Evolution
MoU	Memorandum of Understanding
NMT	Nordic Mobile Telephony
PCS	Personal Communications Service
PCH	Paging Channel
SACCH	Slow Associated Control Channel
SCH	Synchronization Channel

SDCCH	Standalone Dedicated Control Channel
SMS	Short Message Service
SIM	Subscriber Identity Module
TACS	Total Access Communication System
TMSI	Temporary Mobile Subscriber Identity
UMTS	Universal Mobile Telecommunication System
USIM	Universal Subscriber Identity Module
USRP	Universal Software Radio Peripheral

Obsah

Úvod

Systém GSM je v současnosti stále světově nejrozšířenější technologií pro mobilní komunikaci. Již od prvního zveřejnění dokumentace systému dochází k upozorňování na výskyt možných bezpečnostních problémů. Tato diplomová práce je zaměřena na analýzu bezpečnostních rizik v rámci systému GSM. Na základě analýzy technické proveditelnosti a stupni rizika takovýchto útoku budou následně realizovány vybrané typy útoků. Tyto útoky jsou provedeny za využití open-source nástrojů, softwarově programovatelného rádia USRP a DVB-T přijímače.

V první části práce je čtenář seznámen s teoretickými podklady rádiového rozhraní systému GSM společně s popisem bezpečnostních mechanismů tohoto systému. Následuje analýza známých bezpečnostních hrozeb společně s popisem již realizovaných útoků.

V praktické části pak jsou realizovány a popsány 3 typy útoků: IMSI catcher, aktivní odposlech s podvržením základnové stanice a pasivní odposlech. IMSI catcher slouží k zachycení identifikátoru IMSI. IMSI je citlivý údaj umožňující jednoznačnou identifikaci koncového uživatele. Při aktivním odposlechu dochází k provozu podvržené základnové stanice, ke které se připojí mobilní stanice v dané oblasti, což umožňuje útočníkovi přístup k veškeré komunikaci. Třetím typem pak je pasivní odposlech komunikace v síti GSM s využitím levného DVB-T přijímače.

Tato práce také v poslední části rozebírá možná opatření pro snížení bezpečnostních rizik.

1 Vlastnosti GSM/UMTS sítí

V této kapitole je čtenář seznámen se základními pojmy, rozdělením, funkčním uspořádáním a vlastnostmi jednotlivých generací mobilních telekomunikačních systémů.

Historicky lze z vývojového hlediska rozdělit mobilní systémy do 4 generací.

Mobilní systémy, které pracovaly s analogovým signálem, jsou řazeny do 1. generace. Dalším vývojovým krokem jsou pak první digitální systémy 2. generace. V souvislosti s potřebou zvládat náročnější datové přenosy v mobilní síti pak vznikají systémy 3. a v současnosti i 4. generace[1].

1. generace - analogové mobilní systémy

2. generace - GSM

3. generace - UMTS

4. generace - LTE

Obecně se však lze v různých publikacích setkat i s neoficiálními mezistupni mezi jednotlivými výše popsanými generacemi (např. 2.5 generace označující GPRS, popř. 3.5 generace pro technologii HSDPA).

Stručně budou v následujících podkapitolách popsány systémy 1., 3., a 4. generace. Pro potřeby praktické části této diplomové práce je pak podrobněji popsána funkčnost systému 2. generace – GSM.

1.1 1. generace

První předchůdci mobilních telefonních systémů začali vznikat v průběhu 70. let 20. století. Ve většině případů se jednalo o komerční služby rozšiřující možnosti připojení ke klasické veřejné telefonní síti pomocí bezdrátových zařízení. Mobilní stanice byly většinou montovány do osobních a nákladních automobilů z důvodu svých velkých rozměrů a nadměrné hmotnosti.

Systémy 1. generace jsou někdy také nazývány analogovými telekomunikační systémy. Mezi nejrozšířenější zástupce této generace patřil systém NMT (Nordic Mobile Telephony) a systémy AMPS a TACS. [1]

V těchto systémech je obvykle analogový signál modulován na nosné frekvence v rozmezí 250 až 450 MHz (u NMT 900 pak 900 MHz). Lídrem ve vývoji mobilních sítí 1. generace byly skandinávské země Norsko, Finsko a Švédsko, jelikož se například u NMT jednalo o bezplatně přístupnou specifikaci, došlo krátce po nasazení do provozu k podstatnému rozšíření (v roce 1985 ve Skandinávii 110 tis. uživatelů).[1]

NMT – Buňky systému NMT mají velikost od 2 do 30 km. Menší buňky se využívají ve městech k navýšení kapacity současně prováděných hovorů.[2]

Pro obousměrnou komunikaci je u NMT využito plně duplexního provozu, což znamená, že během hovoru dochází k přijímání i vysílání signálu současně. Automobilové stanice mají vysílací výkon až 15 W (NMT-450) resp. 6 W (NMT-900), ruční mobilní stanice pak do 1 wattu. Hlavní výhoda NMT oproti předchozím komunikačním systémům je podpora přecházení mezi základnovými stanicemi, podpora pro mezinárodní roaming a specifikace účtování přímo ve standardu. [2]

V původní verzi NMT nebylo použito žádné bezpečnostní kódování přenášeného hlasového signálu, což mělo za následek velice jednoduchou možnost zneužití pomocí libovolného rádiového přijímače pracujícího na dané frekvenci. Snaha o zvýšení bezpečnosti hovoru vedla k vypuštění NMT pásem z rozsahu přijímačů.[2] Toto řešení je však z pohledu narušitele sítě naprosto banální. Proto došlo v dalších vývojových verzích technické specifikace k zavedení metody scramblingu. V analogovém přenosu se jednalo o úpravu signálu před vlastním vysíláním do nezabezpečeného kanálu a poté byl na přijímacím zařízení signál reverzně převeden zpět do původní podoby. Scrambling mohl byt provozován dvěma způsoby - scrambling mezi základnovou a mobilní stanicí nebo scrambling mezi dvěma mobilními stanicemi.[2]

1.2 2. generace

Sítě první generace po svém prvotním rozmachu rychle narážejí na své hranice způsobené analogovou podstatou systému. Bylo potřeba razantně navýšit kapacitu sítě, kvalitu a rozsah poskytovaných služeb stejně jako snížit cenu, která by umožnila masovější rozšíření technologie. Mobilní systémy 2. generace přecházejí od analogového zpracování signálů k digitálnímu.

Nejrozšířenějším digitálním systémem 2. generace se celosvětově stalo GSM. Mezi další systémy pak patří:

- ADC (IS-54, D-AMPS) - americký standart, který byl zpětně kompatibilní s analogovým systémem AMPS [3]
- JDC - japonský standart nasazený od roku 1991 [3]

1.2.1 Historie a vývoj GSM

V průběhu 80. let dochází především v Evropě k prudkému rozvoji různorodých analogových mobilních systémů, což sebou přináší několik podstatných problémů - neslučitelnost jednotlivých systému, které vedou k nepoužitelnosti mobilního zařízení za hranicemi jednotlivých zemí. Tato rozmanitost měla také ekonomické problémy, jelikož výrobce zařízení nemohl dodávat z důvodu kompatibility své výrobky na ostatní trhy ve sjednocující se Evropě. Z těchto důvodů byla organizací CEPT (Konference evropských správ a pošt) vytvořena v roce 1982 nová standardizační skupina GSM (Groupe Spécial Mobile)[2], jejímž úkolem bylo vytvořit standarty pro nový digitální systém, který by byl kompatibilní v zemích celé Evropy resp. světa.

Pro vývoj nového systému byly definovány především následující požadavky[2]:

- důraz na nízkou cenu zařízení a služeb
- kvalitní přenos lidské řeči
- podpora mezinárodního roamingu
- frekvenční hospodárnost - maximalizace kapacity sítě
- podpora ISDN služeb

V roce 1987 byla přijata první technická specifikace systému GSM. V tomto roce bylo 13 zeměmi Evropy jednotně přijato MoU (Memorandum of Understanding) o vývoji a spolupráci jednotného evropského buňkového telefonního systému, díky tomuto rozhodnutí vstoupili do procesu vývoje se svými finančními prostředky operátoři, což umožnilo výrazně zrychlit vývoj.[2]

V roce 1989 byla správa nad vývojem GSM převedena pod ETSI (Evropský telekomunikační standardizační institut). V následujícím roce byl ukončen vývoj primární specifikace, která byla publikována jako GSM - Phase 1.

Některé součásti specifikace GSM - Phase 1[3]:

- základní hlasové a faxové/datové služby
- mezinárodní roaming
- předávání a blokování hovorů
- služba SMS
- SIM karta a šifrování

První hovor v síti GSM byl proveden v roce 1991 mezi soudobým premiérem Finska Harrim Holkerim a starostkou města Tampere Kaarina Suonio.[2] Na základě specifikace GSM - Phase 1 vznikají v Evropě první komerční sítě a byla také uzavřena první roamingová smlouva mezi Velkou Británií a Finskem.

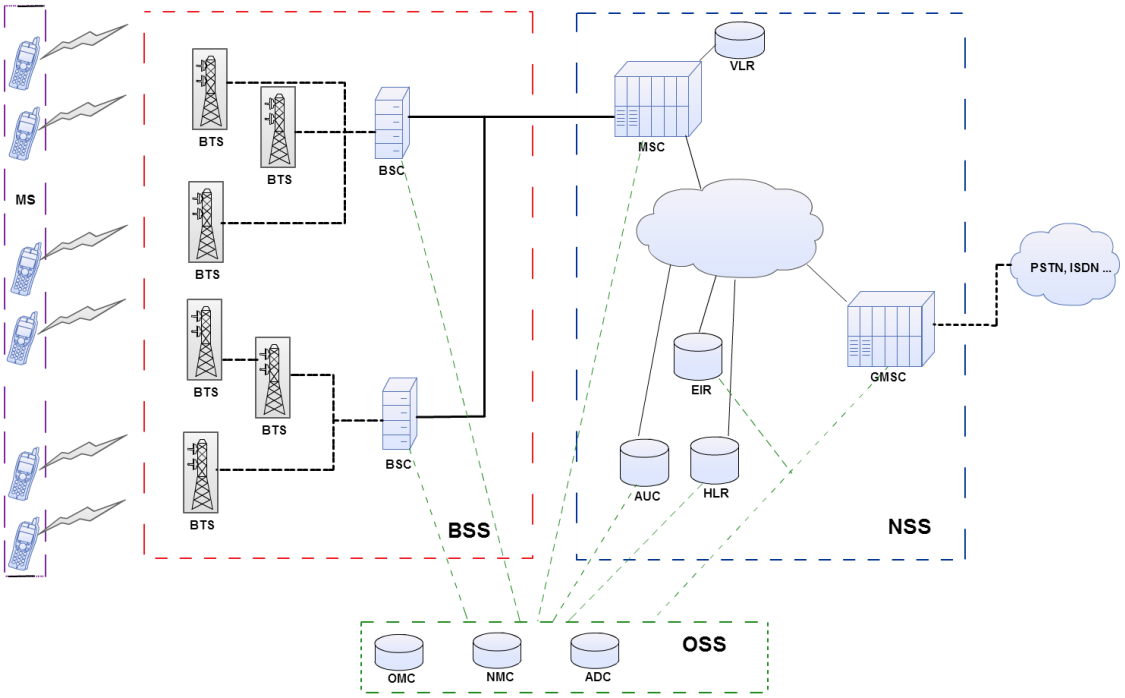
Souběžně se zaváděním GSM - Phase 1 do provozu pokračovala také práce na dalším vývoji standartu GSM. O necelé dva roky později přišla specifikace GSM Phase 2, která již definovala rozšířené služby, jako je například tarifikace hovorů na mobilním telefonu dle impulsů sítě, ale i identifikaci volajícího, konferenční hovory a další. Zároveň plně integrovala další frekvenci 1800 MHz (Digital Cellular System- DCS1800), která se pro systémy na bázi GSM začala také používat. V neposlední řadě GSM Phase 2 akceptovala požadavek na integraci některých funkcí (zejména kódování řeči enhanced full rate a half rate), které umožnily expanzi systému GSM i ve Spojených státech na frekvenci 1900MHz pod názvem PCS-1900.[3]

Některé součásti specifikace GSM - Phase 2[3]:

- GSM 1800 a 1900 MHz
- identifikace volaného a volajícího
- přidržení hovoru a konferenční hovory
- rozšířené možnosti datových služeb

1.2.2 Struktura sítě GSM

Z pohledu architektury můžeme GSM síť rozdělit do 4 základních logických částí. Rozdělení je znázorněno na obrázku 1.1. Struktura sítě GSM se skládá z těchto prvků: Mobilní stanice (MS) a 3 subsystémy; Subsystém základnových stanic (BSS), Síťový spojovací subsystém (NSS) a Operační a podpůrný subsystém (OSS).



Obrázek 1.1: *Struktura sítě GSM*

Vysvětlivky k obrázku:

MS – mobilní stanice
BSS – subsystém základnových stanic
BSC – základnová řídící jednotka
BTS – základnová radiostanice
NSS – síťový spojovací subsystém
MSC – mobilní spínací ústředna
HLR – domovský lokační registr

AUC – centrum autentičnosti
EIR – registr mobilní komunikace
VLR – návštěvnický lokační registr
OSS – operační a podpůrný subsystém
OMC – provozní a servisní centrum
NMC – centrum managementu sítě
ADC – administrativní centrum

1.2.2.1 ***Mobilní stanice (MS)***

Koncové zařízení, které slouží uživateli pro přístup k síti. V současnosti se nejčastěji vyskytují v podobě mobilního telefonu, tabletu nebo USB modemu.

Dle specifikací GSM se mobilní stanicí rozumí jednak vlastní mobilní zařízení (ME-Mobile Equipment), navíc také předplatitelský identifikační modul SIM (Subscriber Identification Module) - ten umožňuje unikátní identifikaci uživatele v rámci celé sítě GSM.[2][2]

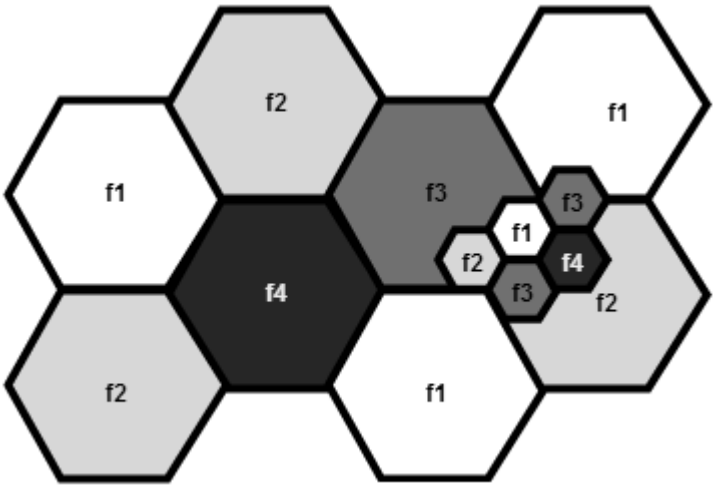
Mobilní zařízení (ME) - tvořeno rádiovým přijímačem/vysílačem sloužícím ke komunikaci se základnovou stanicí, obvody pro zdrojové a kanálové kódování a další součásti pro komunikaci s uživatelem. Uživatelské prvky mobilního zařízení jsou displej, mikrofon, reproduktor popř. klávesnice. Pro komunikaci s jinými zařízeními může obsahovat obvody pro obsluhu dalších rozhraní (Bluetooth, NFC apod.). Mobilní zařízení je identifikováno pomocí čísla IMEI, které je trvale uloženo v paměti.[2]

Karta SIM - je nedílnou součástí MS, která by byla, s výjimkou tísňového volání, bez této karty nepoužitelná. V paměti SIM jsou uloženy její identifikační údaje, dále uživatelské čtyřmístné identifikační číslo PIN (Personal Identification Number) a neměnné identifikační číslo PUK (Personal Unblocking Key). Úkolem SIM karty je autentizace uživatele a identifikace služeb jemu přístupných. Karta je přenosná a lze ji použít s libovolným mobilním telefonem.[2] SIM dále uchovává číslo IMSI sloužící k jednoznačné identifikaci uživatele, údaje potřebné k autentizaci MS vůči síti (klíč K_i), dále některé dočasné údaje – klíč pro šifrování komunikace K_C, TMSI pro dočasnou identifikaci uživatele, identifikátor buňky, číselný kód oblasti LAI. [2][3]

1.2.2.2 ***Subsystém základnových stanic (BSS)***

Jedná se o subsystém, se kterým prostřednictvím rádiového rozhraní komunikují jednotlivé mobilní stanice. Obvykle se BSS skládá z jedné či více základnových stanic BTS, které jsou řízeny jedinou BSC, viz obrázek 1.1. Systém provádí překódování hovorových kanálů, přidělování hovorových kanálů mobilním stanicím (MS), handover a další. Systém GSM je tvořen typicky buňkami o velikosti 1-3 km v průměru (v oblastech s nízkým provozem lze využít buňky až o velikosti 35 km). Buňky jsou slučovány do větších celků tzv. svazků. U 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). Při sektorizaci dojde k navýšení kapacity svazku pomocí využití směrových antén, kdy každá vyzařuje v sektoru 120°.[2][3]

Buňková struktura GSM sítě umožňuje ve srovnání s tradičními systémy poskytnout vyšší kapacitu s využitím minimálních rádiových prostředků.[2] Struktura umožňuje několika násobné znovu-využití přidělené rádiové frekvence. Z důvodů vzájemné interference je potřeba dodržet využití rozdílných frekvencí v sousedících buňkách. Buňková struktura sítě je zobrazena na obrázku 1.2.



Obrázek 1.2: *Buňková struktura GSM*

Základnová stanice (BTS) – Zařízení zajišťující bezdrátovou komunikaci mezi koncovými zařízeními (MS) a sítí, modulaci a demodulaci signálu, kódování, opravu chyb, handover mezi sektory a měření kvality signálu. Skládá se z vysílací a přijímací části.[2]

Základnová řídicí jednotka (BSC) – stará se o provoz rádiového rozhraní. Přiděluje a uvolňuje rádiové kanály pro komunikaci BTS s MS, řídí handover, frekvenční přeskoky. BSC zpravidla odpovídá za řízení několika desítek BTS. [2]

1.2.2.3 ***Síťový spojovací subsystém (NSS)***

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. Subsystém NSS dále realizuje celou řadu specifických úloh, spojených s mobilitou účastníků.[2]

Domovský lokační registr (HLR) - Tato v podstatě databáze slouží k ukládání veškerých údajů o uživatelích sítě jednotlivého operátora. Obsahuje mimo jiné důležitá čísla IMSI , MSISDN, 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.[2]

Identifikační registr stanic (EIR) - Na registr HLR je dále napojen identifikační registr mobilních stanic EIR. V této databázi jsou uložena čísla IMEI 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.[2]

Návštěvnický lokační registr (VLR) – Pro bezproblémovou mobilitu účastníků je využíván 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.[2]

Centrum autentičnosti (AuC) - Obsahuje informace potřebné k autentizaci SIM a možnosti zavedení šifrovaného spojení mezi MS a BTS. V mnoha případech je AuC implementováno jako součást domovského registru. Pro každé uživatelské číslo IMSI je obsažen klíč K_i a použitý šifrovací algoritmus A3 a A8. Stejné hodnoty jsou uloženy i na odpovídající SIM.[2][4]

1.2.2.4 ***Operační a podpůrný subsystém (OSS)***

Poslední částí GSM architektury je operační a podpůrný subsystém, jehož součástí je provozní a servisní centrum (OMC), řídící dohledové centrum (NMC) a administrativní centrum (ADC). Mezi hlavní funkce OSS patří kontrola a údržba NSS a BSS, management a monitoring mobilních stanic včetně jejich registrace a tarifikace.[3]

1.2.3 **Rozhraní sítě GSM**

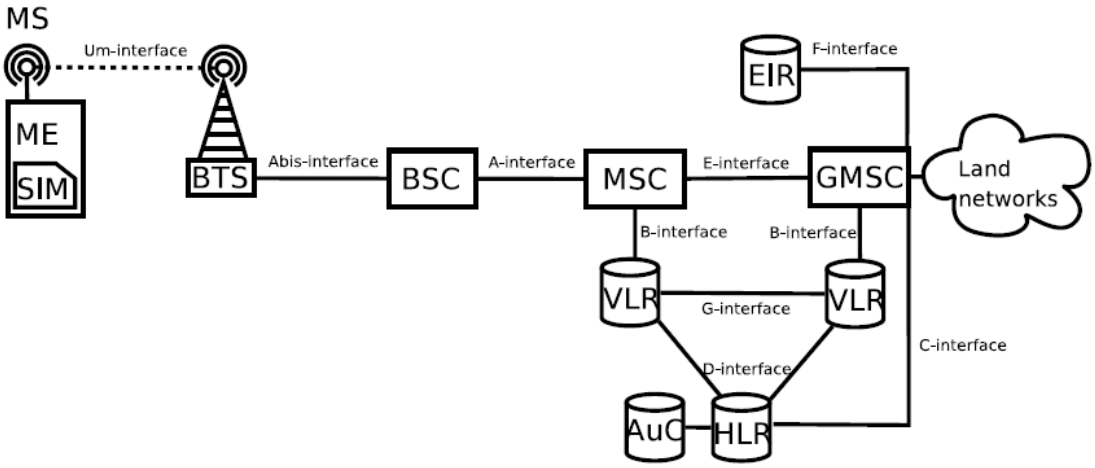
V síti GSM je definováno několik rozhraní sloužících k vzájemné komunikaci mezi jednotlivými částmi. Mezi rozhraní, které slouží k propojení MS s pozemní telefonní sítí (PSTN) patří: U_m, A_{bis}, A a E. Pro tyto rozhraní jsou definovány logické kanály určené pro přenos uživatelských dat - tzv. traffic channels a kanály sloužící k přenosu řídících dat - tzv. signalizační/řídící kanály.[5] Jednotlivé rozhraní můžete vidět na obrázku 1.3.

Rozhraní B, C, D, F a G slouží k synchronizaci různých informací v zázemí sítě. Implementace rozhraní mezi AuC a HLR není oficiálně definováno[5] a záleží proto pouze na provozovateli sítě. Jak již bylo zmíněno často tak dochází k vzájemné integraci těchto součástí.

