Systém pro sledování 2/3/4G signálů

Daniel Janák

Bakalářská práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav informatiky a umělé inteligence

Akademický rok: 2023/2024

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Daniel Janák**
Osobní číslo:	**A20367**
Studijní program:	**B0613A140020 Softwarové inženýrství**
Forma studia:	**Prezenční**
Téma práce:	**Systém pro sledování 2/3/4G signálů**
Téma práce anglicky:	**System for Monitoring 2/3/4G Signals**

Zásady pro vypracování

1. Specifikujte možnosti zachytávání dat z 2/3/4G sítí mobilních operátorů pomocí softwarového rádia (SDR).
2. Popište, jaká data je možné pomocí SDR zachytit o základových stanicích (BSS) a klientech dané sítě.
3. Navrhněte přenosný systém pro základní sledování 2/3/4G signálů.
4. Proveďte sestavení prototypu navrženého systému.
5. Ověřte funkčnost navrženého řešení.

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

Seznam doporučené literatury:

[1] AWAD, Ali Ismail a Jemal H. ABAWAJY. Security and privacy in the Internet of things: architectures, techniques, and applications. Piscatway, NJ: IEEE Press, [2021], ISBN: 978-1-119-60774-8.
[2] DEY, Nilanjan a SANTHI, V. Intelligent techniques in signal processing for multimedia security. Studies in computational intelligence. Cham, Switzerland: Springer, [2016].
[3] MARSZALEK, Lukáš. Využití šifrování v telekomunikačních prostředcích. 2015.
[4] DABROWSKI, Adrian; PIANTA, Nicola; KLEPP, Thomas; MULAZZANI, Martin a WEIPPL, Edgar. IMSI-catch me if you can. Online. In: Proceedings of the 30th Annual Computer Security Applications Conference. New York, NY, USA: ACM, 2014, s. 246-255. ISBN 9781450330053.
[5] ALRASHEDE, Hamad a SHAIKH, Riaz Ahmed. IMSI Catcher Detection Method for Cellular Networks. Online. In: 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS). IEEE, 2019, s. 1-6. ISBN 978-1-7281--0108-8.

Vedoucí bakalářské práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **5. listopadu 2023**
Termín odevzdání bakalářské práce: **13. května 2024**

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
DĚKAN
L.S.

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

prof. Mgr. Roman Jašek, Ph.D., DBA v.r.
ředitel ústavu

Ve Zlíně dne 5. ledna 2024

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 13. května 2024

Daniel Janák, v.r.
podpis studenta

ABSTRAKT

Tato bakalářská práce se zaměřuje na rozbor a pochopení mobilních sítí druhé, třetí a čtvrté generace (2G, 3G, 4G), přičemž klade důraz na standardy těchto technologií a techniky pro jejich sledování. V teoretické části práce jsou popsány jednotlivé generace mobilních sítí s důrazem na jejich technické specifikace a evoluci. Dále je v práci věnována pozornost softwarově definovaným rádiím (SDR), které představují klíčový nástroj pro průzkum a analýzu signálů v současných i budoucích telekomunikačních sítích.

Praktická část práce demonstruje využití RTL-SDR k zachytávání a analýze 2G, 3G a 4G sítí. Provedené experimenty přibližují čtenáři znalost, jak lze efektivně monitorovat a analyzovat mobilní signály. Práce přináší ucelený pohled na aktuální stav a možnosti monitorování mobilních sítí a zdůrazňuje význam SDR pro budoucí vývoj v telekomunikacích.

Klíčová slova: 2G, 3G, 4G, softwarově definované rádio, mobilní sítě

ABSTRACT

This bachelor thesis focuses on the analysis and understanding of second, third and fourth generation mobile networks (2G, 3G, 4G), emphasizing the standards of these technologies and techniques for their monitoring. The theoretical part of the thesis describes each generation of mobile networks with an emphasis on their technical specifications and evolution. Furthermore, the thesis pays attention to Software Defined Radios (SDR), which represent a key tool for the exploration and analysis of signals in current and future telecommunication networks.

The practical part of the thesis demonstrates the use of RTL-SDR for capturing and analyzing 2G, 3G, and 4G networks. The experiments conducted provide readers with knowledge on how mobile signals can be effectively monitored and analyzed. The thesis offers a comprehensive view of the current state and possibilities of monitoring mobile networks and highlights the significance of SDR for future developments in telecomunications.