Jelikož se v další části této diplomové práce pracuje s rádiovou komunikací na rozhraní Um, bude toto rozhraní podrobněji popsáno v další kapitole.

Rozhraní A_{bis} slouží k propojení BTS a řídícím centrem BSC. Toto rozhraní vychází ze standardizovaného rozhraní ISDN - LAPD a zprávy na tomto rozhraní se velké míře shodují se zprávami na druhé vrstvě rozhraní Um. [5]

Rozhraní A je pak definováno pro propojení subsystémů BSS a NSS, rozhraní E pak jako hlavní rozhraní subsystému NSS. Signalizační kanály rozhraní A a E jsou součástí SS7 - soubor signalizačních protokolů definovaných mezinárodní telekomunikační unii – ITU.[5]



Obrázek 1.3: *Rozhraní GSM*

[Zdroj: VAN DEN BROEK, Fabian. Catching and Understarstanding GSM-Signals]

1.2.4 U_m – Rádiová vrstva

Rozhraní mezi mobilní a základnovou stanicí je oficiálně nazýváno Um. Pojmenování vychází z ekvivalentního rozhraní U definovaného v ISDN. Jedná se o plně duplexní rozhraní s využitím metody frekvenčního odstupu (FDD) pro oddělení uplink (MS -> BTS) a downlink (BTS -> MS) komunikace.

Ačkoliv je rozhraní definováno jako duplexní, většina mobilních zařízení není schopna signál vysílat a přijímat současně. Toto je řešeno rychlým přepínáním mezi přijímačem a vysílačem.[5]

Systém GSM využívá pro modulaci signálu gaussovou modulaci MSK, tj. GMSK – kdy je před vlastní modulaci zařazen Gaussův filtr, který snižuje výkonovou úroveň v postranních pásmech a zvyšují tak spektrální efektivnost této modulace ve srovnání s jinými modulacemi. [11]

Pro navýšení kapacity systému bylo přistoupeno k využití dvou metod pro mnohonásobný přístup:

FDMA - (Frequency Division Multiple Access) mnohonásobný přístup pomocí frekvenčního odstupu

TDMA - (Time Division Multiple Access) mnohonásobný přístup pomocí časového odstupu

1.2.4.1 ***FDMA***

Při návrhu GSM sítě se počítalo s možností současného vysílání vyššího počtu MS. K tomu, aby nedocházelo k vzájemnému rušení je pásmo GSM rozděleno na jednotlivé kanály o šířce 200 kHz. V případě využití dvou sousedních rádiových kanálů může docházet

k vzájemnému rušení, proto není možno použít sousední kanály v rámci jedné buňky. Ostatní kanály pak mohou být současně využity bez vzájemného rušení. [3]

Jelikož se jedná o duplexní kanál, je pro každý kanál určena dvojice frekvencí - jedna pro uplink druhá pak pro downlink. Odstup obou směrů můžete vidět v tabulce 1.1.

Tabulka 1.1: *Frekvenční pásma GSM*

Název	Uplink (MHz)	Downlink (MHz)	Odstup (MHz)	Číslo kanálu (ARFCN)
GSM-450	450,4-457,6	460,4-467,6	10	259-293
GSM-480	478.8-486	488.8-496	10	306-340
GSM-850	824-849	869-894	45	128-251
GSM-900	890-915	935-960	45	1-124
EGSM-900	880-915	925-960	45	975-1023, 0-124
GSM-1800	1710-1785	1805-1880	95	512-885
GSM-1900	1850-1910	1930-1990	80	512-810

ARFCN (Absolute Radio Frequency Channel Number) - Každá dvojce kanálů je označena absolutním číslem frekvenčního kanálu. Pro GSM-900 nabývá ARFCN hodnot 1 až 124.

Na základě ARFCN je pak možno dopočítat dvojici odpovídajících frekvencí.[2]

Pro GSM 900:

$f_{uplink} = 890 + 0{,}2 \times ARFCN\ [MHz]$ $f_{downlink} = f_{uplink} + 45\ [MHz]$

Kapacita pásma GSM 900 se brzy ukázala pro praxi jako nedostatečná a došlo k alokaci dalších pásem: EGSM-900 popř. GSM-1800. Podrobnější informace o pásmech je možno nalézt v tabulce 1.1.

Jedna BTS obvykle obsahuje 16 TRX (transceiver), což umožňuje současně obsluhovat 8 kanálů ARFCN - 8 uplink + 8downlink[5]

1.2.4.2 ***Frekvenční přeskoky***

Šíření signálu bezdrátovým prostředím je obecně náchylné na vnější vlivy jakými mohou být např. atmosférický ruch, interference, vícecestné šíření signálu apod. Pro udržení co nejvyšší přenosové kvality může být na straně BTS zavedena technika frekvenčních přeskoků - FH (Frequency Hopping). Podpory ze strany všech MS je zajištěna ve specifikaci GSM.[9]

Pro potřeby GSM byla zvolena metoda SFH (Slow Frequency Hopping), k přeskokům dochází cca každých 4.615ms, což je doba odpovídající jednomu TDMA rámci, tak aby byla

MS schopna naslouchat dalšímu přidělenému časovému slotu - TS (Time Slot). FH je vždy inicializováno ze strany BTS, která zašle MS veškeré parametry potřebné k výpočtu sekvence kanálů pro jednotlivé přeskoky.[5][6]

1.2.4.3 ***TDMA***

Metoda mnohonásobného přístupu TDMA umožňuje současný přístup více zařízení na jednom fyzickém kanálu. Jednotlivé signály jsou vysílány pouze v krátkých pevně definovaných intervalech nazývaných časové sloty (TS - time slot). Prakticky se využívá sloučení jednotlivých slotů jednoho TDMA rámce.

V systému GSM je metodou TDMA každý fyzický nosný kanál rozdělen na 8 TS. Pro jedno koncové zařízení je pak FDMA/TDMA kanál pro přenos signálu definován číslem TDMA rámce, přiděleným time slotem a volitelně sekvencí frekvenčních přeskoků.

Základní jednotkou v systému GSM je tak jeden TS o délce 576,9 μs, při modulační rychlosti 270.833 kbit/s je pak velikost jednoho TS 156,25 bit. Obsah jednoho TS se nazývá burst. [9]

1.2.4.4 ***Burst***

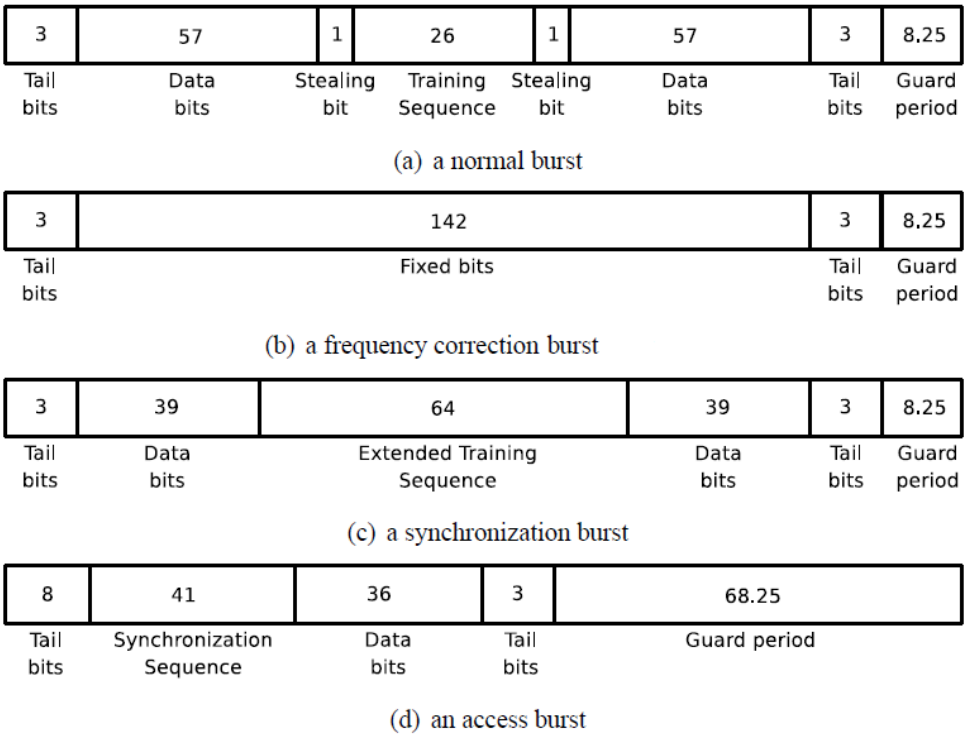
V systému GSM jsou rozlišovány 4 typy burstů [5]. Struktura burstů je znázorněna na obrázku 1.4

- NB - Normal Burst - tento burst je využíván k přenosu informace na logických kanálech TCH (Traffic Channel) a CCH (Control Channel), kromě RACH, normální burst je tvořen 116 bity dat a ochranným časem - tzv. guard time o délce 8,25 bit. Tréninková sekvence pak pomocí předdefinované sekvence bitů umožňuje resynchronizaci přijímače pro omezení vlivů interference.[5]

- FB - Frequency Correction Burst - burst určený pro frekvenční synchronizaci MS. Sekvence FB vytváří kanál FCCH. Pole fixed bits je tvořeno 142 standardně modulovanými hodnotami '0'. Toto umožní MS nalézt základní frekvenci BTS a přizpůsobení přijímače.[5]

- SB - Synchronization Burst - základní funkcí SB je časová synchronizace MS, burst obsahuje prodlouženou tréninkovou sekvenci a 2 datové části o velikosti 39 bitů obsahující informaci o číslu TDMA rámce a identifikačním kódu základnové stanice (BSIC). SB jsou odesílány na logickém kanále SCH.[5]

- AB - Access Burst - přístupový burst může být vysílán pouze MS a je odeslán pouze na kanálu RACH, jelikož BTS nezná přesnou polohu MS je potřeba tomuto burstu poskytnout delší guard time. Data v tomto burstu obvykle obsahují žádost MS o komunikaci a následuje ze strany BTS přidělení SDCCH pomocí normálního burstu.[5]



Obrázek 1.4: *Přehled burstů*

[Zdroj: VAN DEN BROEK, Fabian. Catching and Understarstanding GSM-Signals]

1.2.4.5 ***Rámce sítě GSM***

Jeden TDMA rámec v síti GSM je tvořen 8 bursty, jehož délka je 4,615 ms (8 x 576,9 µs). TDMA rámce následně tvoří multi-rámce. Rozlišují se 2 základní typy multi-rámcu : multi-rámec přenosového kanálu a multi-rámec signalizačního kanálu. [9]

Multi-rámec přenosového kanálu je složen z 26 TDMA rámců (120ms), pro signalizační kanál to je pak 51 TDMA rámců (235,4 ms). Tyto multi-rámce jsou opět sdružovány do větších celků nazývaných super-rámce, které je opět možno rozdělit podle typu kanálu na přenosové a signalizační. [9]

Super-rámec přenosového kanálu je složen z 51 multi-rámců přenosového kanálu, signalizační super-rámec je složen z 26 multi-rámců. Z tohoto vyplývá, že délka obou typů super-rámců je shodná (51*26*4,615 ms = 6119,49 ms). Největší jednotkou v rámci TDMA je tzv. hyper-rámec, který je tvořen 2048 super-rámci. Délka tohoto rámce je pak 12 533,76 s a je celkově složen z 2 715 648 TDMA rámců (51*26*2048). Jednotlivé TDMA rámce jsou následně číslovány podle pořadí v super-rámci. Pořadí TDMA rámce je pak jedním z parametrů pro šifrování komunikace.[6][9] Rozložení rámců je podrobně znázorněno na obrázku 1.5.

1.2.4.6 ***Logické kanály sítě GSM***

Systém GSM definuje širokou řadu logických kanálů, které jsou podle svého účelu tvořeny různými typy burstů. Logické kanály GSM můžeme rozdělit podle své funkce na přenosové kanály (TCH – traffic channel) a signalizační kanály (CCH – control channel). Přenosové kanály jsou určeny k přenosu hlasových popř. dalších dat. Signalizační kanály, jak už název napovídá, slouží k řízení provozu v rámci GSM systému. Celkový přehled logických kanálů je možné vidět v tabulce 1.2.

1.2.4.7 ***Přenosové kanály (TCH)***

Jsou určeny k přenosu hovorových mezi jednotlivými účastníky. Samotný hovor je převeden do sekvence bitů a přenesen pomocí TCH. GSM rozděluje 2 typy přenosových kanálů – Kanál s plnou rychlostí (TCH/F - Full rate) a kanál s poloviční rychlostí (TCH/H - Half rate). V případě TCH/F je kanál určen k přenosu hovorových dat jediného uživatele. Pro TCH/H je přenosový kanál rozdělen na dva kanály TCH/H a umožňuje tak sdílení jediného kanálu dvěma koncovými uživateli a tím dochází k dalšímu navýšení kapacity současně obsluhovaných uživatelů.[5]

1.2.4.8 ***Signalizační kanály (CCH)***

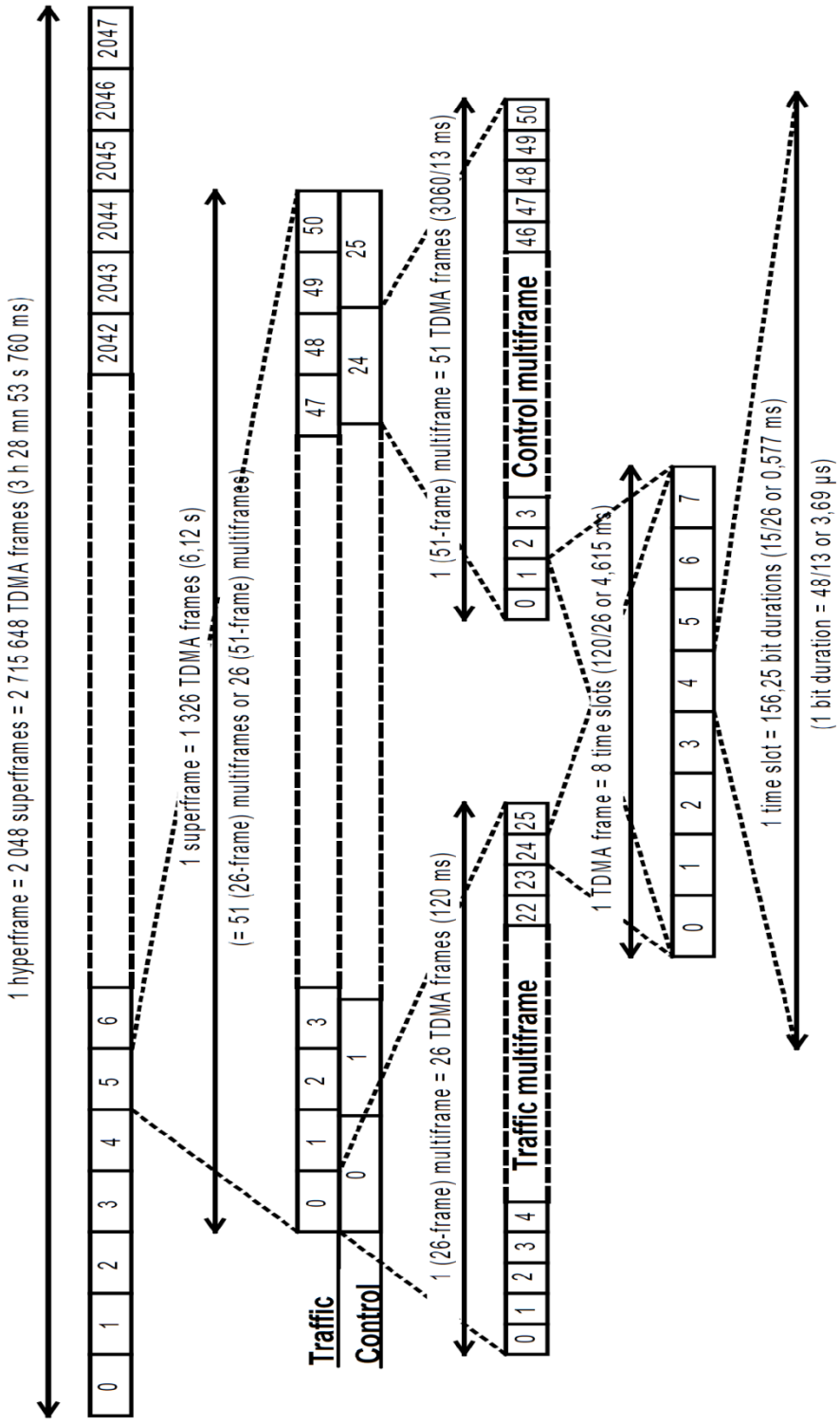
Toto je souhrnné označení pro všechny logické kanály, která nesou informace sloužící k řízení a údržbě komunikace v síti GSM. Systém GSM definuje 10 různých signalizačních kanálů, které můžeme pro potřeby popisu rozdělit do 3 podskupin: rozhlasové kanály (BCH – Broadcast Channel), kanály všeobecného řízení (CCCH – Common Control Channel) a vyhrazené řídící kanály (DCCH – Dedicated Control Channel).[5]

BCH

Kanály BCH slouží k propagaci systémových a synchronizační informací. Tyto kanály jsou vysílány pouze ve směru downlink (BTS -> MS).

Broadcast Control Channel (BCCH) – tento všeobecný rozhlasový kanál je určen k přenosu systémových informací potřebných k identifikaci sítě a možnosti připojení. Toto zahrnuje parametry LAC, MNC, MCC, frekvence sousedních BTS a informace o dalších signalizačních kanálech. MS také využívá BCCH k měření síly signálu a následnému rozhodování o přepojení k nejvhodnější BTS. Tomuto kanálu naslouchají všechny MS.[5][6]

Frequency Correction Channel (FCCH) – kanál informace umožňující korekci naladění mobilní stanice a identifikaci kmitočtu nesoucího signalizační kanály. Tvoří ho bursty pro kmitočtovou korekci.[5][6]



Obrázek 1.5*: Struktura rámců GSM*

[Zdroj: GSM 05.01 version 5.4.0]

Synchronization Channel (SCH) – kanál nesoucí informace o aktuálním číslu TDMA rámce, umožňující MS následnou rámcovou synchronizaci. Tento kanál také nese identifikátor BSIC (Base station identity code) sloužící k rozlišení BTS vysílajících na stejné frekvenci.[5][6]

Cell Broadcast Channel (CBCH) – kanál určený k přenosu různých informací k všem uživatelům v jedné buňce. Pro přenos sice využívá vyhrazený kanál, ale svým principem, kdy je šířen mezi všechny účastníky, spadá do kategorie rozhlasových kanálů (BCH).[5][6]

CCCH

Tyto kanály jsou určeny k signalizaci mezi BTS a MS a obstarávají především žádosti a přidělení přístupu k přenosovým popř. dalším signalizačním kanálům.

Paging Channel (PCH) – Kanál informující MS o příchozím přenosu (hovor, SMS či signalizace). Jednotlivé MS mohou být identifikovány pomocí IMSI nebo TMSI. Tento kanál je sledován každou MS v okamžiku kdy se nachází ve stavu pohotovosti. [5][6]

Random Access Channel (RACH) – Tento kanál umožňuje MS odeslat požadavek o zahájení komunikace. Po odeslání požadavku na RACH následuje výzva směrem k MS pomocí kanálu AGCH. [5][6]

Access Grant Channel (AGCH) – Slouží k přidělení samostatného signalizačního kanálu MS, která o něj požádala. [5][6]

DCCH

Pomocí těchto kanálů je prováděná point-to-point signalizace mezi MS a BTS za účelem sestavení hovoru, řízení handoveru, procedury location update nebo k dalším řídicím funkcím.

Standalone Dedicated Control Channel (SDCCH) – samostatný signalizační kanál sestavuje hovory, provádí location update, řídí autentizaci a identifikaci uživatele nebo slouží k přenosu SMS zpráv. Na rozdíl od ostatních DCCH není tento kanál přidružen k žádnému z dalších kanálů. [5][6]

Slow Associated Control Channel (SACCH) - tento pomalý přidružený kanál zajišťuje signalizaci k existujícímu spojení. Bývá přidružen ke kanálu TCH nebo SDCCH způsobem, že nahradí jeden z burstu TDMA rámce daného kanálu. [5][6]

Fast Associated Control Channel (FACCH) – Tento kanál může být přidružen ke kanálu TCH, kterému „ukradne“ jeden z jeho burstu v případě potřeby. Toto slouží především k signalizaci neočekávaných událostí jako je ukončení hovoru nebo handover. [5][6]

1.2.4.9 ***Kombinace kanálů***

Všechny výše popsané kanály mohou být provozovány na samostatném rádiovém kanálu ARFCN. Toto rozdělení je však pro praxi v ohledu na omezené množství frekvencí

nepoužitelné. Proto je umožněno sdílení všech logických kanálů na jediném fyzickém kanálu ARFCN.

Tabulka 1.2: *Přehled logických kanálů*

Logické kanály	Směr komunikace
Přenosové (TCH)	
TCH/F	obousměrný
TCH/H	obousměrný
Signalizační (CCH)	
BCH	
BCCH	downlink
FCCH	downlink
SCH	downlink
CBCH	downlink
CCCH	
PCH	downlink
RACH	uplink
AGCH	downlink
DCCH	
SDCCH	obousměrný
FACCH	obousměrný
SACCH	obousměrný

Ve specifikaci GSM jsou určeny následující možné kombinace[7][10]:

1) TCH/F + FACCH + SACCH
2) TCH/H + FACCH + SACCH
3) TCH/H + FACCH + SACCH + TCH/H
4) FCCH + SCH + BCCH + CCCH
5) FCCH + SCH + BCCH + CCCH + 4*SDCCH
6) BCCH + CCCH
7) SDCCH * 8 + SACCH *8

Kde kanál CCCH označuje kanály PCH + RACH + AGCH + NCH.

Nejčastěji je pak provozována konfigurace kdy pro TS 0 je zvolena možnost 4) FCCH + SCH + BCCH + CCCH, pro TS 1 pak konfigurace 7) a zbylé TS jsou určeny pro přenos hovorových dat v konfiguraci 1-3). Podrobnější informace k logickým kanálům je možné nalézt v [7], [10].