Keywords: 2G, 3G, 4G, software-defined radio, mobile networks

Rád bych zde poděkoval svému vedoucímu práce panu Ing. Davidu Malaníkovi PhD., za jeho odborný nadhled nad mojí prací a jeho schopností poskytovat mi podnětné nápady pro její další rozpracování.

Také bych chtěl poděkovat své mamce za její odborný a trpělivý dohled nad gramatickou částí mé práce. Také bych chtěl poděkovat všem mým známým, kteří mě při vypracovávání této bakalářské práce podporovali a věřili ve mě.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

V současné době se telekomunikační technologie rychle vyvíjejí a mobilita dat se stává stále důležitější. V této bakalářské práci se zabývám poskytnutím uceleného přehledu o standardech mobilních sítí 2G, 3G a 4G, jejich vývoji, technických specifikacích a metodách pro sledování těchto sítí.

Teoretická část práce systematicky popisuje každý z těchto mobilních standardů a také celulární sítě, na kterých tyto standardy operují. Poskytuje čtenáři vhled do základních principů fungování 2G, 3G a 4G sítí a také popis softwarové definovaných rádií (SDR), které hrají stále větší roli v moderních komunikačních technologiích. Na jejím konci jsou teoreticky popsány metody zachytávání signálů těchto sítí.

Praktická část práce se zaměřuje na využití RTL-SDR pro demonstraci a ověření popsaných metod sledování signálů v reálném prostředí za použití cenově dostupných periferií. Experimenty provedené v této části práce ukazují, jak lze moderní RTL-SDR využít pro zachytávání a analýzu signálů, což umožňuje hlubší pochopení teoretických konceptů. V závěrečné kapitole je návrh dalších možností pro další výzkum a testování v oblasti monitorování mobilních sítí.

I. TEORETICKÁ ČÁST

1 HISTORIE MOBILNÍCH SÍTÍ

V roce 1945 byl poprvé teoreticky popsán systém celulární rádiové sítě, který pracoval s myšlenkou znovupoužití stejné frekvence pro malé oblasti, což je hlavní element celulárních sítí. V roce 1947 pan D. H. Ring z Bellových laboratoří, s pomocí W. R. Younga formulovali reálný návrh skutečné celulární rádiové sítě. Pan Young později, řekl že všechny potřebné elementy pro celulární síť jsou nám již známé a dostupné. Tím zmiňoval mimo jiné například: síť malých geografických oblastí nazývaných buňky, základovou stanici umístěnou v každé z nich, software pro řízení přenosů, znovupoužití přenosových frekvencí pro buňky a další. Na konci šedesátých let minulého století již všechny majoritní telekomunikační společnosti věděli o celulárním systému, ale až v roce 1969 vznikl první celulární systém. Nacházel se na vlakové trati mezi New Yorkem a Washington DC. Šest frekvenčních kanálů se neustále opakovalo na 225 mil dlouhé trati. Celulární sítě, jejichž provoz zahrnoval komunikaci s mobilními zařízeními, byly spuštěny téměř současně, ale nezávisle na sobě, na konci sedmdesátých let v Japonsku a na Skandinávském poloostrově. [1]

V roce 1978 začala mezi Chicagem a New Jersey operovat celulární síť využívající nové technologie Advanced Mobile Phone Service (AMPS). V brzkých osmdesátých letech byly celulární systémy v rozkvětu a v Evropě vznikla síť NMT450, která se rozkládala na Skandinávském poloostrově. Síť byla složená ze 600-ti buněk a podporovala roaming. Byla to nejpokročilejší celulární síť na světě, a v návaznosti vznikly v Evropě další celulární systémy. TACS (Total Access Comunications System) ve Velké Británii, C-Netz v Německu, Radiocom 2000 ve Francii a Italský RTMI/RTMS. V ten moment se v Evropě nacházelo 9 vzájemně nekompatibilních analogových rádiových telefonních systémů. Z tohoto důvodu již v brzkých 80-tých letech začalo v Evropě plánování pro digitální, technologický posun k jedné společné síti pro celou Evropu. USA tento problém zatím neřešilo, kvůli jejich celostátně kompatibilnímu AMPS systému, navíc dosavadní telefonní zařízení by nebyla kompatibilní s novými digitálními sítěmi, což by znamenalo pro mobilní společnosti značně nevýhodný marketingový tah. [1]