1.2.5 Um – Spojová vrstva

Tato část se bude podrobněji věnovat popisu druhé vrstvy rozhraní Um. Signalizační protokol provozovaný na spojové vrstvě se nazývá LAPDm a jedná se o upravenou variantu Link Access Protocol on the D channel (LAPD), který je používán v systémech ISDN.

Jak bylo v předchozích kapitolách zmíněno, signalizace i hovorová data jsou na rádiové vrstvě odesílány pomocí burstů. Spojová vrstva je však definována pouze pro signalizační kanály (CCH) a ne pro přenosové kanály (TCH) .

Komunikace na této vrstvě může být dle způsobu potvrzování přijatých dat rozdělena na potvrzovanou a nepotvrzovanou komunikaci. V případě potvrzované komunikace jsou data odesílána prostřednictvím informačních (I) rámců, jejichž přijetí je vždy potvrzováno (positive acknowledgment). Tento typ je možné použít pouze pro kanály DCCH. V případě nepotvrzované komunikace jsou data posílána prostřednictvím nečíslovaných informačních rámců (UI – unnumbered information) rámců. Tato komunikace neumožňuje na této vrstvě řízení provozu (flow control) nebo ochranu proti chybám. Tento způsob je určen pro kanály BCCH, PCH a AGCH. [3][5][9]

V případě, že celková délka rámce není 23 bytů je rámec doplněn doplňkovými (fill) bity.[5] Tato sekvence je definována jako $(0010\ 1011)_2$ což v hexadecimálním zápisu odpovídá hodnotě $(2b)_{16}$. Této vlastnosti systému GSM bylo následně využito pro prolomení šifrování, toto je popsáno v kapitole 4.2.

1.2.6 U_m – Síťová vrstva

Síťová vrstva je dále rozdělena na 3 podvrstvy, kdy jedna z podvrstev je dále rozdělena na 3 části. Na rozdíl od spojové vrstvy, rámce na síťové vrstvě nemají definovánu pevnou délku. Na síťové vrstvě tedy rozlišujeme [8]:

1) RR (Radio resource management) – vrstva správy rádiových zdrojů, která řídí konfiguraci logických a fyzických kanálů rozhraní U_m, řídí např. handover nebo správu výkonu.
2) MM (Mobility management) – tato podvrstva řeší funkce související s mobilitou účastníků – aktualizace polohy, identifikace a autentifikace účastníků.
3) CM (Comunication management) – správa komunikace, je dále rozdělena na 3 podvrstvy
    a. SS (Supplementary services) – obstarává správu doplňkových služeb a funkcí systému GSM
    b. SMS (Short Message Service) – řeší přijímání a odesílání SMS zpráv
    c. CC (Call Control) – zajišťuje vytváření, udržování a ukončování hovorů

V následujících podkapitolách jsou podrobněji rozebrány vybrané podvrstvy, na které je dále odkazováno v této práci.

1.2.6.1 ***Radio Resource Management***

V rámci síťové vrstvy se jedná o nejnižší podvrstvu, jejímž hlavním úkolem je přidělování a udělování logických kanálů. Některé ze zpráv, které tato podvrstva využívá, jsou popsány níže v tabulce 1.3, podrobnější informace je pak možno nalézt v [8].

Tabulka 1.3: *Zprávy podvrtvy RR*

Název	Směr	Popis
Channel Request	MS->BTS	MS odesílá požadavek na přidělení kanálu pro sestavení následné komunikace. Obsahuje důvod požadavku (např. odpověď na paging) a náhodné číslo jako referenci pro odpověď.
Cipher Mode Command	BTS->MS	Příkaz pro začátek šifrování komunikace na Um rozhraní, obsahuje informace o použitém šifrování (A5/x)
Immediate Assignment	BTS->MS	Zpráva přiřazující kanál pro další komunikaci. Umožňuje určit fyzický kanál ARFCN, logický kanál, TS nebo informace pro určení sekvence frekvenčních přeskoků.

1.2.6.2 ***Mobility Management***

Podvrstva MM využívá kanálu vytvořeného pomocí RR pro správu mobility uživatelů. Obstarává správu polohy, řízení pagingu a autentizaci uživatelů. Některé zprávy využívané touto podvrstvou jsou uvedeny v tabulce 1.4.[5][8]

1.2.6.3 ***Call Control***

Tato podvrstva obstarává sestavování a ukončování hovorů na základě spojení sestaveného na podvrstvě MM. Tabulka 1.5 popisuje některé ze zpráv CC. Podrobnější popis je možno nalézt v [8].

1.2.7 **Scénáře komunikace**

V této části je popsáno využití logických kanálů a řídících zpráv v rámci scénářů komunikace mezi MS a BTS, na které je dále odkazováno v praktické části této diplomové práce.

1.2.7.1 ***Registrace do sítě***

Location Registration, je zvláštní případ Location Update, kdy probíhá registrace MS do sítě a MS se identifikuje pomocí IMSI, jelikož ještě nemá přidělenu aktuální dočasnou identifikaci TMSI. Průběh registrace je zobrazen na obrázku 1.6 a)

Tabulka 1.4: *Zprávy podvrstvy MM*

Název	Směr	Popis
Location Update Request	MS->BTS	Požadavek MS o zahájení procesu aktualizace polohy, obvykle obsahuje informace o LAI, TMSI/IMSI a podporovaných typech šifrování. LUR může probíhat periodicky nebo v případě přihlášení MS do sítě.
Authentication Request	BTS->MS	Obsahuje náhodnou hodnotu RAND, která slouží k výpočtu SRES, popis autentizace je popsán v kap. 2.1.
TMSI Reallocation Commnad	BTS->MS	V případě úspěšného Location Update je MS touto zprávou přiřazena hodnota TMSI.

Tabulka 1.5: *Zprávy podvrstvy CC*

Název	Směr	Popis
Allerting	MS<->BTS	V případě příchozího hovoru tato zpráva oznamuje zahájení vyzvánění. V případě odchozího hovoru pak BTS oznamuje MS začátek vyzvánění u volaného.
Setup	MS<->BTS	Opět je odesílána v případě odchozího i příchozího hovoru. Nese informace o čísle volaného/volajícího (MSISDN), typ přenosového kanálu (full/half rate).
Connect	MS<->BTS	Touto zprávou MS oznamuje přijetí příchozího hovoru. V případě odchozího hovoru oznamuje BTS úspěšné vytvoření spojení.

V prvních dvou krocích probíhá proces sestavení spojení. Nejprve žádá MS prostřednictvím RACH o přidělení kanálu pro komunikaci (CHANnel_REQuest), obsahující důvod požadavku (Location Update) a referenční hodnotu, která následně identifikuje následující zprávu IMMediate_ASSignment_CoMmanD, aby MS věděla, která odpověď je určena pro předchozí požadavek, Immediate Assignment Command přidělí MS kanál SDCCH určený ARFCN a TS. Sestavení spojení je řízeno podvrstvou RR.

Po přístupu na přidělený kanál SDCCH, odešle MS požadavek LOCation_UPDate_REQuest. Tento požadavek slouží jako potvrzení o přijetí Imm. Ass. Command a obsahuje IMSI a předchozí hodnotu oblasti – LAI. Jedná se o zprávu podvrstvy MM a přijetí této zprávy musí být potvrzeno ze strany BTS.

Následuje autentizační fáze, autentizace je řízena podvrstvou MM. Odpovědí MS (AUTHentication_RESponse) na požadavek o autentizaci (AUTHentication_REQuest) je SRES vypočtený na základě náhodné hodnoty RAND v tomto požadavku. Podrobněji je proces autentizace popsán v kapitole věnující se zabezpečení - 2.1.1.

V případě, kdy má být následující komunikace šifrována následuje ze strany sítě zpráva CIPHer_MODe_CoMmanD, učující použitý šifrovací algoritmus A5/0-3. V okamžiku kdy je tato zpráva potvrzena MS pomocí CIPHer_MODe_COMplete je obousměrná komunikace šifrována.

Na šifrovaném kanálu pak může proběhnout zaslání různých identifikátorů MS (IMEI, IMEISV, IMSI, TMSI) pomocí zpráv IDENTity_REQuest/RESpones.

Přidělení nové hodnoty TMSI je pak provedeno pomocí TMSI_REALlocation_CoMmanD, jehož přijetí je potvrzeno TMSI_REALocation_COMplete. Celá procedura registrace je následně ukončena zasláním zprávy LOCation_UPDate_ACCept.[5][6]

1.2.7.2 ***Odchozí hovor***

Pro průběh odchozího hovoru (MOC – Mobile Originating Call) rozlišuje specifikace GSM 3 různé průběhy sestavení hovoru. Rozdílnost je v okamžiku, kdy je MS přidělen přenosový kanál TCH

Very Early Assignment – Na požadavek o odchozí hovor je ihned přidělen TCH a veškerá signalizace sestavování hovoru probíhá prostřednictvím přidruženého signalizačního kanálu FACCH, tento způsob však vede ke zbytečné alokaci TCH i v případě, kdy není hovor nakonec sestaven a proto není v praxi příliš využíván.

Early Assignment – V tomto případě je nejprve přidělen samostatný signalizační kanál SDCCH pro počáteční inicializaci hovoru (autentizace, šifrování, call setup), hovoru je dedikován přenosový kanál až v okamžiku před začátkem vyzvánění.

Late Assignment – Průběh spojení je velice podobná Early Assignment, rozdíl je v tom, že k sestavení hovoru dojde až po přijetí hovoru ze strany volaného.

Níže je podrobněji popsán průběh Early Assignment, který je nejčastěji využívaným způsobem sestavování hovorů. Průběh je pak zobrazen na obrázku 1.6 b)

Nejprve dojde stejně jako v případě registrace k požadavku MS o přidělení kanálu (Channel Request/Immediate Assignment Command). Na přiděleném signalizačním kanálu zašle MS požadavek o službu – CM_SERVice_REQuest, identifikující požadovanou službu, hodnotu TMSI, a identifikaci o použitém šifrovacím klíči – CKSN – Ciphering Key Sequence Number. Zahájení šifrování je pak shodné s průběhem v předchozím scénáři.

Po potvrzení služby a sestavení spojení na vrstvě MM (CM Service Accept) odešle MS zprávu CALL_SETUP – obsahující číslo volaného (MSISDN). Po ověření možnosti spojení následuje potvrzení přijetí hovoru – CALL_PROCeed. Následně dojde k přidělení přenosového kanálu pomocí ASSignment CoMmanD.

Jako potvrzení přechodu na TCH zašle MS prázdnou zprávu, která je poté potvrzena i ze strany sítě. Následná signalizace probíhá prostřednictvím FACCH. Do okamžiku přijetí hovoru na straně volaného je ze strany sítě odesílána zpráva ALLERT informující o vyzvánění. Po přijetí hovoru je zaslána zpráva CONnect a následuje výměna hlasových dat prostřednictvím TCH.[5][6]

1.3 3. generace

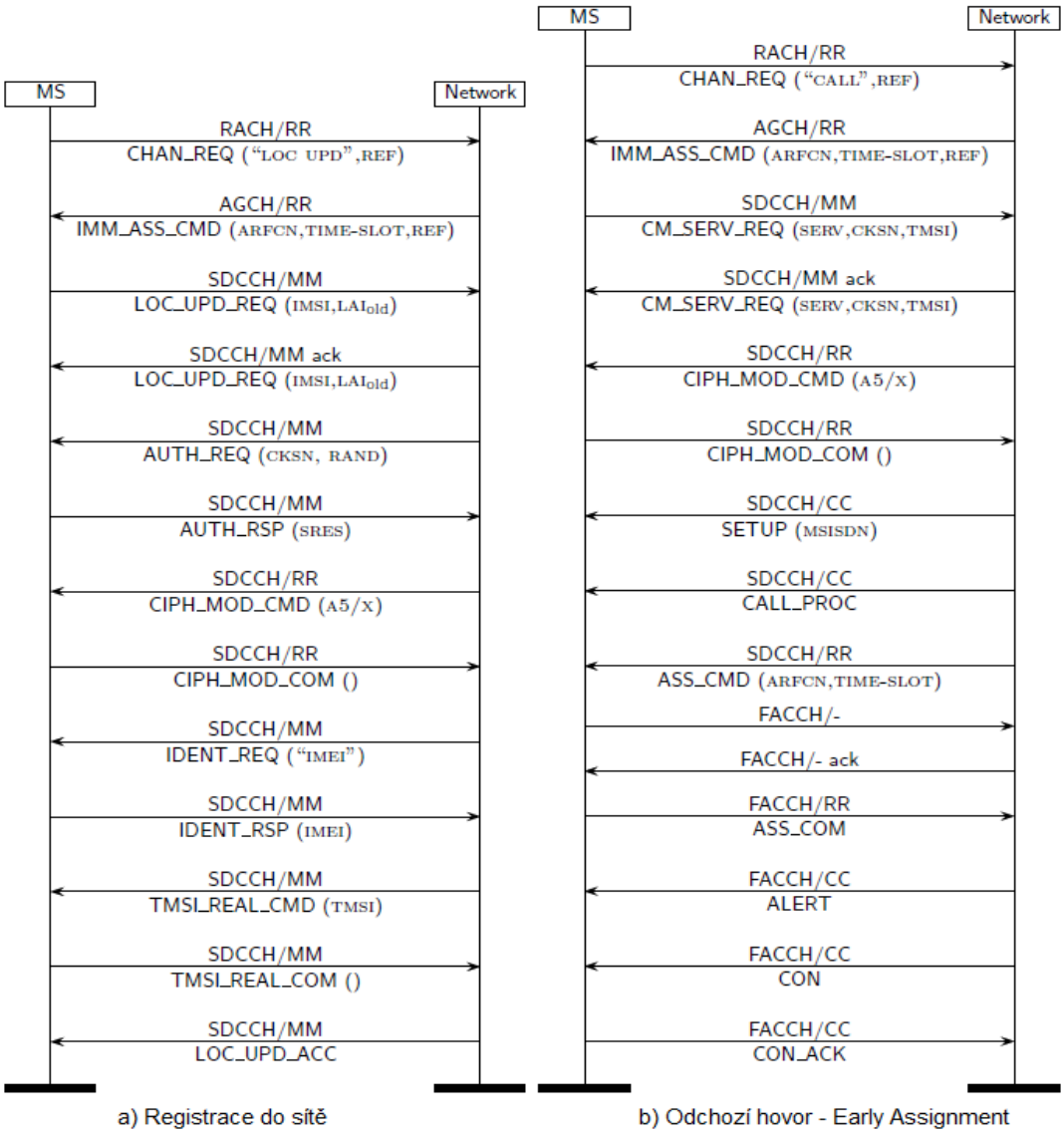
Po rozmachu hovorových služeb v síti GSM se v 90. letech minulého století začala rozvíjet poptávka po datových službách v této síti. Někdy jsou jako systémy 2,5. generace prezentovány nadstavby nad GSM sítí umožňující datové přenosy – GPRS, EDGE. Tyto služby však poskytují jen omezenou přenosovou kapacitu a rychlost, a proto bylo potřeba vytvořit celý nový systém, který poskytne širokopásmový přístup k datovým sítím.

Přehled některých požadavků na systémy 3. generace[2]:

- Zvýšení přenosových rychlostí současných systémů 2. generace na hodnoty až 2 Mbit/s
- Lepší využití rádiových frekvencí (vyšší spektrální účinnost modulací, účinnější zdrojové a kanálové kódování)
- Malé a levné terminály pro různé typy aplikací
- Široké spektrum služeb s různým stupněm kvality

1.3.1 Historie a vývoj UMTS

Organizace ITU proto zahájila první přípravné kroky pro definování nové sítě třetí generace. Projekt pod názvem IMT-2000 (International Mobile Telecommunications 2000) má své kořeny už v roce 1985. Číslovka 2000 znamená využití frekvence v oblasti 2000MHz, přenosovou rychlost 2000 kbps a definici do roku 2000. V roce 1992 pak bylo na mezinárodní konferenci WRC 92 v Malaze rezervováno pásmo 1885-2025 a 2110 a 2200 pro využití v systémech IMT-2000. [1]



Obrázek 1.6: *Průběh přidělení kanálů a výměny zpráv mezi MS a sítí*

[Zdroj: VAN DEN BROEK, Fabian. Catching and Understarstanding GSM-Signals]

V brzké době došlo k rozdělení vývoje systému 3. generace na dva hlavní směry – UMTS pro Evropu a CDMA2000 pro oblast USA. Vývoj systému UMTS byl převeden pod nově vytvořenou organizaci 3GPP, která publikovala první specifikaci v roce 1999.

Vlastnosti Release 99 [2]:

- hovorový kanál 64 kbps
- paketový přenos 384 kbps
- lokalizační služby
- kompatibilita s GSM

- kvalita hlasového přenosu

Tento standart položil základ pro budování UMTS sítě v Evropě. Do dnešní doby bylo vydáno několik dalších specifikací, které se především věnují zkvalitňování služeb, přechod jádra systému na protokol IP a navyšování přenosové rychlosti a kapacity. Prvního komerčního nasazení se síť UMTS dočkala v roce 2001 v Norsku. Problémem však byla nedostupnost koncových zařízení, které se postupně dostávaly na trh až ke konci následujícího roku.

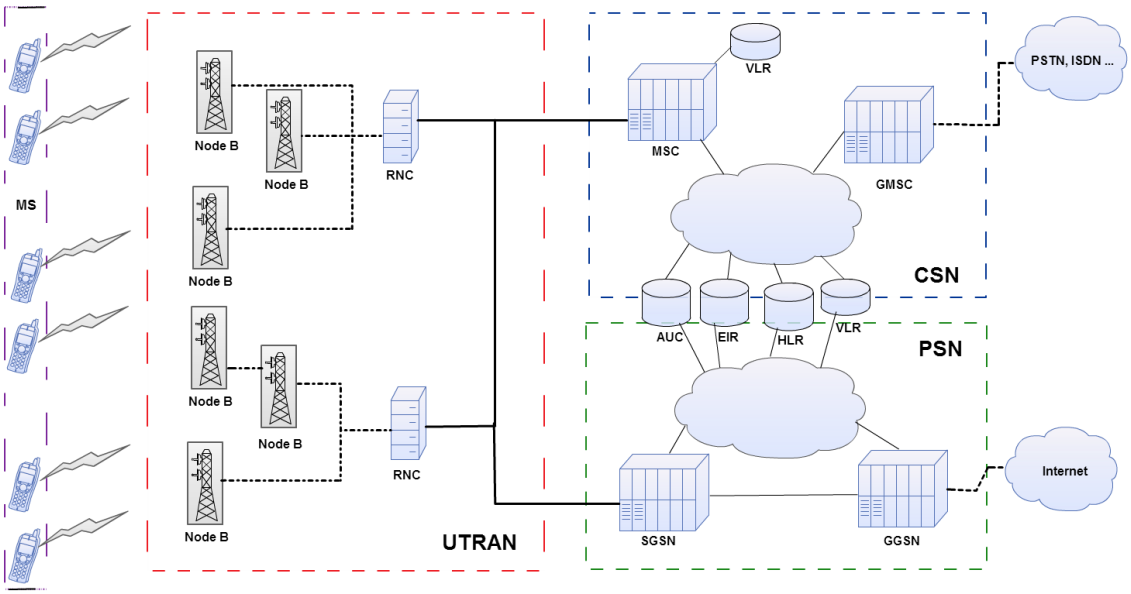
1.3.2 Struktura sítě UMTS

Systémy 2. generace byly primárně zaměřeny na přenos hlasových dat, zatímco UMTS je systém přinášející především širokopásmový datový přístup.[2]

Pro sítě 3. generace byla zvolena technologie CDMA (Code Division Multiple Access), což je přístupová metoda kódového dělení. Pro UMTS je použita její širokopásmová varianta W-CDMA (Wideband CDMA. Na rozdíl od TDMA u GSM u CDMA neexistuje žádné dělení na jednotlivé TS a všichni uživatelé používají přidělené frekvenční pásmo po celou dobu. Aby bylo umožněno rozpoznání jednotlivých uživatelů využívajících jedno frekvenční pásmo současně, dochází k přidělení binárního kódu jednotlivým uživatelům. Frekvenční spektrum se skládá z párového pásma (1920-1980 MHz + 2110-2170 MHz) a nepárového pásma (1910-1920 MHz + 2010-2025 MHz).[2] Podle typu pásma se používají rozdílné metody pro duplexní provoz:

- FDD (Frequency Division Duplex) pro párové pásmo;
- TDD (Time Division Duplex) pro pásmo nepárové.

Podobně jako u systému GSM lze i UMTS rozdělit do několika základních funkčních částí, toto rozdělení popisuje obrázek 1.7.



Obrázek 1.7: *Architektura systému UMTS*

1.3.2.1 ***MS***

Mobilní stanice systému UMTS je obdobou MS v systému GSM, je tvořeno mobilním zařízením (ME) a USIM (Universal Subscriber Identity Module). USIM přidává především podporu nových bezpečnostních prvků jako je vzájemná autentizace MS a Node B nebo použití delších šifrovacích klíčů.[2]

1.3.2.2 ***UTRAN***

UTRAN je zkratkou pro rádiovou přístupovou síť pro UMTS (UMTS Terrestrial Radio Access Network). Představuje tu část sítě, která zprostředkovává rádiový přenos , řízení a přidělování rádiových kanálů. Jedná se o obdobu BSS v systému GSM. Podobně jako BSS je i UTRAN složena ze dvou základních jednotek[2]:

Node B – základnová stanice systému UMTS (obdoba BTS u GSM)

RNC (Radio Network Controller) – řídicí jednotka systému UMTS (obdoba BSC u GSM)

1.3.2.3 ***CSN***

CSN (Circuit switched network) je označení pro původní prvky systému GSM využívané především k uskutečňování hovorů pomocí přepínání okruhů. Tato část je dále propojena s veřejnou telefonní sítí.[2]

1.3.2.4 ***PSN***

Tato část sítě vychází z prvků využitých již pro GPRS a slouží k přenosu dat prostřednictvím paketové sítě.[2]

SGSN (Serving GPRS Support Node)- prvek řídící paketový prvek

GGSN (Gateway GPRS Support Node) – Rozhraní pro propojení vnitřní sítě operátora s globální sítí – v dnešní době především sítí Internet.

1.4 4. generace

Čtvrtá generace mobilních telekomunikačních sítí si klade za úkol obsloužit stále se zvyšující požadavky uživatelů na přenosovou kapacitu. Systém vedle poskytování klasických hovorových a dalších služeb známých ze systémů 2. a 3. generace je rozšířen o vysokorychlostní datový přístup, aby bylo možné využívat služeb přístupu k Internetu, VoIP, mobilní TV, cloud-computing apod.

Pojem 4. generace je pouze komerčním označením pro specifikaci definovanou ITU-R pod názvem IMT-Advanced (International Mobile Telecommunications). V Březnu roku 2008 bylo organizací ITU-R přijato několik požadavků pro sítě IMT-Advanced[12][27]:

- Přenosová rychlost 100 Mbit/s pro komunikaci s rychle se pohybujícím zařízením
- Přenosová rychlost 1 Gbit/s pro stacionární a pomalu pohybující se zařízení
- Vzájemná kompatibilita s ostatními sítěmi

- Celosvětová použitelnost systému
- Škálovatelnost šířky rádiového kanálu podle potřeby

První technologií plně splňující požadavky pro IMT-Advanced je standart LTE-Advanced schválený v Březnu 2011. LTE-Advanced navazuje na svého předchůdce LTE, který ačkoliv je někdy označován za síť 4. generace v materiálech operátorů nesplňuje požadavky definované ITU-R. Na vývoji LTE-A se podílela především organizace 3GPP, která také stálá za specifikací 3G systému UMTS.

Některé vlastnosti systému LTE-Advanced[12]:

- Škálovatelnost šířky pásma až na 100MHz
- Využití více antén umožňující vícenásobný MIMO (Multiple Input/Multiple Output) přístup.
- Asymetrická šířka pásma pro FDD
- Automatická konfigurace sítě
- Až 3.3 Gbit/s přenosová rychlost

První LTE-A sítě jsou od roku 2013 provozovány v Jižní Koreji a Rusku. Zatím je na trhu dostupný pouze omezený počet zařízení podporujících tuto technologii a výrazný nástup lze očekávat až v následujících letech.

2 Zabezpečení v GSM/UMTS sítích

2.1 Zabezpečení sítě GSM

Bezpečnost sítě GSM je postavena na 4 základních bodech.[2][13]

- autentizace uživatele
- utajení identity uživatele
- utajení přenášených dat
- utajení signalizace

Zajištění zabezpečení sítě má na starost několik jejích částí. Konkrétně se jedná o Subscriber Identity Module (SIM), mobilní zařízení (MS) a centrum autentičnosti (AUC).

SIM - obsahuje mimo jiné IMSI (International Mobile Subscriber Identity), tajný klíč K_i, dále algoritmus pro generování šifrovacího klíče A8, autentizační algoritmus A3 a osobní identifikační číslo PIN.

Mobilní stanice - obsahuje šifrovací algoritmus A5.

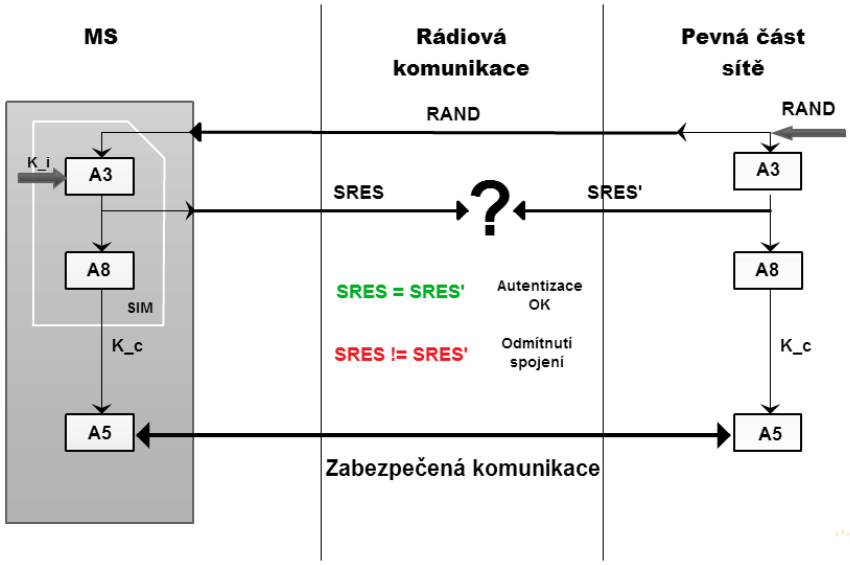
AUC - obsahuje databázi s identifikačními a autentizačními údaji uživatelů sítě. V databázi jsou uloženy IMSI, TMSI (Temporary Mobile Subscriber Identity), LAI (Location Area Identity) a tajný klíč K_i, který je unikátní pro každého uživatele.

Z obecného pohledu je nejzranitelnější bezdrátová část sítě, kde probíhá samotná komunikace mezi MS a BTS, která je šířena volným nezabezpečeným prostředím. Některými z metod pro zabezpečení přenosu jsou např. přelaďování vysílací frekvence, kanálové kódování, digitální modulace GMSK nebo ověření účastníka.

2.1.1 Autentizace uživatele

Autentizace uživatele se provádí při přístupu uživatele do sítě. Systém GSM ověří identitu uživatele pomocí mechanismu challenge-response. BTS odesláním 128 bitového náhodného čísla RAND vyzve mobilní stanici k výpočtu ověřené odpovědi SRES. Hodnota SRES je vypočtena na základě znalosti K_i a RAND a implementaci algoritmu A3. tzn. SRES = A3(K_i, RAND). MS pak pošle výslednou hodnotu zpátky do sítě, kde je v registru VLR proveden obdobný výpočet se stejnými hodnotami. Pokud síť dojde ke stejnému výsledku, jako obdržela od MS, je autentizace úspěšná. Pokud ne, dojde k ukončení spojení.[13]

Schéma autentizace uživatele je na obrázku 2.1.



Obrázek 2.1: *Autentizace uživatele*

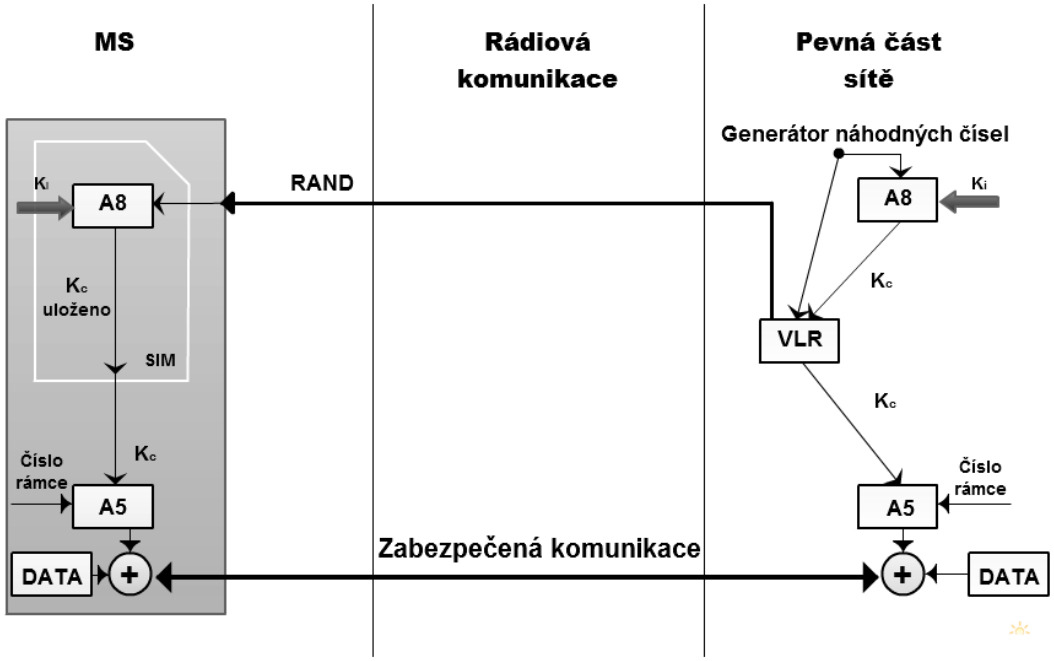
2.1.2 Utajení identity uživatele

Jak bylo popsáno výše, číslo IMSI slouží k jednoznačné identifikaci uživatele v rámci sítě a je uloženo na SIM kartě. Aby došlo ke snížení rizika zneužití IMSI zavádí se po autentizaci uživatele dočasný identifikátor TMSI (Temporary Mobile Subscriber Identity). TMSI je dočasně uloženo na SIM a v registru VLR. TMSI se vztahuje jen k lokalitě, v níž bylo vydán. V případě přesunu do jiné lokality je vydáno nové TMSI. Konfigurace GSM sítě umožňuje průběžnou změnu TMSI i v případě, kdy nedochází k přechodu mezi lokalitami – tento mechanismus posiluje utajení identity uživatele.[13]

2.1.3 Utajení přenášených dat a signalizace

Průběh šifrování v systému GSM je založen na proudové šifře A5, kdy je k bitové posloupnosti dat přičítána hodnota šifrovací posloupnosti (tzv. keystream). Proces šifrování v systému GSM je popsán obrázkem 2.2. V registru HLR (AuC) je vygenerováno náhodné číslo RAND**.** Na základě tohoto čísla je pak s pomocí autentizačního klíče K_i podle šifrovacího algoritmu A8 vygenerován šifrovací klíč K_c. Tato trojice (RAND - 128 bitů, SRES - 32 bitů a K_c - 64 bitů) je předána do registru VLR, kde je po dobu spojení uchována.[2] BTS pak přepošle číslo RAND mobilní stanici, která na SIM kartě obdobným procesem opět vygeneruje klíč K_c. Vstupem pro algoritmus A5 je 64 bitový šifrovací klíč, 22 bitové číslo TDMA rámce a vlastní data určená k šifrování. Z důvodu výpočetní náročnosti tohoto algoritmu již není uložen na SIM kartě, ale je implementován na koncových mobilních zařízeních. Pokud v průběhu hovoru dochází k handoveru, tak se šifrovací klíč nemění. Z výše zmíněného tedy vyplývá, že ani při šifrování nedojde k přenosu klíče rádiovým rozhraním a jsou přenášena pouze hodnoty RAND a vlastní šifrovaná data.[2]

Implementace algoritmů A3 a A8 není závazně specifikována a ponechává tak určitou volnost domluvy mezi operátorem a výrobcem SIM karet.[2]

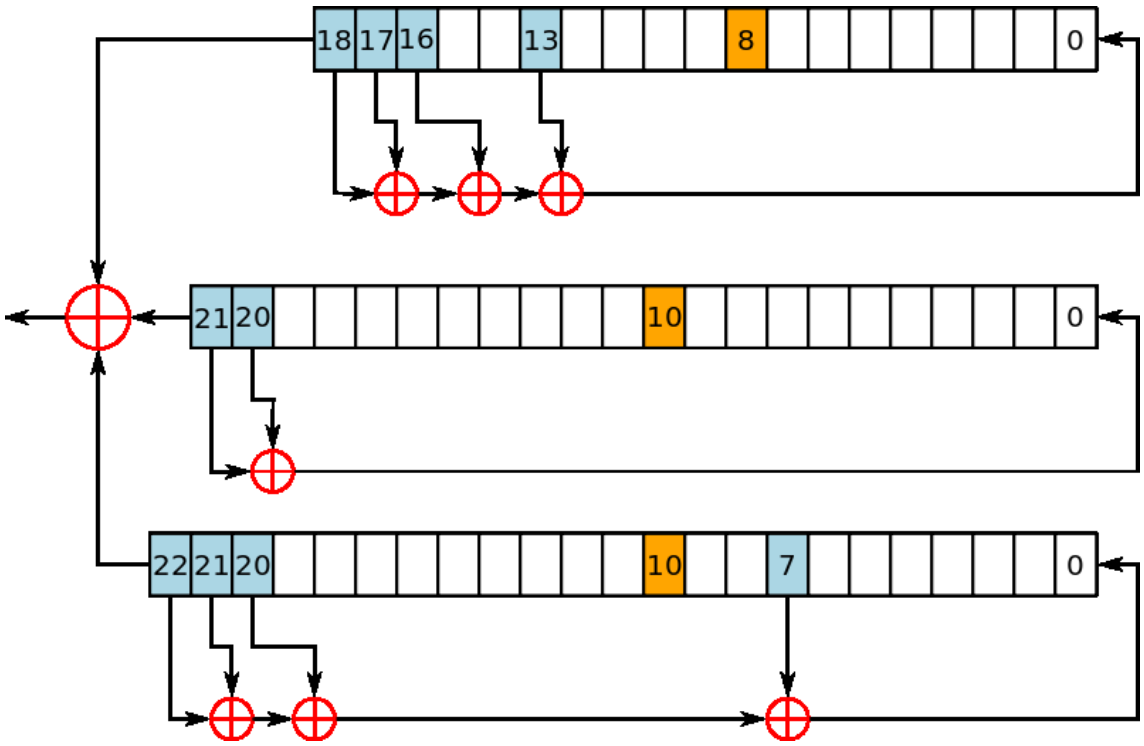


Obrázek 2.2: *Utajení přenášených dat*

Pro možnost využití v systému GSM jsou popsány následující typy šifrovacího algoritmu A5 :

- A5/0- žádné šifrování
- A5/1- proudová šifra využívající 64 bitového klíče
- A5/2- implementační varianta A5/1 určena pro export mimo země Evropy a USA, podstatně slabší zabezpečení, umožňující real-time prolomení. V současnosti se téměř nepoužívá
- A5/3- bloková šifra nazývaná také KASUMI využívá 128bitového šifrovacího klíče, s 64 bitovým datovým vstupem i výstupem. Jedná se o podstatné zesílení bezpečnosti, ačkoliv se tato šifra ukázala jako akademicky prolomitelná.

Algoritmus A5/1 je založen na kombinací 3 posuvných registrů s lineární zpětnou vazbou (LSFR – Linear Shift Feedback Register). Délka registrů je 19,22 a 23 bitů. Počáteční stav šifry je určen šifrovacím klíčem K_c a číslem TDMA rámce. Následně dojde k zahození výstupu pro prvních 100 cyklů. Nyní je algoritmus připraven vytvořit 114 bitovou výstupní sekvenci šifrovaných resp. dešifrovaných dat.[14] Šifrovací algoritmus je graficky znázorněn na obrázku 2.3



Obrázek 2.3*: Algoritmus A5/1*

[Zdroj: http://en.wikipedia.org/wiki/A5/1]

2.2 Zabezpečení sítě UMTS

Zabezpečení sítí 3. generace ve velké míře vychází z bezpečnostních prvků využívaných u sítí předchozí generace. Při tvorbě zabezpečení pro 3G sítě se vývojáři zaměřili především na známé zranitelnosti GSM systému. Jelikož je síť UMTS tvořena s ohledem na širokopásmový datový přístup je potřeba zohlednit lepší zabezpečení přenášených dat.

Architektura zabezpečení 3G sítí se skládá z následujících částí[21][13]:

- Zabezpečení přístupové sítě - Zde je opět kladen důraz na utajení identity uživatele, autentizaci uživatele, bezpečnost a integritu dat. Pro utajení identity je využita dočasná identita, na rozdíl od GSM je kladen důraz na častější změnu této identity tak, aby uživatel nemohl být dlouhodobě identifikován. Pro posílení autentizace bylo zvoleno vzájemné ověření účastníka sítě. Pro zajištění vyšší bezpečnosti přenášených dat nejsou dále podporovány šifrovací algoritmy A5/1 a A5/2. S tím souvisí využití 128 bit šifrovacího klíče i v rámci SIM. Především pro ochranu signalizačních dat byl zaveden mechanismus pro kontrolu integrity přenášených zpráv. Tato vlastnost umožňuje vždy zkontrolovat, zda přijatá zpráva nebyla změna a pochází z ověřeného zdroje.

- Zabezpečení síťové domény - Na rozdíl od GSM se specifikace UMTS zaobírá zabezpečením komunikace uvnitř sítě operátora a při komunikaci mezi sítěmi různých operátorů.

- Zabezpečení uživatelské domény - Umožňuje zabezpečit MS proti zneužití. Stejně jako v GSM je zde využito PIN kódu.

- Aplikační zabezpečení – Vlastnosti umožňující zabezpečení uživatelských aktivit v rámci sítě operátora.

- Ověřitelnost a konfigurovatelnost zabezpečení – Dává možnost uživateli ověřit si, zda jsou hovory a data přenášena zabezpečeným rádiovým kanálem, např. pomocí indikační ikony na MS.

3 Bezpečnostní rizika GSM

V předchozí kapitole jsem vás seznámil se základním zabezpečením GSM sítí proti zneužití. V této části bych chtěl poukázat na možná bezpečnostní rizika, která plynou z vlastní struktury a fungování GSM sítě.

Na rizika při mobilní komunikaci lze pohlížet ze dvou stran – z pohledu koncového uživatele a pohledu operátora sítě. Základním požadavkem obyčejného uživatele je zaplatit pouze za služby, které mu byly poskytnuty. Dle architektury GSM sítě je za toto odpovědná autentizace uživatele vůči síti pomocí tajného klíče – dojde-li tedy k úniku tohoto klíče, může pak útočník provádět hovory na účet oběti. K dalším požadavkům zákazníka patří zabezpečení přenášených dat proti odposlechu. Už z podstaty bezdrátového provozu vyplývá ve srovnání s metalickým vedením mnohem jednodušší přístup útočníka k přenosovému kanálu. Z tohoto důvodu je potřeba přenášena data šifrovat dostatečně silným zabezpečením, které však nebude narušovat provoz sítě např. nadměrným datovým tokem, zvýšenou chybovostí nebo náklady. Dojde-li proto k úniku klíče pro šifrování jsou data libovolně přístupná útočníkovi.

Z pohledu operátora mobilní sítě, jehož hlavním cílem je finanční zisk, je zabezpečení stejně důležité jako kvalita služeb. Při zneužití sítě může dojít k přímé finanční ztrátě formou zneužití jeho sítě pro cizí služby nebo k nepřímým ztrátám, kdy dochází k odchodu koncového zákazníka, kterému není poskytnuto bezpečné zázemí.

Z výše zmíněného vyplývá, že hlavním objektem zájmu útočníka je zisk tajného šifrovacího klíče K_i, který se nachází na SIM kartě a AuC . Z kapitoly 1.2 víme, že klíč K_i se používá jak pro autentizaci uživatele, tak i pro výpočet dalšího klíče K_c, který dále slouží k šifrování přenášených dat. Pro odposlech hovorů je tedy dostačující pouhá znalost klíče K_c. Detailněji bude tato problematika rozebrána v následujících podkapitolách.

3.1 Klonování SIM karty

Z historického pohledu se jednalo o první popsaný způsob zneužití chyb v zabezpečení. 13. Dubna 1998 byl publikován Ianem Goldbergem (ISAAC Security Research Group) a Marcem Bricenem (SDA - Smartcard Developer Association) článek popisující možnost klonování SIM karty. Za pomocí fyzického přístupu k SIM a jednoduché čtečky se jim podařilo získat IMSI a klíč K_i, který poté nahráli do nové SIM karty a získali tak kopii napadené karty.[15]

Standart GSM definuje, že pro autentizaci bude využit libovolný algoritmus na základě volby operátora, který však bude odpovídat požadavkům na autentizaci definovaných jako A3/8. Jedním z nejrozšířenějších autentizačních algoritmů je COMP128, podstatným problémem tohoto algoritmu je, že byl vyvíjen jako utajený, což sebou nese problémy ve formě nemožnosti odhalit některé skryté problémy, které by byly snadněji odhalitelné v případě vývoje algoritmu v otevřeném formátu s možností komentářů ostatních odborníků.

Algoritmus COMP128 pracuje s dvěma vstupními hodnotami – K_i a RAND a jednou výstupní hodnotou. Analýza uniklých informací o algoritmu COMP128 ukázala na nízký rozptyl výstupních hodnot. Podle údajů ze zprávy je pro získání K_i potřeba algoritmu předložit cca. 150 tis. požadavků. Útok pak probíhá hledáním kolizí mezi výstupními hodnotami tak, že jsou zadávány dvojice velice blízkých RAND čísel – mění se pouze jeden nebo dva byty zadávaného čísla a to tím způsobem, že hledáme-li 0. a 8. byte klíče K_i měníme pouze 0. a 8. byte RAND, pro hledání 1. a 9. byte měníme 1. a 9. byte RAND apod. Je-li výstupem jedné dvojice RAND stejná hodnota, můžeme na základě znalosti algoritmu COMP128 dopočítat příslušné 2 byty klíče K_i. [15]

Po získání klíče K_i a IMSI napadené SIM, lze vytvořit klon karty a dále ji využít pro provádění extra placených hovorů, zneužití identity apod. Ačkoliv je tento útok velice jednoduchý na provedení, nelze jej považovat za velkou hrozbu v globálním měřítku hned z několika důvodů. Nejprve je potřeba k provedení útoku získat fyzický přístup k SIM na dostatečně dlouhou dobu, pokud se toto útočníkovi podaří pak nastupují různé ochranné mechanismy nových SIM karet(cca. od roku 2002), omezený počet dotazů – po překročení limitu dojde k zablokování SIM, umělé zpomalení výpočtu odpovědi což velice navyšuje dobu provádění útoku a riziko odhalení. Dále je možno mít v síti přihlášenou právě jednu identickou SIM současně, v případě přihlášení další SIM se stejným IMEI dojde pomocí vnitřních mechanismů sítě k zablokování účastníka a nahlášení zneužití.[15] Pokud se vše zmíněné útočníkovi podaří, stále jde o napadení pouze jediného zařízení a nejedná se o rozsáhlé zneužití.

3.2 Jednosměrná autentizace

V této části se zaměříme na další ze známých bezpečnostních problému systému GSM. Systém GSM je navržen tak, že je ověřována pouze identita účastníka vůči síti, ke které se připojuje a není prováděna opačná autentizace sítě vůči účastníkovi – tento způsob se nazývá jednosměrná autentizace a vytváří ohromnou skulinu v zabezpečení GSM sítě. Je tak možno vytvořit falešnou základnovou stanici (BTS), která se poté tváří jako opravdová BTS operátora, a mohou se k ní připojovat mobilní stanice (MS), aniž by toto odhalili. Na tento problém bylo upozorňováno od počátku GSM systému, ale nebylo to považováno za hrozbu z důvodu velmi vysokých nákladů na pořízení a provozování falešné BTS. S narůstajícím rozšířením sítě však také dochází k výraznému poklesu nákladů na pořízení a provoz falešné základnové stanice. V současnosti jsou pak dostupná softwarově ovládaná rádia, která s využitím volně dostupného softwaru pro zpracování signálu snižují náklady na tento způsob zneužití na zanedbatelnou částku. [16]

3.3 Prolomitelnost algoritmu A5

V kapitole 2 zabývající se zabezpečením GSM je zmíněn utajený vývoj šifrovacích algoritmů A5. Díky tomuto nebylo možno dlouhou dobu získat přístup k vlastní implementaci tohoto algoritmu a nebylo tak možné ověřit vlastní bezpečnost. Po zveřejnění implementace

A5/2 v roce 1999 byla ihned pod vedením Iana Goldberga vypracována analýza upozorňující na kritické problémy v zabezpečení umožňující real-time prolomení šifrování za využití běžného PC. Popis jejich útoku však pracoval se znalostí nešifrovaných dat a pro praktickou implementaci nebyl optimální. V roce 2003 byla zveřejněna zpráva popisující prolomení zabezpečení pouze na základě znalosti malého množství šifrovaných dat. Jejich implementace vychází z vlastnosti GSM systému, kdy jsou často odesílány prázdné šifrované rámce se známým obsahem – doplňkové bity. Tento princip umožnil rozšířit proveditelnost tohoto útoku následně i na bezpečnější šifru A5/1.[15][16]

V kombinaci s možnosti podvržení základnové stanice, pak bylo možné získat klíč K_c pro komunikaci šifrovanou libovolným algoritmem. Útočník zachytí výzvu RAND a následnou šifrovanou komunikaci. Následně využitím podvržené BTS využije stejnou hodnotu RAND pro autentizaci v rámci vlastní sítě s aplikovaným šifrováním A5/2. Po provedení výše popsaného útoku tak získá šifrovací klíč, který může následně využít k dešifrování dříve zachycených dat a v tomto případě nezáleží na použité šifře.[16]

3.4 Absence zabezpečení v páteřní síti

Specifikace GSM vůbec neřeší zabezpečení komunikace uvnitř vlastní sítě operátora. Signalizační protokol SS7 používaný v páteřní síti systému neposkytuje dostatečné zabezpečení a autentizaci v rámci vzájemně propojené sítě různých operátorů. Při rozšiřování IP sítí pro propojení jednotlivých prvků systému GSM je potřeba brát v potaz také obecné hrozby zneužití související s globální sítí. V případě proniknutí útočníka do vnitřní sítě může podvrhnutím jednoho z prvků systému získat přístup ke kritickým částem jako je HLR, VLR popř. AuC.[16]

4 Realizované útoky

V této kapitole jsou popsány základní principy některých útoků využívajících bezpečnostních chyb systému GSM k neoprávněnému zásahu do soukromí uživatelů. S velkou pravděpodobností lze předpokládat využívání různých proprietárních řešení na úrovni vládních a bezpečnostních agentur. V této práci jsem se však zaměřil především na provedení útoků za využití volně dostupných prostředků.

4.1 IMSI catcher pomocí USRP

Již od roku 1996 jsou dostupná první komerční řešení IMSI catcher vyvíjených firmou Rhode&Schwarz. Možnost využití USRP pro provozování IMSI catcher byla popsána Chrisem Pagetem v rámci konference 26C3 a následně prakticky předvedena na konferenci DEF CON 30. Srpna 2010.

Využívá programovatelného rádia USRP 1 ve spolupráci s open-source implementací GSM protokolu – OpenBTS. Následnou jednoduchou konfigurací OpenBTS, kdy jsou nastaveny identifikační hodnoty MCC a MNC základnové stanice je dosaženo zprovoznění podvržené BTS jednoho z lokálních operátorů. Upozornil také na zablokování notifikace použitého šifrování koncovému uživateli.

Podrobnější informace a samotný průběh prezentace je dostupný v angličtině na webových stránkách konference.[17]

4.2 Pasivní odposlech pomocí USRP

Tento útok byl poprvé prakticky předveden v rámci 26. konference 3C Chrisem Pagetem a Karstenem Nohlem 27. 12. 2009 v Berlíně.

Vlastní útok se skládá ze dvou základních částí. První částí je pasivní zachycení komunikace mezi BTS a MS pomocí softwarového rádia USRP, druhým krokem pak je získání Kc pro dešifrování zachycených dat.

Pro zachycení komunikace je využit nástroj založený na open-source GNU Radio, umožňující jednoduchou obsluhu zařízení USRP. Následná interpretace zachyceného signálu vychází z implementace GSM rozhraní v OpenBTS, pro tento úkol byl na této konferenci zveřejněn nástroj Airprobe. Airprobe umožňuje zachycení downlink komunikace na jediném rádiovém kanálu bez podpory frekvenčních přeskoků.[17][19]

Komplexnějším úkolem pak bylo prolomení šifrovacího algoritmu A5/1. Princip prolomení tohoto šifrování vychází ze znalosti obsahu některých šifrovaných zpráv. Toto je obdobou prolomení A5/2 popsané v kapitole 3.3. Jelikož se jedná o proudovou šifru, lze operací XOR shodné zprávy v šifrované a plain-textové podobě získat proud bitů (tzv. keystream) použitý k jejich zašifrování.[14]

Pomocí předem vypočtených tabulek pak lze na základě keystreamu získat použitý šifrovací klíč. Aby byl však tento krok proveditelný je potřeba získat tento klíč v rozumném čase za využití dostupných paměťových prostředků. Délka klíče K_c je 64 bitů a nabývá tedy hodnot z množiny 2^{64} stavů. Pro uložení všech těchto stavů do tabulky by bylo potřeba 64 * 2^{64} bit = 134 217 728 TB paměti. Bylo teda potřeba přistoupit k mechanismům, které umožní zredukovat paměťovou náročnost na zvládnutelnou míru. Tímto mechanismem je TMTO (Time-memory trade-off), kdy na úkor navýšení výpočetního času je dosaženo nižších paměťových nároků.[14][18]

Celkovou výpočetní a paměťovou náročnost bylo možné výrazně snížit využitím vlastnosti systému GSM popsaném profesorem Golicem v práci *Cryptanalysis of Alleged A5 Stream Cipher,* kde popisuje chybu v implementaci šifry A5/1, kdy dojde k redukci dosažitelných stavů na 14% původní teoretické hodnoty 2^{64}. Tento problém souvisí s provedením 100 cyklů při inicializaci šifrovacích registrů. Na základě pokusů, kdy provedl 100 reverzních cyklů na množině 1 milionu stavů, došel k závěru, že v 86% případů není počáteční stav dosažitelný.[19]

Jednou z metod pro efektivní uložení předem vypočtených dat je využití tzv. rozlišitelných bodů (Distinguished points), kdy nejsou do výsledné tabulky uloženy všechny dvojice počátečních a koncových stavů, ale pouze některé splňující předem zvolenou podmínku, např. mají posledních 16 bitů nulových. Tímto dojde k výraznému snížení počtu potřebných přístupů do tabulky. Aby nedocházelo ve výsledné tabulce k ukládání duplicitních koncových stavů, které by následně způsobily zacyklení. Proto byla pro výpočet následujícího stavu využita mírně odlišná funkce než v předchozím kroku. Výsledná tabulka se pak nazývá Rainbow table a minimalizuje výskyt redundantních záznamů. [14][16]

Využitím těchto technik došlo ke snížení paměťové náročnosti na 2TB předvypočtených tabulek rozdělených na 41 částí umožňující distribuované výpočty – tzv. Berlin rainbow tables set s celkovým pokrytím 19,13% možných stavů.

Společně s tabulkami byla na konferenci zveřejněna aplikace kraken obstarávající potřebné výpočty a přístup k tabulkám. Vstupní hodnotou pro získání šifrovacího klíče je vložení XORu šifrovaného burstu a známého plain-text ekvivalentu. Pro tuto potřebu jsou využity bursty se známým obsahem, které se využívají především jako výplňkové v případě kdy, BTS nemá žádná data k odeslání.

Video prezentace a další podrobnosti jsou dostupné na[18].

4.3 Pasivní odposlech pomocí OsmocomBB

Předchozí útok za využití USRP umožňoval zachycení komunikace při, které nedochází k frekvenčním přeskokům na rádiovém rozhraní. Pro podporu frekvenčních přeskoků s využitím USRP by bylo potřeba implementovat tuto funkcionalitu přímo do programovatelného pole FPGA. Jako jednodušší varianta se ukázalo využití mobilního telefonu s upraveným firmware, který pracuje s jedním fyzickým kanálem.

Toto bylo představeno na konferenci 27C3 (Chaos Computer Conference) v rámci prezentace Karstena Nohla a Sylvaina Munauta. Firmware využitý pro provoz MS byl vytvořen v rámci projektu OsmocomBB, který se zaměřuje na open-source implementaci GSM protokolu na straně mobilního zařízení.

Za využití levného mobilního telefonu Motorola a upraveného firmware OsmocomBB představili možnost zachycení komunikace v obou směrech MS<->BTS i v případě kdy dojde k zavedení frekvenčních přeskoků, které primárně slouží k potlačení rušení. Bylo potřeba obejít proces dešifrování signálu, který probíhá na nejnižší úrovni tak, aby byla dostupná čistá šifrovaná data, které je možno následně využít pro nástroj kraken, představený v předchozí kapitole.

Následující krok pro prolomení šifrování je totožný s průběhem popsaným v předchozí části. Podrobnější informace a video z konference je dostupné z [20].

5 Praktická realizace

Součástí této diplomové práce bylo praktické provedení vybraných typů útoku vůči GSM síti. Pro realizaci byly zvoleny následující 3 scénáře zneužití GSM sítě:

1) IMSI catcher – zařízení sloužící k získání informací o koncových zařízeních pohybujících se ve zvolené oblasti
2) Falešná BTS – podstatou je vytvoření falešné základnové stanice, která umožňuje po připojení MS na danou BTS kontrolovat veškerou komunikaci
3) Pasivní odposlech – odchycení komunikace mezi BTS a MS oběti, prolomení zabezpečení a následně přístup k soukromé komunikaci

Provozování zařízení v licencovaných pásmech je v ČR upraveno zákonem č. 127/2005 Sb., o elektronických komunikacích. Aby nedocházelo k rušení komunikace, bylo veškeré testování prováděno v laboratoři N211 katedry Telekomunikací při VŠB-TU Ostrava s nastavením výkonu vysílače tak, aby nedocházelo k ovlivnění okolního signálu.

V případě, kdy docházelo k zachycení/dešifrování komunikace, bylo tak provedeno pouze pro testovací zařízení.

5.1 Použitá zařízení a software

Před vlastním popisem realizace útoků jsou v následujících podkapitolách popsány zařízení a softwarové nástroje využívány v rámci této diplomové práce. Instalace a konfigurace jednotlivých zařízení bude podrobněji popsána v kapitolách věnujících se jednotlivým útokům.

5.1.1 USRP N210

USRP (Universal Software Radio Peripheral) jsou softwarově řízené rádiové zařízení. Byly navrhnuty a v současnosti prodávány firmou Ettus Research LLC., která je nyní součástí společnosti National Instruments. USRP byla navržena jako low-cost platforma pro tvorbu softwarového rádia. USRP jsou s hostujícím zařízením (počítačem) propojeny pomocí USB (USRP 1) nebo pomocí Gigabit Ethernetu (např. USRP N210).[22]

K obsluze a komunikaci mezi USRP a PC je vytvořen open-source ovladač UHD (USRP Hardware Driver) poskytovaný Ettus Research.

Konfigurace jednotlivých USRP je modulární a je možno ji přizpůsobit dle požadavků. Pro tuto práci byl využit modul WBX. Jedná se o široko pásmový transceiver poskytující výstupní výkon až 100 mW. Umožňuje zároveň nezávisle provozovat vysílač i přijímač ve frekvenčním rozsahu 50 MHz – 2,2 GHz.[22]

USRP N210 umožňuje použití externího zdroje hodinového signálu popř. využití referenčního hodinového zdroje za využití modulu pro příjem GPS signálu.

Využitím programovatelných hradlových polí FPGA bylo dosaženo vysoké propustnosti až 100MS/s a zároveň umožňují jejich úpravu pomocí přehrání firmwaru FPGA.

5.1.2 DVB-T/DAB USB Dongle

Toto zařízení bylo primárně určeno k příjmu DVB-T signálu, pro příjem tohoto signálu je také vybavené HW demodulátorem. Podpora zpracování dalších typů signálu DAB nebo FM je dosažena využitím A/D převodníku, který poskytuje čistá I/Q data pro následnou softwarovou demodulaci.

Zařízení je založeno na chipsetu Realtek RTL2832U a je vybaveno laditelným tunerem Rafael Micro R820T. Toto umožňuje využití zařízení v rozsahu frekvencí 35 MHz až 1100 MHz, což zahrnuje pásmo GSM 900. [23]

Pro příjem signálu je zařízení vybaveno konektorem MCX, který umožňuje po připojení přechodového členu MCX -> SMA využít široké spektrum antén. Zařízení je možné vidět na obrázku 5.1

Obrázek 5.1: *DVB-T přijímač*

5.1.3 GNU Radio

GNU Radio je opensource softwarový balík poskytující nástroje ke zpracování signálu za využití softwarového rádia. Umožňuje využít jak externí hardware v podobě rádiového přijímače k vytvoření SDR (software defined radio) nebo také umožnuje vytvoření simulovaného prostředí pro testování a vývoj.

V rámci této práce bylo GNU Radio využito především jako základ pro další nástoje OpenBTS a Airprobe, které jsou na knihovnách GNU Radio silně závislé.

Dále byl použit nástroj GRC (GNU Radio Companion), který umožňuje tvorbu schémat v grafické prostředí a následnou automatizovanou tvorbu skriptů.

5.1.4 OpenBTS

OpenBTS (Open Base Transceiver station) je UNIXovou aplikací vytvořenou a vyýjenou skupino Range Networks. Využívá softwarové rádio k vytvoření základnové stanice sítě GSM umožňující připojení GSM kompatibilních mobilních zařízení.

OpenBTS implementuje funkce rádiového rozhraní Um v GSM architektuře. Pro funkce na nejvyšší vrstvě pak využívá SIP softswitche popř. PBX pobočkové ústředny k vlastnímu propojení hovorů. Kombinace globálního standartu GSM a VoIP umožňuje vytvořit a

provozovat nízkonákladové sítě s minimálními náklady na provoz ve srovnání s klasickými GSM sítěmi současných poskytovatelů.

Přehled částí implementovaných v OpenBTS (v závorce je uvedena zdrojová dokumentace GSM ETSI specifikace)[24] :

L1 – funkce TDM (GSM 05.02)

L1 – funkce FEC (GSM 05.03)

L1 – časování, synchronizace (GSM 05.08 a 05.10)

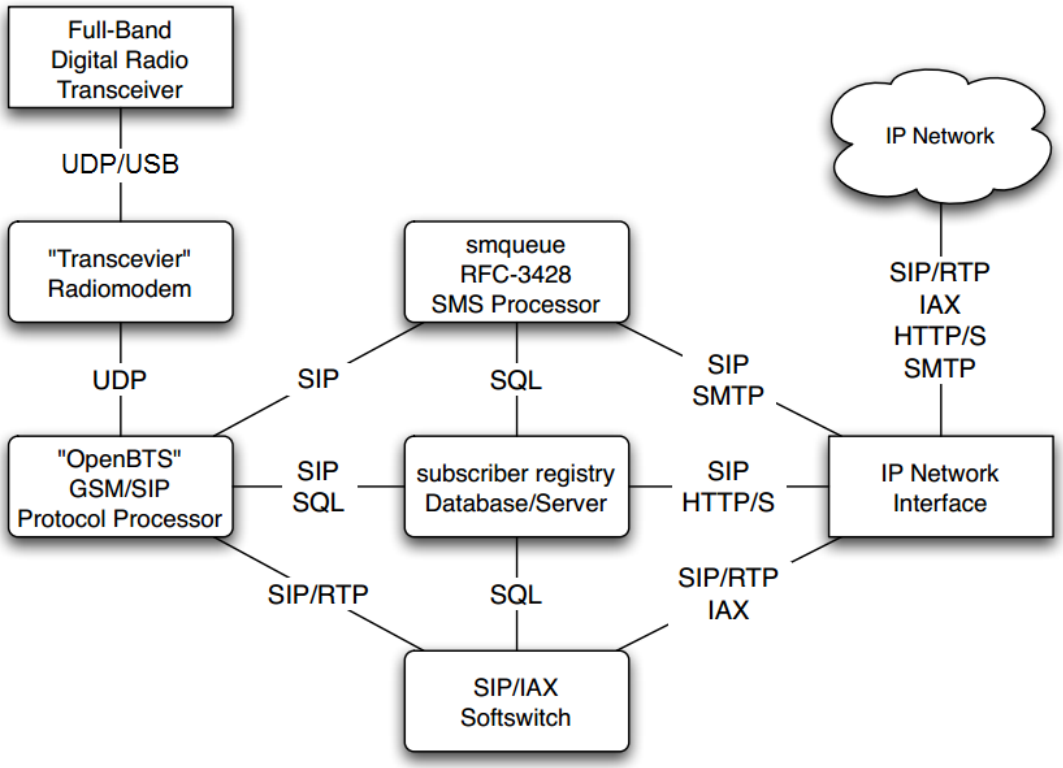
L2 – LAPDm (GSM 04.06)

L3 – Radio Resource management – náhrada BSC (GSM 04.08)

L3 – GSM-SIP brána pro mobility management – náhrada HLR a VLR registru

L3 – GSM-SIP brána pro signalizaci hovorů – náhrada MSC

L4 – GSM-SIP brána pro zprávy SMS



Obrázek 5.2: *Komponenty OpenBTS a jejich komunikační kanály*

[Zdroj: Range Network: OpenBTS User Manual]

Obrázek 5.2 zobrazuje funkční propojení jednotlivých entit systému OpenBTS. Popis k obrázku:

Full-Band Digital Radio Transceiver – USRP použité jako vlastní přijímač/vysílač

Transceiver radiomodem – Obstarává funkce na fyzické vrstvě L1 GSM architektury

OpenBTS – vlastní aplikace – popis viz výše (Přehled implementovaných částí)

smsqueue – server sloužící v systému OpenBTS k přeposílání SMS zpráv mezi jednotlivými uživateli.

Subscriber registry – OpenBTS využívá upravenou variantu SIP registru pro správu účastníků. Tato databáze slouží jako náhradu za HLR

SIP Softswitch/PBX – slouží k obsluze hovorů v systému OpenBTS, oficiálně je pro práci s OpenBTS doporučeno použití PBX Asterisk

5.1.5 **Asterisk**

Asterisk je opensource řešení určené pro provozování komunikačních systémů a aplikací. Umožňuje provozovat softwarové PBX (pobočková ústředna), které jsou určeny pro platformy Unix/Linux. Mezi široké možnosti Asterisku patří např. VoIP gateway, server interaktivního hlasového průvodce, PBX. Asterisk podporuje široké spektrum kodeků (G.711, μ-law, A-law, Speex, GSM …), zahrnuje jak VoIP technologie (SIP, H.323, IAX, MGCP) tak i tradiční technologie (T1, ISDN, analogové POTS a PSTN). [25]

Asterisk je z pohledu architektury rozdělen na jádro a dodatečné moduly, které jsou načítány podle aktuální potřeby, což vede ke zvýšení efektivnosti celého systému. [25]

Asterisk byl zvolen v této DP pro spolupráci s OpenBTS z důvodu, že se jedná o nejrozšířenější a ze strany OpenBTS nejvíce podporované řešení. Při tomto řešení je každé koncové zařízení GSM sítě registrováno v Asterisku jako koncový SIP uživatel. Uživatelé jsou registrování na základě IMSI, kdy je poté potřeba pro každé IMSI vložit do konfiguračního souboru asterisku.

5.1.6 **rtl-sdr**

Jedná se o samostatnou část softwarového balíku z rodiny osmocom. Software umožňuje komunikovat se zařízením, které je založeno na čipsetu Realtek RTL2832U a použít tak zařízení jako velice levné softwarové rádio (SDR – software defined radio). Využívá vlastnosti tohoto chipsetu, kdy dochází k odesílání surových dat přes USB rozhraní a až k následné softwarové demodulaci signálu. [23]

Pro vlastní komunikaci se zařízením je využito knihovny librtlsdr. Balík obsahuje několik dalších nástrojů, které slouží k práci se získanými daty.

rtl_sdr – umožňuje uložení získaných vzorků do výstupního souboru, tento nástroj byl primárně využíván při pasivním odposlechu prováděném v rámci této diplomové práce (kap. 5.4)

rtl_fm – zachycení a demodulace FM signálu

rtl_tcp – slouží k přístupu a ovládání rtl-sdr pomocí vzdáleného síťového přístupu

5.1.7 **Airprobe**

Airprobe je softwarový nástroj sloužící k analýze GSM komunikace. Formálně jej lze rozdělit na 3 základní části[19]:

- Získaní dat
- Demodulace získaných dat
- Interpretace dat

Pro získávání dat Airprobe využívá nástrojů ze softwarového balíku GNURadio. Většina těchto nástrojů je hardwarově závislých, v současné době jsou podporovány dva základní typy hardwaru a to USRP (více v kap. 5.1.1) a SDR (kap. 5.1.2)

Demodulace – jak název napovídá, tato část slouží k vlastní demodulaci získaných surových dat.

Interpretace dat – tato část obsahuje veškeré nástroje pro zpracování – parsování a dekódování získaných dat. Nástroj umožňuje data obalit za využití protokolu gsmtap pro jejich následnou vizualizaci v aplikaci Wireshark. Nástroj také umožňuje následné dešifrování dat zabezpečených algoritmem A5 pokud je poskytnut šifrovací klíč.

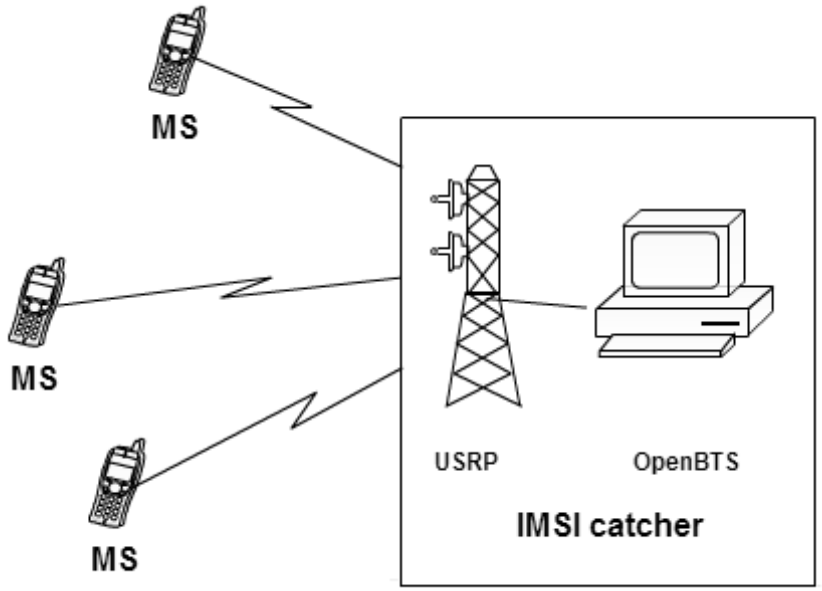
5.2 IMSI catcher

IMSI catcher je zařízení sloužící k identifikaci uživatele získáním jeho IMSI. K získání IMSI využívá vytvoření falešné BTS, ke které se následně připojí okolní mobilní stanice a dojde k odeslání IMSI, aby bylo možno připojené zařízení identifikovat (viz kap. 2.1.1).

IMSI catcher využívá vlastnosti GSM sítě, kdy nedochází k autentizaci BTS vůči MS, a je tak možno ji podvrhnout.

Pro vytvoření IMSI catcheru v rámci této práce bylo využito zařízení USRP společně s OpenBTS. Konfigurace, nastavení a vlastní dokumentace provedení je popsána v následujících podkapitolách.

Teoretický průběh útoku je znázorněn na obrázku 5.3 – je vytvořena falešná BTS s podvrhnutou identitou, v okamžiku kdy dojde k připojení MS v dosahu falešné BTS je v rámci procesu identifikace MS vůči BTS zaznamenána hodnota IMSI.



Obrázek 5.3: *Scénář útoku - IMSI catcher*

5.2.1 **Instalace a konfigurace softwaru**

Pro instalaci byla zvolena verze OpenBTS 2.8. Software byl kompilován ze zdrojových souborů. Výchozím návodem pro postup byl manuál OpenBTS.[24]

```
svn co http://wush.net/svn/range/software/public
```

Před vlastní kompilací OpenBTS je potřeba doinstalovat nezbytné závislosti.

UHD 003.005.002

```
wget https://github.com/EttusResearch/UHD-
Mirror/archive/release_003_005_002.tar.gz
tar -xzf release_003_005_002.tar.gz
```

Před kompilací UHD je potřeba nainstalovat další závislosti :

```
sudo apt-get install libboost-all-dev libusb-1.0-0-dev python-cheetah
doxygen python-docutils cmake
```

Kompilace UHD :

```
cd release_003_005_002/host
mkdir build
cd build
cmake ../
make
make test
sudo make install
sudo ldconfig
```

Další závislosti OpenBTS :

```
autoconf libtool libosip2-dev libortp-dev libusb-1.0-0-dev g++ sqlite3
libsqlite3-dev erlang build-essential subversion
```

Před vlastní kompilací OpenBTS bylo ještě potřeba doinstalovat knihovnu liba53, která je zahrnuta v balíku OpenBTS.

V kořenovém adresáři OpenBTS:

```
cd a53/trunk
sudo make install
```

Poté je možno přistoupit k vlastní instalaci OpenBTS ze zdrojového kódu

```
cd openbts/trunk
autoreconf -i
./configure --with-uhd
Make
```

Vytvoření symbolického odkazu na aplikaci transceiver:

```
cd apps
ln -s ../Transceiver52M/transceiver .
```

V tomto okamžiku bylo možno přistoupit k vlastní konfiguraci OpenBTS pro použití jako IMSI catcher.

Pro uložení konfigurace je v projektu OpenBTS využita externí SQLite databáze, její inicializaci provedeme následovně:

```
sudo mkdir /etc/OpenBTS
sudo sqlite3 -init ./apps/OpenBTS.example.sql /etc/OpenBTS/OpenBTS.db
".quit"
```

5.2.2 **Průběh útoku**

Spuštění OpenBTS :

```
cd apps
sudo ./OpenBTS
```

Po úspěšném spuštění by se měla v okně terminálu zobrazit informace o připravenosti systému:

```
system ready
use the OpenBTSCLI utility to access CLI
```

Při použití defaultní konfigurace je vytvořená síť identifikováná jako testovací – MCC 001 MNC 01. Je zakázána registrace nových zařízení. Proto je potřeba provést konfigurace parametrů pro potřeby IMSI catcheru.

V následující tabulce můžete vidět přehled MCC a MNC českých komerčních mobilních operátorů.

Tabulka 5.1: Přehled MCC a MNC českých operátorů

Provozovatel	MCC	MNC	Název
T-Mobile Czech Republic a.s.	230	01	T-Mobile – CZ
Telefónica O2 Czech republic a.s.	230	02	O2 – CZ
Vodafone Czech Republic a.s.	230	03	Vodafone
Mobilkom a.s.	230	04	U:fon
Vodafone Czech Republic a.s., R&D Centre	230	99	Vodafone / ČVUT

Dále je potřeba zvolit vhodný kanál ARFCN tak, aby nedocházelo k vzájemnému rušení s okolními BTS operátora. Přehled rozdělení kanálů mezi jednotlivé operátory je obsažen v příloze této práce.

Je potřeba připomenout, že obsluhující BTS pomocí kanálů BCCH a informačních zpráv zasílá MS seznam okolních BTS na kterých MS následně provádí měření úrovně signálů, na základě naměřených hodnot může dojít k reselekci BTS.

Podmínky pro přepojení MS k jiné než aktuálně připojené BTS [26]:

1) Hodnota C2 pro neobsluhující BTS je vyšší než hodnota C2 pro obsluhující BTS po dobu 5s, toto platí pro případ, kdy jsou obě BTS ve stejné oblasti (mají stejný LAI).

2) Rozdíl hodnoty C2 pro neobsluhující a obsluhující BTS je vyšší než parametr CELL_RESELECTION_HYSTERESIS, tento parametr je distribuován na kanálu BCCH aktuálně obsluhující BTS, toto platí pro případ, kdy jsou BTS v rozdílných oblastech.

3) Hodnota C1 pro obsluhující BTS spadne pod nulovou hodnotu ($C1 < 0$) po dobu 5s . Toto značí, že došlo k poklesu úrovně signálu pod minimální úroveň.

4) Dojde k blokování/odstavení aktuální BTS

5) Na MS vyprší časový interval DSC (Downlink Signaling Failure Counter), který značí chybu ve spojení s BTS, poté dochází k prohledání celého GSM spektra podobně jako v případě po zapnutí MS

Pro konfiguraci IMSI catcheru jsem zvolil přístup pomocí 2. podmínky pro přepojení MS k IMSI catcheru. Pro provedení testů jsem disponoval SIM kartou operátora O2 Telefonica a proto bylo potřeba provést monitoring okolních BTS tohoto operátora. Abych dosáhl co nejrychlejšího přechodu MS k IMSI catcheru zvolil jsem ARFCN stejné jako měla BTS s nejnižší hodnotou úrovně signálu, jež byla uvedena v seznamu okolních BTS. Pro zobrazení kvality signálu byla použita aplikace GSM Signal monitoring pro Android. Průběh měření je zachycen v následující tabulce 5.2. Tabulka zahrnuje informace o aktuálně obsluhující základnové stanici (tučně zvýrazněna) a informace z měření kvality signálu sousedních BTS.

Tabulka 5.2: *Měření signálu okolních BTS*

Cell ID	LAC	ARFCN	Síla signálu [dBm]
7047	**1713**	**84**	**-95**
17051	1713	94	-101
27108	1713	46	-103
17041	1713	45	-103
17050	1713	87	-105

Provedení konfigurace OpenBTS pro provozování IMSI catcher prostřednictvím konzolového přístupu k OpenBTS :

```
config Control.LUR.OpenRegistration .* // umožní registraci všech
zařízení
config GSM.Radio.Band 900 // volba GSM pásma 900
config GSM.Radio.C0 87  // nastavení ARFCN
config GSM.Identity.MCC 230 // nastavení MCC operátora O2
config GSM.Identity.MNC 02 // nastavení MNC operátora O2
config GSM.Identity.ShortName O2-CZ // nastavení názvu sítě
config GSM.Identity.ID 10 // nastavení Cell ID
config GSM.Identity.LAC 1714 //nastavení LAC
```

Po této konfiguraci bylo potřeba restartovat aplikaci OpenBTS, aby došlo k aplikování nového nastavení.

Následující tabulka 5.3 znázorňuje výsledky měření kvality signálu okolních BTS ještě před okamžikem než došlo k připojení na BTS s vyšší kvalitou signálu. Je možno vidět stále stejnou obsluhující BTS s Cell ID 7047, následně však druhá v pořadí je již podvržená BTS v podobě IMSI catcheru. Následně dochází k handoveru MS k BTS se silnějším signálem. Je potřeba zmínit, že při těchto měřeních není správně zobrazeno Cell ID a LAC IMSI catcheru, podle dostupných informací se jedná o problém v měřící aplikaci.

Tabulka 5.3: *Měření signálu okolních BTS po spuštění IMSI catcheru*

Cell ID	LAC	ARFCN	Síla signálu [dBm]
7047	**1713**	**84**	**-89**
17050	1713	87	-51
27108	1713	46	-103
17051	1713	45	-105
17041	1713	87	-105

Při testování bylo zjištěno, že u různých mobilních zařízení dochází k rozdílnému chování v okamžiku, kdy by mělo přijít k přepojení na BTS se silnějším signálem. Většina starších zařízení se připojovala na OpenBTS téměř okamžitě, po provedení měření a výpočtu hodnoty C2. Toto bylo otestováno na telefonech Nokia 3210, Nokia 6230i a LG C3300. V případě novějších zařízení docházelo k rozdílnému chování. Např. Samsung Galaxy S2, Apple IPhone 4 se připojili opět téměř ihned, na rozdíl od zařízení Gigabyte GSMART Roma R2 nebo Sony Xperia L, kdy pro připojení k BTS bylo potřeba zařízení restartovat a vyvolat tak znovu prohledání GSM spektra.

Tabulka 5.4 pak zobrazuje situaci poté, co došlo k připojení MS k IMSI catcheru. Z hlediska běžného uživatele není možné registrovat, že je objektem jakéhokoliv útoku. V konfiguraci OpenBTS není nastaven seznam okolních BTS a proto nebude docházet k měření okolních BTS popř. následného přechodu k těmto BTS.

Tabulka 5.4: *Měření signálu po připojení k IMSI catcheru*

Cell ID	LAC	ARFCN	Síla signálu [dBm]
10	**1714**	**87**	**-51**

Pro zobrazení IMSI mobilních zařízení obsluhovaných OpenBTS pak slouží příkaz *tmsis*, který v konzoli vypisuje seznam IMSI a k nim přiřazeným TMSI. Zachycené IMSI jsou pak zobrazeny v následujícím výpisu:

```
OpenBTS> tmsis
TMSI       IMSI            age  used
       1 230022901372117   16d    7d
       3 230024100906226   16d    7d
       6 230029101230104   16d   16d
       5 231060900102504   16d   16d
       4 231014451342246   16d   16d
       2 230020701214669   16d   16d
```

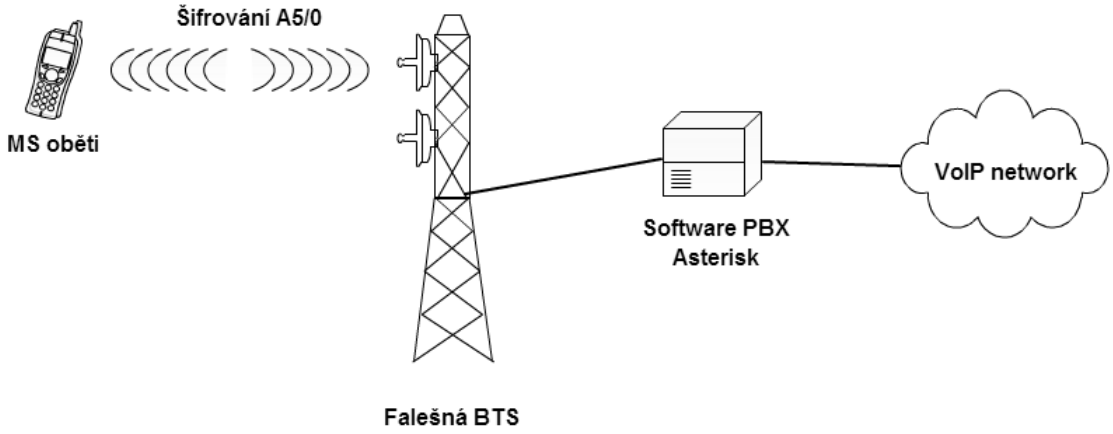
Za použití volně dostupných nástrojů bylo možno vytvořit a úspěšně provozovat IMSI catcher. Po prvotní instalaci je možno IMSI catcher nakonfigurovat podle aktuálních podmínek a následně spustit v řádu několika málo minut. Je potřeba si uvědomit, že v okamžiku kdy je mobilní zařízení připojeno k IMSI catcheru nelze na zařízení přijímat a odesílat hovory či SMS. Aby nedošlo k prozrazení probíhajícího útoku je potřeba minimalizovat dobu kdy je IMSI catcher v provozu. Provozování IMSI catcheru je v ČR i většině ostatních zemí nelegální.

5.3 Aktivní odposlech - falešná BTS

Princip aktivního útoku vychází z koncepce IMSI catcheru, kdy je jeho funkčnost rozšířená o možnosti realizace odchozích hovorů a odesílání SMS. Tím, že útočník má plnou

kontrolu nad konfigurací BTS, je možno kompletně vypnout šifrování hovorových dat a získat tak k datům okamžitý přístup.

Scénář útoku je zobrazen na následujícím diagramu (obrázek 5.4), je vytvořena falešná BTS s podvrhnutou identitou, následně dojde k přepojení MS oběti k falešné BTS. V okamžiku kdy dojde k odchozímu hovoru je zaznamenáno číslo volajícího a celý hovor je pomocí Asterisku nahrán a přesměrován pomocí sítě VoIP na volanou stanici s podvrženou identitou volajícího.



Obrázek 5.4*: Scénář útoku pomocí falešné BTS*

5.3.1 **Instalace a konfigurace**

Jak bylo zmíněno v úvody této podkapitoly, vytvoření falešné BTS vychází z IMSI catcheru a pro vlastní realizaci bylo také použita kombinace softwarového rádia USRP N210 pro rádiovou část a OpenBTS pro demodulaci signálu a řízení základnové stanice. Postup instalace a konfigurace této části je popsán v podkapitole 5.2.1. Aby bylo možno pomocí OpenBTS uskutečňovat hovory a odesílat SMS zprávy je potřeba doinstalovat další součásti OpenBTS:

Subscriber registry – slouží k nahrazení funkčnosti HLR v běžné GSM síti a pomocí upraveného SIP registru umožňuje uchovávat data o uživatelích.[24]

Smqueue – server pro zpracování a odesílání SMS zpráv v systému OpenBTS.[24]

Pobočková ústředna Asterisk slouží jak k provádění signalizace prostřednictvím protokolu SIP, tak k řízení a přepojování hovorů.

Instalace Subscriber registry z balíku OpenBTS :

```
cd subscriberRegistry/trunk/
make
cd configFiles/
mkdir -p /var/lib/asterisk/sqlite3dir
sqlite3 -init subscriberRegistryInit.sql
/var/lib/asterisk/sqlite3dir/sqlite3.db ".quit"
```

```
sqlite3 -init ../sipauthserve.example.sql /etc/OpenBTS/sipauthserve.db
".quit"
```

Instalace Smqueue:

```
cd smqueue/trunk/
./autogen.sh
autoreconf -i
./configure
make
make install
sqlite3 -init smqueue.example.sql /etc/OpenBTS/smqueue.db ".quit"
```

Instalace pobočkové ústředny Asterisk 1.8.13.1 :

```
apt-get install asterisk
```

Podrobná konfigurace Asterisku je přiložena k této diplomové práci.

Každý účastník připojený pomocí OpenBTS je pro potřeby asterisku identifikován jako SIP koncový uživatel s uživatelským jménem „IMSIxxxxxxxxxxxxxx“, kde xxx je IMSI registrované SIM karty o délce 14-15 znaků. IP adresa uživatele je shodná s IP obsluhující OpenBTS. Samotná OpenBTS je pak v případě vytvoření VoIP sítě „neviditelná“.[24]

5.3.2 **Průběh útoku**

Nejprve bylo potřeba podobně jako v případě IMSI catcheru zjistit údaje pro konfiguraci OpenBTS. Pro vytvoření falešné BTS byla zvolena síť operátora O2, přehled hodnot GSM identifikačních údajů operátora je možné nalézt v tabulce 5.1. Výsledná konfigurace OpenBTS:

```
config Control.LUR.OpenRegistration .* // umožní registraci všech
zařízení
config GSM.Radio.Band 900 // volba GSM pásma 900
config GSM.Radio.C0 1 // nastavení ARFCN
config GSM.Identity.MCC 230 // nastavení MCC operátora O2
config GSM.Identity.MNC 02 // nastavení MNC operátora O2
config GSM.Identity.ShortName O2-CZ // nastavení názvu sítě
config GSM.Identity.ID 10 // nastavení Cell ID
config GSM.Identity.LAC 1000 //nastavení LAC
```

Po spuštění OpenBTS dojde k vytvoření falešné BTS s výše uvedenými parametry. Následně dochází k připojení MS oběti k této BTS. Připojení MS je možno kontrolovat pomocí konzolové aplikace OpenBTS příkazem *tmsis*.

V případě odchozího hovoru je daný hovor přesměrován pomocí konfigurace Asterisku na jeden z pevně definovaných softwarových telefonů ve VoIP sítí vytvořené Asteriskem. Toto

v laboratorních podmínkách simuluje uskutečnění hovoru pomocí externího poskytovatele VoIP telefonie.

Podvržení identity volajícího a záznam hovoru je proveden pomocí funkcí Asterisku. Nastavení identity volajícího je provedeno pomocí konfigurace v souboru extensions.conf. V tomto souboru dochází také k definici nahrávání hovorů do audio stopy v prostředí asterisku. Celý konfigurační soubor je součástí přílohy této DP.

5.4 Pasivní odposlech

V obou předchozích popsaných případech bylo potřeba provozovat obousměrnou komunikaci mezi napadenou MS a falešnou BTS. Při využití vysílače se však útočník vždy vystavuje možnosti odhalení a poměrné snadné lokalizace v případě, kdy se na něj někdo zaměří. V případě pasivního odposlechu komunikace nedochází k žádnému aktivnímu vysílání ze strany útočníka, a proto se možné odhalení v tomto ohledu minimalizuje.

V kapitole 4.2 byl popsán odposlech komunikace mezi BTS a MS pomocí zařízení USRP. I přes podstatné snížení nákladů na provedení útoků využitím open-source nástrojů je stále potřeba využít relativně drahé zařízení USRP (desítky tis. Kč). V průběhu roku 2013 se ukázala možnost využití velice levného zařízení určeného primárně pro příjem DVB-T signálu. Tímto krokem došlo ke snížení nákladů na provedení pasivního odposlechu na minimální úroveň (stovky až jednotky tisíc Kč).

Tato část pak popisuje celkový průběh prováděného odposlechu komunikace. Je rozdělena na dvě části, nejprve byl proveden odposlech komunikace v testovací sítí vytvořené pomocí OpenBTS. Druhá část se věnuje odposlechu komunikace v sítí reálného mobilního operátora.

5.4.1 Instalace a konfigurace

Pro první variantu odposlechu testovací sítě bylo potřeba nainstalovat a nakonfigurovat USRP a OpenBTS, tento proces je popsán v kap. 5.3.

Pro zachycení komunikace byl použit nástroj rtl-sdr z balíku Osmocom. Před vlastní instalací je potřeba získat doplňkové balíky.

```
sudo apt-get install libusb-1.0-0-dev
```

Instalace rtl-sdr:

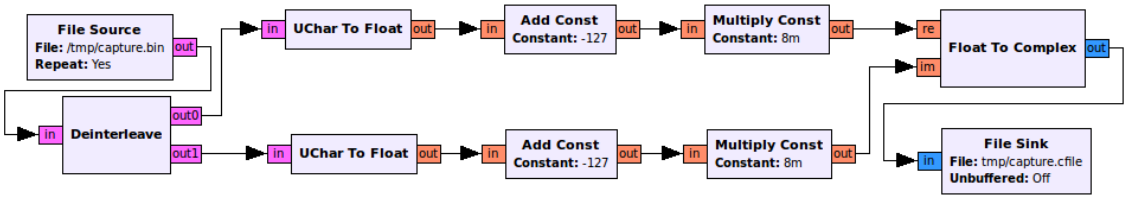
```
git clone git://git.osmocom.org/rtl-sdr.git
cd rtl-sdr/
mkdir build
cd build
cmake ../
make
sudo make install
sudo ldconfig
```

Levné zařízení rtl-sdr sebou nese také určité problémy ohledně kvality použitého tuneru. Je proto potřeba provést kalibraci zařízení – jedná se o zjištění odchylky v reálné frekvenci tuneru a frekvenci, která se zobrazuje uživateli. Pro účel kalibrace byl použit nástroj kalibrate-rtl.

```
git clone https://github.com/steve-m/kalibrate-rtl.git
cd kalibrate-rtl/
./bootstrap
./configure
make
make instar
```

Nyní je pro zjištění odchylky (offset) potřeba aplikaci pomocí parametru – *c* poskytnout hodnotu ARFCN jedné z okolních BTS. Pro zjištění ARFCN okolních BTS je možno spustit aplikaci s parametrem *–s GSM900*. [23]

Pro převod dat získaných pomocí aplikace rtl_sdr do formátu podporovaného aplikací airprobe bylo použito jedné z aplikací balíků GNU Radio – GRC – umožňuje vytvářet pomocí grafického rozhraní spustitelné skripty pro různé využití. Návrh diagramu pro vytvoření skriptu byl převzat z OsmocomSDR.[23] Ukázka diagramu je na obrázku 5.5. Využití tohoto převodu je dáno tím, že aplikace airprobe používá pro vstup formát souboru cfile s komplexními hodnotami, kdežto výstupem aplikace rtl-sdr je binární datový soubor.



Obrázek 5.5: *GRC schéma pro převod zdrojových dat na cfile*

Aby bylo možno zobrazit získaná data v protokolovém analyzátoru Wireshark využívá airprobe pseudo-záhlaví GSMTAP, které slouží k obalení zpráv systému GSM do UDP paketů.[19] Toto obstarává balík libosmocore.

```
git clone git://git.osmocom.org/libosmocore.git
cd libosmocore
autoreconf -i
./configure
make
sudo make install
sudo ldconfig
```

Jak již bylo několikrát zmíněno pro vlastní interpretaci zachycených dat je využit nástroj Airprobe. U tohoto balíku jsem při instalaci narazil na značné množství problému, jednalo se především o problémy s balíky, na kterých je airprobe závislé. Dále pak o problémy s vlastní kompilací zdrojových souborů. Původní balík zveřejněný autory na webu srlab.de v roce 2009 nebyl nadále udržován a pro dnešní použití byl nepoužitelný. Proto byla využita

modifikovaná varianta vytvořena uživatelem ttsou. Před vlastní instalací bylo potřeba přidat další balíky závislostí.

```
sudo apt-get install gnuradio-dev libboost-all-dev libfftw3-dev swig
python-numpy
```

Instalace airprobe:

```
git clone https://github.com/ttsou/airprobe.git
cd airprobe/gsm-receiver
./bootstrap
./configure
make
```

5.4.2 **Průběh útoku – OpenBTS**

Tento scénář byl zvolen z důvodu ověření funkčnosti všech komponent systému. Bylo totiž možno využít znalostí o konfiguraci GSM sítě. Toto zahrnuje především znalost kanálu ARFCN, na kterém je BTS provozována, dále možnost získat jednoduše informace o identifikaci uživatelů v rámci sítě (IMSI, TMSI). OpenBTS byla provozována ve stejné laboratoři, kde byl prováděn také odposlech, což zajistilo vysokou úroveň přijímaného signálu a následně také bezproblémovou demodulaci a interpretaci získaných dat.

Dalším zásadním rozdílem mezi reálnou sítí operátora a využitím OpenBTS byla absence šifrování signalizačních a komunikační kanálů systému GSM. Proto také není v této části řešen způsob získání šifrovacího klíče K_c.

Konfigurace OpenBTS :

```
config Control.LUR.OpenRegistration .* // umožní registraci všech
zařízení
config GSM.Radio.Band 900 // volba GSM pásma 900
config GSM.Radio.C0 1  // nastavení ARFCN
config GSM.Identity.MCC 001 // nastavení testovacího MCC
config GSM.Identity.MNC 02 // nastavení testovacího MNC
config GSM.Identity.ShortName OpenBTS // nastavení názvu sítě
config GSM.Identity.ID 10 // nastavení Cell ID
config GSM.Identity.LAC 1000 //nastavení LAC
```

Pro nastavení Asterisku byla využita konfigurace, která vychází z konfigurace popsané v kap. 5.3. Je tedy nastaveno přesměrování všech hovorů na jedinou koncovou stanici identifikovanou pomocí IMSI 230024100906226. Kompletní konfigurace je obsažena v příloze této práce.

Bylo opět potřeba také provést kalibraci DVB-T USB receiveru, pro toto jsem využil aplikaci kalibrate-sdr. Kalibrace byla provedena pomocí testovací OpenBTS na kanálu ARFCN 1 :

```
kal -c 1
Found 1 device(s):
  0:  ezcap USB 2.0 DVB-T/DAB/FM dongle
```

```
Using device 0: ezcap USB 2.0 DVB-T/DAB/FM dongle
Found Rafael Micro R820T tuner
Exact sample rate is: 270833.002142 Hz
kal: Calculating clock frequency offset.
Using GSM-900 channel 58 (946.6MHz)
average         [min, max]    (range, stddev)
- 39.908kHz     [-39921, -39886]    (35, 9.224885)
overruns: 0
not found: 0
average absolute error: 42.159 ppm
```

Z výše zjištěného je podstatná zejména hodnota -39.908 kHz, která udává absolutní hodnotu odchylky. Relativní odchylka je pak udána jako hodnota 42.159 ppm. Tuto hodnotu je pak nutno odečíst od hodnoty frekvence při zachytávání komunikace.

V tomto okamžiku je možné přistoupit k zachycení komunikace mezi OpenBTS a MS.

```
rtl_sdr –f 935.2M –s 1.0e6 data_openbts_arfcn1.bin
```

- parametr –f určuje frekvenci signálu GSM
- parametr –s nastavuje vzorkovací frekvenci 1MHz
- data_openbts_arfcn1.bin určuje název souboru se získanými daty

```
rtl_sdr -f 935.161e6 -s 1.0e6 data_openbts_arfcn1.bin
Found 1 device(s):
  0:  Realtek, RTL2838UHIDIR, SN: 00000001

Using device 0: ezcap USB 2.0 DVB-T/DAB/FM dongle
Found Rafael Micro R820T tuner
Exact sample rate is: 1000000.026491 Hz
Tuned to 935200000 Hz.
Reading samples in async mode...
```

V průběhu útoku byla odesláná SMS z terminálu OpenBTS na MS identifikovanou IMSI 230024100906226. Dále byl proveden telefonní hovor mezi dvěmi MS připojenými k testovací BTS. Po dokončení testovacího hovoru je ukončeno získávání dat pomocí Ctrl + C.

```
OpenBTS> sendsms 230024100906226 1234 Testovaci
message submitted for delivery
```

Dalším krokem je převod získaných dat do formátu cfile. V aplikaci GRC byl jako zdrojový soubor zvolen soubor zachycených dat *data_openbts_arfcn1.bin*, jako výstupní soubor pak *data_openbts_arfcn1.cfile* ve složce */home/gsmsec/airprobe/gsm-receiver/src/python/*

Pro další analýzu dat bude využit skript go.sh z aplikace gsm-reciever v balíku airprobe. Tento skript demoduluje získaná data na základě poskytnuté konfigurace a získaný výstup pak odesílá na místní síťové rozhraní – localhost s doplněným pseudo-záhlavím GSMTAP[19].

Parametry skriptu go.sh jsou následující[19]:

go.sh *decimation_rate channel_config session_key*

decimation_rate – určuje hodnotu pro downsampling, pro kompatibilitu s rtl_sdr je tato hodnota 64

channel_config – umožňuje určit logický kanál a timeslot pro zpracování, možné konfigurace channel_config :

- 0C – Konfigurace s kombinovaným signalizačním kanálem
- 0B – Konfigurace s odděleným signalizačním kanálem
- 1S – Signalizační kanál v timeslotu 1
- 1-7T – Přenosový kanál v timeslotu 1 až 7

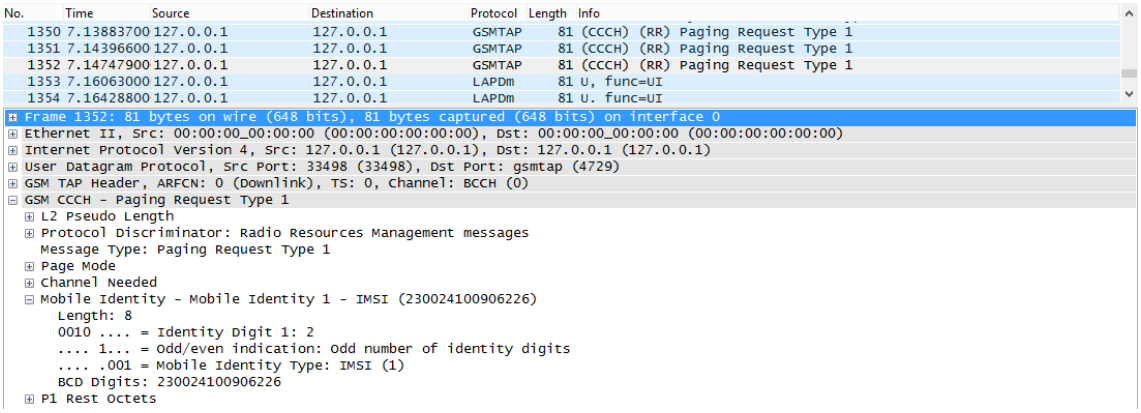
session_key – hodnota šifrovacího klíče Kc

Bližší popis logických kanálu sítě GSM je možno nalézt v kapitole 1.2.4.6

Dle dokumentace OpenBTS je použita varianta s kombinovaným signalizačním kanálem, proto jsou zvoleny následující parametry. Pokud není parametr *session_key* uveden dojde ke zpracování pouze nešifrovaných burstů.

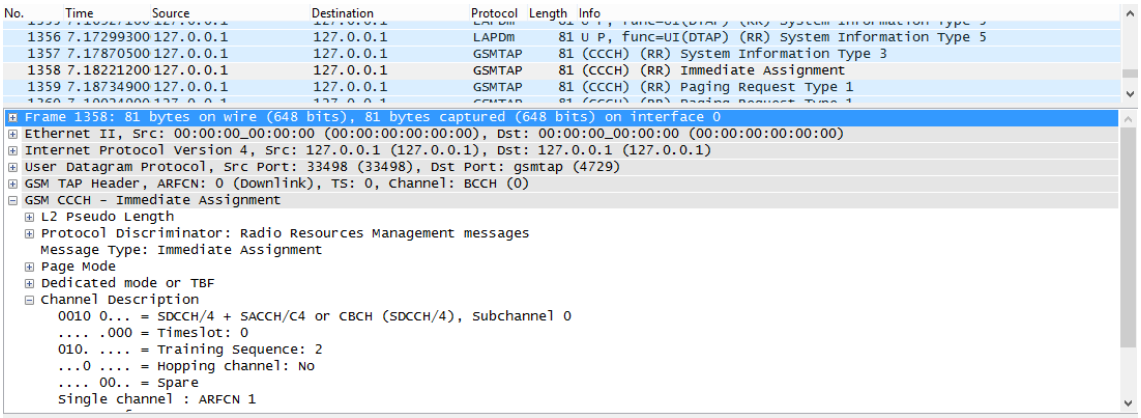
```
./go.sh data_openbts_arfcn1.cfile 64 0C
```

Na obrázku 5.6 je možno vidět okamžik kdy dojde k pagingu MS, což MS oznamuje, že má na určeném kanálu naslouchat následující signalizaci.



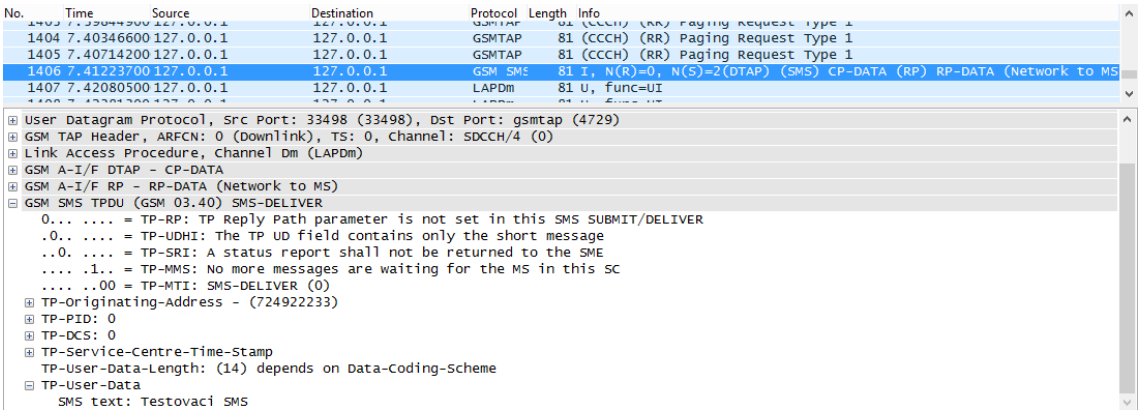
Obrázek 5.6: *Paging MS*

Poté je odesláním Immediate Assignment (obrázek 5.7) sestaven logický komunikační kanál mezi MS a BTS, jehož prostřednictvím bude odeslána vlastní SMS.



Obrázek 5.7: *Immediate Assignment – přidělení SDCCH kanálu*

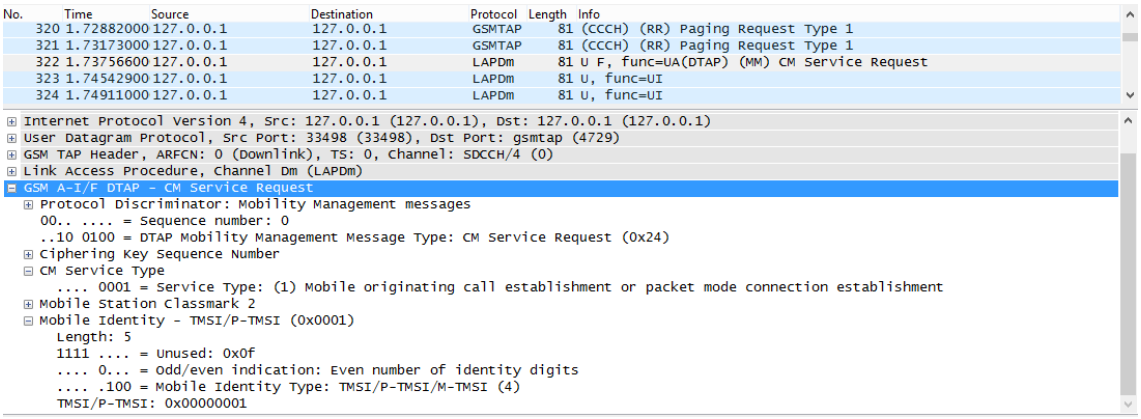
V tomto okamžiku je možno přistoupit k přečtení odeslané SMS. Obsah SMS je zachycen na obrázku 5.8.



Obrázek 5.8: *Odeslaná SMS*

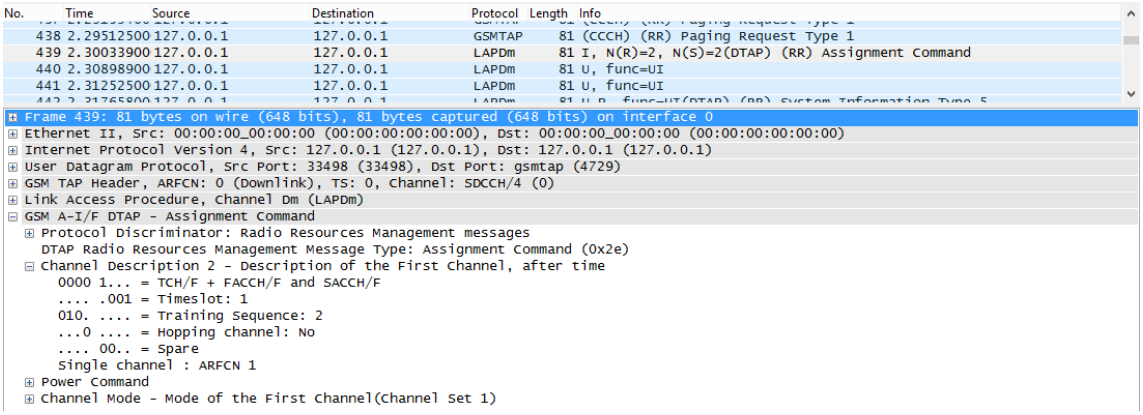
Po potvrzení odeslání a přijetí SMS následuje příkaz k uvolnění signalizačního kanálu.

Před získáním hovorových dat je potřeba provést analýzu signalizačního kanálu. Opět je stejně jako v případě SMS vyvolán Paging a přidělení signalizačního kanálu pomocí Immediate Assignment. V tomto okamžiku MS odesílá požadavek služby (CM Service Request – obrázek 5.9). MS v této zprávě žádá o službu odchozího hovoru MOC (Mobile originating call) a identifikuje se pomocí TMSI. BTS odpovídá pomocí CM Service Accept, ve které službu (v tomto případě MOC) potvrzuje.



Obrázek 5.9: *CM Service Request*

Následně je MS, ze které je hovor prováděn pomocí zprávy Assignment Command oznámeno, aby naslouchala přenosovému kanálu TCH a k němu asociovanému signalizačnímu kanálu na TS 1 (Obrázek 5.10).



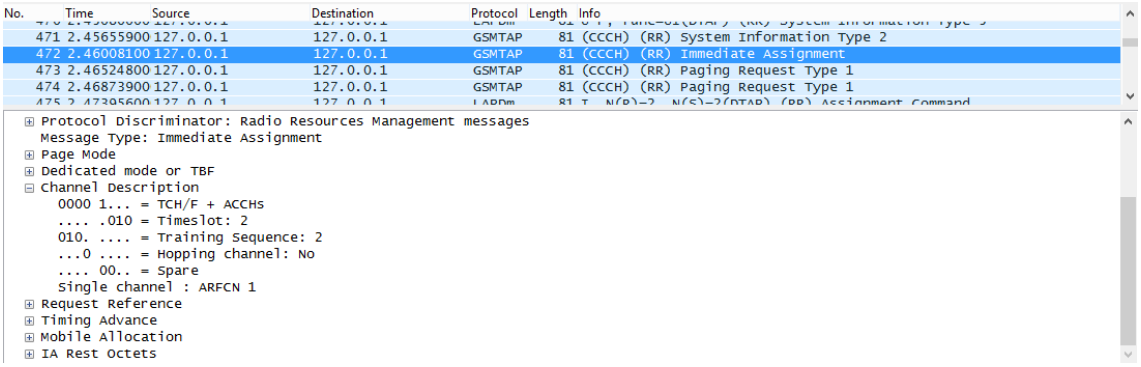
Obrázek 5.10: *Assignment Command*

Jelikož je i volaná MS připojena ke stejné BTS dochází zároveň k sestavení příchozího hovoru - MTC (Mobile Terminated Call) – opět je nejprve MS oznámeno pomocí pagingu na BCCH, že je potřeba sledovat sdílený signalizační kanál SDCCH. Immediate Assignment pak přiděluje volané MS rovnou hovorový kanál na TS 2, kde proběhne nezbytná signalizaci i vlastní hovor. Toto je možno vidět na obrázku 5.11. BTS dále na přiděleném signalizačním kanále odesílá zprávu Call Setup obsahující informace o volajícím.

Nyní jsou již známy veškeré potřebné informace k dekódování hovorových dat. Tyto údaje jsou shrnuty v následující tabulce 5.5.

Tabulka 5.5: *Přehled přidělených hovorových kanálů*

Identita	**Kanál (Timeslot)**
TMSI 1	TCH/F (1)
IMSI 230024100906226	TCH/F (2)



Obrázek 5.11: *Immediate Assignment volané MS*

Airprobe v případě konfigurace s hovorovým kanálem ukládá do výstupního souboru získaná hovorová data. Hovor je pak uložen v audio formátu *au.gsm*.

Pro získaní hovorových dat z TS1 je použit následující příkaz :

```
./go.sh data_openbts_arfcn1.cfile 64 1T 0000000000000000
```

Pro správnou funkci skriptu je potřeba doplnit šifrovací klíč samými nulami.

Výstupem pak je soubor *speech.au.gsm*.

Jelikož soubor formátu *gsm* není možno běžně přehrát je potřeba převést získaný soubor pomocí aplikace *toast* do audio formátu *au*.

```
toast -d speech.au.gsm
```

Získaný soubor jsem následně přejmenoval

```
mv speech.au call_ts1.au
```

Tento soubor lze následně přehrát pomocí konzolové verze přehrávače VLC

```
cvlc call_ts1.au
```

Obdobný proces byl následně proveden i pro TS 2 :

```
./go.sh data_openbts_arfcn1.cfile 64 2T 0000000000000000
toast -d speech.au.gsm
mv speech.au call_ts2.au
cvlc call_ts2.au
```

Při poslechu získaných hovorů je bohužel možno slyšet rušení, jelikož hovorová data jsou vysoce citlivá na chybovost. Toto je jednak způsobeno nedokonalostí synchronizace MS a OpenBTS. Dále může být kvalita zhoršena rušením signálů získaného pomocí DVB-T přijímače.

Všechny výstupní soubory a logy z aplikace Wireshark jsou součástí příloh této práce.

5.4.3 **Průběh útoku – Reálná BTS**

Jako další krok v pasivním odposlechu jsem chtěl ověřit možnost zachycení a analýzy datového provozu mezi BTS a MS v reálné sítí GSM provozované lokálním operátorem.

Při reálné útoku by bylo potřeba nejprve oběť lokalizovat, toto by bylo provedeno pomocí HLR Query. Princip této lokalizace je popsán v kapitole 4.

Následně by bylo potřeba zjistit identitu TMSI oběti útoku. Toto je možno provést zasíláním narušených SMS zpráv tzv. Silent SMS, které jsou doručeny na cílovou MS, avšak nejsou z důvodu poškození uživateli zobrazeny. Opět je princip tohoto útoku podrobněji rozebrán v kapitole 4.

Oba tyto kroky bylo možno přeskočit, protože jsem prováděl testovací odposlech komunikace MS ve svém vlastnictví.

Po analýze okolní situace byla jako nejvhodnější BTS k zachycení provozu zvolena BTS operátora O2 s identifikátorem 17051. Analýza byla provedena pomocí aplikace GSM Signal Monitoring na mobilním telefonu s OS Android. Bližší popis odposlouchávané BTS jsem získal pomocí databáze českých základnových stanic na webu www.gsmweb.cz a je znázorněn v tabulce 5.6.

Tabulka 5.6: *Informace o BTS s identifikátorem Cell ID 17051*

CID	LAC	ARFCN	BSIC	Okres	Umístění0
17051	1713	94	45	Ostrava	Ostrava-Poruba, Pavlouskova 4333/1

Zvolené BTS je provozujícím operátorem přidělen frekvenční kanál ARFCN 94. Toto odpovídá frekvenci 953.8MHz pro downlink a 908.8MHz pro uplink.

Pro záznam komunikace byl použit nástroj rtl_sdr s následující konfigurací :

rtl_sdr –f 953.761e6 –s 1e6 data_gsm_17051.bin

Výsledná frekvence f byla opět získána odečtením odchylky zařízení od reálné frekvence. Komunikace pak byla zaznamenána do souboru *data_gsm_17051.bin*. Jako vzorkovací frekvence byla zvolena hodnota 1MHz.

Během zachytávání komunikace byl proveden telefonní hovor ve směru od monitorované MS a následně byla na tuto stanici také zaslána SMS zpráva.

Po ukončení sběru dat bylo potřeba převést soubor *data_gsm_17051.bin* do formátu cfile pomocí aplikace GRC. Výsledný soubor pak byl uložen pod názvem *data_gsm_17051.cfile*

Před další analýzou dat je potřeba získat hodnotu TMSI oběti. TMSI je identifikace MS pro potřeby sítě GSM a proto je tato hodnota pro koncového uživatele běžným způsobem nepřístupná. Pro zjištění TMSI bylo proto v laboratoři využito čtečky SmartCard a aplikace SIMSpyII. Pomocí této aplikace je také možno zjistit poslední použitou hodnotu šifrovacího klíče K_c. Výstup aplikace SIMSpy je zachycen na obrázku 5.12

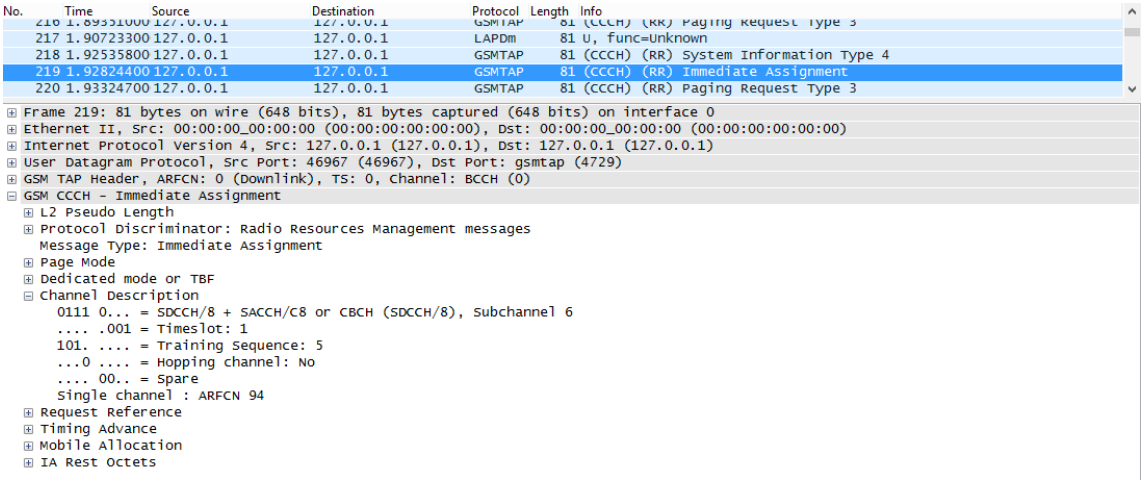
EF_{loci}	Location information	TMSI: 16 21 A3 15 LAI: 230 02 06B1 (1713) LA update state: updated successfully
EF_{kc}	Ciphering key Kc	33 B2 9A 6B E4 75 68 3A (key sequence nr. 3)

Obrázek 5.12: *Získání TMSI a šifrovacího klíče K_c pomocí aplikace SIMSpyII*

Nyní bylo možné provést analýzu získaných dat.

```
./go.sh data_gsm_17051.cfile 64 0C
```

Jelikož se jednalo o reálnou BTS bylo potřeba zjistit kdy došlo k Pagingu sledované MS a to proto, že poté následuje příkaz Immediate Assignment určující následný kanál pro komunikaci. Na následujícím obrázku 5.13 je možné vidět Paging Request s TMSI oběti a následný Immediate Assignment.



Obrázek 5.13: *Přidělení signalizačního kanálu pro odchozí hovor*

V tomto okamžiku MS začne sledovat signalizační kanál SDCCH/8 na TS 1. Dalším krokem je tedy analýza tohoto kanálu:

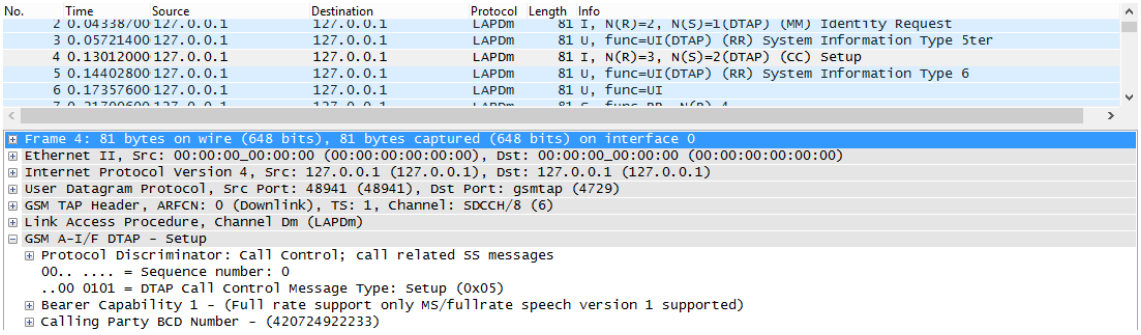
```
./go.sh data_gsm_17051.cfile 64 1S
```

Většina komunikace na tomto kanálu je však šifrovaná a proto při nezadání šifrovacího klíče získáme pouze nešifrované informace, jako jsou autentizační požadavky, Location Update, a především zprávy Ciphering Mode Command, které zahajují proces šifrování komunikace mezi MS a BTS.

V reálném útoku by nyní bylo potřeba provést prolomení šifrovacího klíče Kc, princip tohoto útoku je popsán v kapitole 4. Jak již bylo zmíněno výše, pro testovací účely byl získán šifrovací klíč pomocí aplikace SIMSpy a čtečky SmartCard.

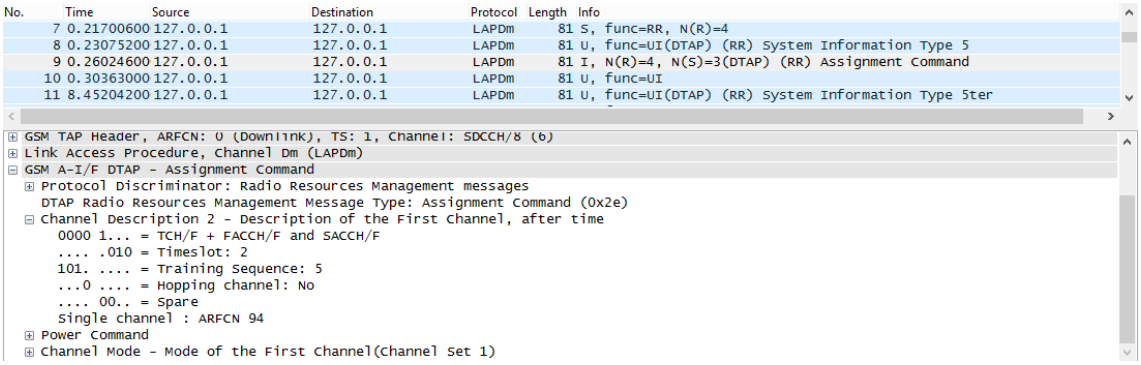
```
./go.sh data_gsm_17051.cfile 64 1S 33b29a6be475683a
```

Analýzou výstupu je možno odhalit číslo volajícího (obrázek 5.14) ve zprávě Call Setup.



Obrázek 5.14: *Číslo volajícího*

Následuje přidělení hovorového kanálu zprávou Assignment Command, ze které je možné identifikovat TS (2) a konfiguraci hovorového kanálu. Toto je zobrazeno na obrázku 5.15.



Obrázek 5.15: *Přidělení hovorového kanálu*

Následně je možné přistoupit také k získání vlastních hovorových pomocí následujícího příkazu:

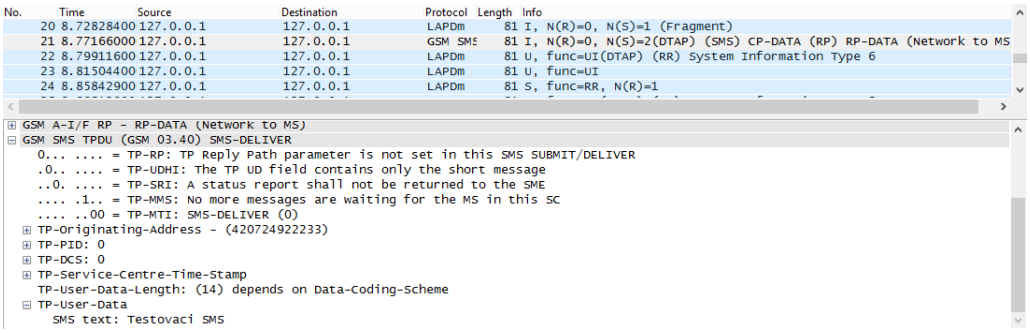
```
./go.sh data_gsm_17051.cfile 64 2T 33b29a6be475683a
```

Výstupní zvukový soubor je následně konvertován a přejmenován.

```
toast -d speech.au.gsm
mv speech.au call_ts2_gsm_17051.au
cvlc call_ts2_gsm_17051.au
```

Délka audio souboru odpovídá délce hovoru, nicméně provedené konverzaci nelze rozumět.

Zachycení SMS pak mělo obdobný průběh jako při odposlechu v testovací síti a samotná SMS včetně odchozího čísla je možné vidět na obrázku 5.16.



Obrázek 5.16: *Odeslaná SMS*

V rámci této části se tedy úspěšně podařilo získat a dešifrovat signalizační data přenášená rádiovým prostředím mezi reálnou BTS a testovacím mobilním zařízením. Je možno získat obsah SMS zpráv, popř. informace o sestavování hovorů. Vlastní telefonní hovor se nepodařilo úspěšně obnovit, toto je pravděpodobně způsobeno nedostatečnou kvalitou signálu popř. dalšími problémy při zachytávání dat.

6 Vhodná bezpečnostní opatření

V této části se zaměřuji na zhodnocení rizik v systému GSM a na možnosti vhodných bezpečnostních opatření k jejich minimalizaci. Jak z teoretické části, kde popisuji realizované útoky vůči GSM síti tak z prakticky provedených pokusů je patrné, že bezpečnost GSM systému je v kritické situaci a její zneužití je možné s minimálními náklady.

6.1 Obousměrná autentizace

Ačkoliv se podvržení základnové stanice zdálo při návrhu systému GSM jako nepravděpodobné, s rozvojem technologií a snížením nákladu se tento útok stal jednoduše uskutečnitelný. Jako minimální vhodné opatření proti podvržení základnové stanice je posílení procesu autentizace. Zavedením obousměrné autentizace mezi MS a BTS by bylo významně komplikováno podvržení základnové stanice.

Na téma vzájemné autentizace v systému GSM bylo publikováno několik zpráv, nicméně závazně nebyla přijata žádná specifikace umožňující následnou implementaci. V tomto ohledu je potřeba urychlit přechod na sítě 3. nebo 4. generace, které vzájemnou autentizaci nativně podporují.

6.2 Šifrování komunikace

Šifrovací algoritmy A5/1 a A5/2 použité pro utajení dat a signalizace lze v současnosti považovat za nedostatečné. V roce 2006 vydala asociace 2006 doporučení ohledně zastavení podpory šifry A5/2. Podpora šifrovacího algoritmu A5/3 byla dodatečně přidána a v současnosti se její podpora postupně rozšiřuje napříč jednotlivými operátory.

Byly vypracovány zprávy popisující teoretickou prolomitelnost A5/3, které jsou však v současné době prakticky nerealizovatelné. Nicméně ani použitím silnějšího šifrování není zajištěna bezpečnost přenášených dat. Konfigurace šifrování je v systému GSM volitelná a dokud bude GSM podporovat šifry, které jsou již prolomeny (A5/1) je možno využitím útoku prostřednictvím falešné BTS získat použitý šifrovací klíč. Toto je dáno principem fungování A3/8 (viz kapitola 2.1.1) , kdy pro shodnou výzvu RAND je vypočten shodný šifrovací klíč.

Závěr

Cílem této práce bylo provedení analýzy bezpečnostních problému systému GSM a následná praktická realizace vybraných útoků. Je zde popsána architektura sítě GSM se zaměřením na rádiové rozhraní, kde jsou především popsány bezpečnostní mechanismy, logické kanály a signalizace. Jsou zde prezentovány nejznámější bezpečnostní rizika systému GSM společně s popisem realizace útoků, které byly do dnešní doby prezentovány.

Hlavní částí této práce pak byla samotná realizace vybraných útoků. Realizace všech útoků byla spojena s komplikacemi ohledně kompatibility a dostupností potřebných nástrojů, kde tyto nástroje většinou nebyly doplněny o potřebnou dokumentaci.

V případě realizace IMSI catcheru jsem úspěšně za využití OpenBTS a softwarového rádia USRP vytvořil podvrženou základnovou stanici, která umožňovala získání hodnot IMSI uživatelů, kteří se nacházeli v oblasti obsluhované tímto zařízením. Pro aktivní odposlech jsem využil znalostí z předchozího útoku, kde OpenBTS byla rozšířena o softwarovou pobočkovou ústřednu Asterisk, která obstarávala propojování hovorů. Prostřednictvím Asterisku se pak povedlo zaznamenat realizované odchozí hovory.

Při pasivním odposlechu jsem úspěšně v rámci laboratorních podmínek realizoval zachycení signalizačních zpráv a vlastních hovorových dat, které bylo možné následně přehrát ve formě audio záznamu. V případě dat získaných z reálného provozu se podařilo získat přístup k zabezpečené signalizaci, což umožnilo otevřený přístup k SMS zprávám. V případě hovoru se podařilo získat informace o volajícím či volaném, ale z důvodů vysoké náchylnosti na chybovost a nízkou kvalitou přijímače se vlastní audio záznam hovoru nepodařilo získat.

Na základě této práce byl podán článek na odbornou konferenci NAEC2014 v Itálii s názvem „Study of security issues in GSM network and their practical demonstration“. Tento článek byl následně komisí úspěšně přijat.

Na tuto práci je možno navázat v oblasti získání šifrovacího klíče na základě dat zachycených při pasivním odposlechu za využití předpočítaných tabulek tzv. Rainbow tables. Dále je možno se více věnovat zachytávání komunikace za využití mobilních telefonů s programovatelným firmware v rámci projektu OsomocomBB.

Použitá literatura

[1] KOKEŠOVÁ, Nikol. *Principy činností soudobých mobilních komunikačních sítí*. Brno, 2007. 67 l. Bakalářská práce. MU Brno, Fakulta informatiky. Vedoucí práce doc. Ing. Jan Staudek, CSc.

[2] RICHTR, Tomáš. *Technologie pro mobilní telekomunikaci* [online]. 2001, 19. 1. 2002 [cit. 2013-11-26]. Dostupné z: http://tomas.richtr.cz/mobil/

[3] REDL S., WEBER, M., OLIPHANT M. *GSM and Personal Communications Handbook*. Artech House, 1998, ISBN 978-0-89006-957-8.

[4] HARTE, Lawrence. *Introduction to global system for mobile communication (GSM): Physical channels, network, and operation*. Fuquay-Varina, NC: Althos, 2005. ISBN 19-328-1304-7.

[5] VAN DEN BROEK, Fabian. *Catching and Understarstanding GSM-Signals*. Nijmegen, 2010. Master thesis. Radboud University Nijmegen. Vedoucí práce Prof. dr. Bart Jacobs

[6] HEINE, Gunnar. *GSM networks: protocols, terminology, and implementation*. Boston: Artech House, 1998, xi, 416 s. ISBN 08-900-6471-7.

[7] GSM 04.03. *Digital cellular telecommunications system (Phase 2+): Mobile Station - Base Station System (MS - BSS) interface; Channel structures and access capabilities*. ver. 5.1.0. Valbonne: European Telecommunications Standards Institute, 1997 [cit. 2014-02-10]. Dostupné z: http://www.etsi.org/deliver/etsi_gts/04/0403/05.01.00_60/gsmts_0403v050100p.pdf

[8] GSM 04.07. *Digital cellular telecommunications system (Phase 2+): Mobile radio interface signalling layer 3*. ver. 5.1.0. Francie: European Telecommunications Standards Institute, 1996 [cit. 2014-02-10]. Dostupné z: http://www.etsi.org/deliver/etsi_gts/04/0407/05.01.00_60/gsmts_0407v050100p.pdf

[9] GSM 05.01. *Digital cellular telecommunications system (Phase 2+): Physical layer on the radio path; General description*. ver. 5.4.0. Valbonne: European Telecommunications Standards Institute, 1998 [cit. 2014-02-12]. Dostupné z: http://www.etsi.org/deliver/etsi_gts/05/0501/05.04.00_60/gsmts_0501v050400p.pdf

[10] GSM 05.02. *Digital cellular telecommunications system (Phase 2+): Multiplexing and multiple access on the radio path*. ver. 5.0.0. Valbonne: European Telecommunications Standards Institute, 1996 [cit. 2014-02-12]. Dostupné z: http://www.etsi.org/deliver/etsi_gts/05/0502/05.00.00_60/gsmts_0502v050000p.pdf

[11] Digital Modulation and GMSK: Appendix D. In: . *Electromagnetic Compatibility Aspects of Radio-based Mobile Telecommunications Systems: Final Report* [online]. Hull (Anglie): University of Hull, 1999 [cit. 2014-03-10]. Dostupné z: http://www.emc.york.ac.uk/reports/linkpcp/appD.pdf

[12] *LTE for UMTS - OFDMA and SC-FDMA based radio access*. 1st ed. Editor Harri Holma, Antti Toskala. Chichester: John Wiley, 2009, xxv, 433 s. ISBN 978-0-470-99401-6.

[13] GSM Security and Encryption. MARGRAVE, David. GEORGE MASON UNIVERSITY. *www.hackcanada.com* [online]. [cit. 2014-03-10]. Dostupné z: http://www.hackcanada.com/blackcrawl/cell/gsm/gsm-secur/gsm-secur.html

[14] SEDLÁŘ, Martin. *Time-memory tradeoff útoky v kryptografii*. MU Brno, 2012. Diplomová práce. Masarykova Univerzita. Vedoucí práce Jan Krhovják.

[15] GSM cloning. GOLDBERG, Ian a Marc BRICENO. ISAAC RESEARCH GROUP, SDA. *ISAAC: Internet Security, Applications, Authentication and Cryptography* [online]. 1998 [cit. 2013-03-10]. Dostupné z: http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html

[16] YOUSEF, Paul. *GSM-Security: a Survey and Evaluation of the Current Situation*. Linköping, 2004. LiTH-ISY-EX-3559-2004. Master's thesis. ISY, Linköping Institute of Technology. Vedoucí práce Viiveke Fåk.

[17] 26th Chaos Communication Congress: GSM: SRSLY?. *Chaos Communication Congress* [online]. 2009-12-27 [cit. 2014-03-18]. Dostupné z: http://events.ccc.de/congress/2009/Fahrplan/events/3654.en.html

[18] Speakers and Presentations: Defcon 18. *DEFCON* [online]. 2010 [cit. 2014-03-18]. Dostupné z: https://defcon.org/html/links/dc-archives/dc-18-archive.html#Paget2

[19] Decrypting GSM phone calls. *Security Research Labs* [online]. 2009 [cit. 2014-03-18]. Dostupné z: https://srlabs.de/decrypting_gsm/

[20] 27th Chaos Communication Congress: Wideband GSM Sniffing. *Chaos Communication Congress* [online]. 2010-12-28 [cit. 2014-03-22]. Dostupné z: http://events.ccc.de/congress/2010/Fahrplan/events/4208.en.html

[21] NIEMI, Valtteri a Kaisa NYBERG. *UMTS security*. Chichester: John Wiley, 2003, xii, 273 s. ISBN 04-708-4794-8.

[22] Ettus N200-210 DS. *USRP™ N200/N210 Networked series datasheet*. California: Ettus Research, 2012. Dostupné z: https://www.ettus.com/content/files/07495_Ettus_N200-210_DS_Flyer_HR_1.pdf

[23] OsmoSDR. *Osmocom* [online]. [cit. 2014-03-07]. Dostupné z: http://sdr.osmocom.org/trac/wiki/rtl-sdr

[24] BURGESS D., HARVIND S. *Open BTS Project.* Kestrel Signal Processing, California, 2008

[25] WIJA, Tomáš, David ZUKAL a Miroslav VOZŇÁK. *Asterisk a jeho použití: Technická zpráva*. In: CESNET. [online]. 30.10.2005 [cit. 2014-03-03]. Dostupné z: http://archiv.cesnet.cz/akce/20051115/pr/voz05_asterisk.pdf

[26] SONG, Yubo, Kan ZHOU a Xi CHEN. Fake BTS Attacks of GSM System on Software Radio Platform. *Journal of Networks* [online]. 2012-02-01, vol. 7, issue 2, s. - [cit. 2014-04-23]. DOI: 10.4304/jnw.7.2.275-281. Dostupné z: http://ojs.academypublisher.com/index.php/jnw/article/view/5666

[27] ITU-R M.1645. *Recommendation: Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000*. Geneva: ITU-R, 2003. Dostupné z: http://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.1645-0-200306-I!!PDF-E.pdf

Seznam příloh

Příloha na DVD

Obsah DVD:

	pro477_dp.pdf	Text diplomové práce
Pasivni		
	/openBTS	Pasivní odposlech s OpenBTS
	/realGSM	Pasivní odposlech v reálné síti
	/ostatní	Ostatní zachycená data
Aktivni		
	/konfigurace	Konfigurační soubory
	/log	Výsledky měření
	/terminal	Konzolové výstupy