2 STANDARDY MODERNÍCH MOBILNÍCH TELEFONÍCH SÍTÍ

Evropské společnosti si zisk z nového digitálního směru uvědomovaly a i za cenu zpětné nekompatibility stávajících mobilních zařízení byly ochotny tento krok kupředu provést. V roce 1982 začalo 26 Evropských společností na vývoji GSM (Groupe Speciale Mobile). Toto byla globální ukázka toho, čeho byla Evropská soudržnost schopna na celesvětové obchodní škále. Zároveň to byl jeden z největších prvních světový kroků směrem k 2G sítím. [1]

2.1 2G

Druhá generace mobilních sítích byla v rozvoji od 80-tých do konce 90-tých let minulého století. Hlavní rozdíl oproti první generaci byl v používání digitálních telekomunikačních kanálů oproti analogovým. 2G sítě ze začátku nabízely přenosové rychlosti až 64kbps a šířku přenosového pásma 30-200kHz. Stejně jako 1G sítě, hlavním záměrem byl stále přenos hlasu, který byl stále kvalitnější, ale 2G sítě již umožňovaly další služby jako třeba pagery, sms zprávy, hlasové schránky a se stále dalším vývojem později přinesly i internetové služby. [2]

2.1.1 GSM

Zkratka GSM pro Groupe Speciale Mobile, vznikla podle výzkumné skupiny, která tento standard vytvořila. Nyní známý jako Global System for Mobile Communications přinesl světu spoustu vylepšení oproti minulým generacím mobilní telekomunikace a používá se aktivně dodnes. Komerční GSM síť se v Evropě začala používat v roce 1991 a okamžitý kapacitní nárůst oproti analogu byl až trojnásobný. Nové technologie, které GSM přineslo byly SMS (Short Messaging Services) a Subscriber Identity Module (SIM) karty pro ukládání kontaktů do mobilních zařízení. V roce 2004 bylo oznámeno, že síť GSM má již 1 miliardu zákazníků. Do USA se GSM dostalo poprvé v roce 1995 a během pouhých šesti měsíců již bylo GSM sítí v USA 15. [1]

GSM síť je primárně složena ze tří částí. To jsou Network and Switching Subsystem (NNS), Basic Station Subsystem (BSS) a Operation Support Subsystem (OSS). Mobile-Services Switching Center (MSC) je jádrem NNS, který slouží pro routování a přepojování požadavků v síti. BSS se skládá z Basic System Controller (BSC), Basic Transceiver System (BTS) a Mobile System (MS). OSS se stará o chod a monitorování celého GSM systému. Skládá se z Maintenance Centre (OMC) a System Software. [3]

GSM Systém po celém světě primárně operuje na dvou frekvenčních pásmech 900MHz a 1800MHz. Systém používá Frequency Division Duplex (FDD) a Time Division Multiple Access (TDMA) pro modulaci a přenos komunikačních signálů. Příchozí kanál je rozdělen na 128 kanálů, každý s šířkou pásma 200KHz. Mezi další kapacitní vymoženosti tohoto systému se řadí také to, že každý kanál může sdílet až osm uživatelů zároveň. [3]

2.1.2 2.5G/2.75G

General Packet Radio Services (GPRS) a také Enhanced Data rates for Global Evolution (EDGE) byly obě dvě velmi důležité kroky ve vývoji technologií pro přenos dat skrze celulární sítě. GPRS se nazývá 2.5 generací, protože přineslo technologii přepojování paketů. Technologie jako Serving GPRS a Gateway GPRS spolu s IP routers, firewall servers a DNS byly součástí takzvané „packet core network“. Všechny tyto kroky dohromady umožňovaly přístup k Internetu a přenosovou rychlost až 150kbps v optimálních podmínkách. [2]

EDGE technologie byla dalším krokem rapidně se rozvíjejích GSM sítí po celém světě. EDGE je tak řečeno nadstavená GPRS technologie, která používá efektivnější kódovací metody a umožňující přenos dat rychlostí až 384kbps. EDGE technologie byla dostupná na jakékoliv již funkční GPRS síti jakmile došlo k upgradu a díky svým možnostem poskytovala až čtyřnásobnou přenosovou kapacitu sítě oproti standartnímu GPRS. [2]

Generations	2G	2.5	2.75
Starts from	1990	2000	2003
Frequency	850-1900 MHz(GSM) 825-849MHz(CDMA)	850-1900 MHz	850-1900 MHz
Data capacity	10KBPS	200 KBPS	473 KBPS
Technology	Digital wireless	GPRS	EDGE
Standard	CDMA TDMA GSM	Supported TDMA/ GSM	GSM CDMA
Multiplexing	TDMA CDMA	TDMA CDMA	TDMA CDMA
switching	Circuit Packet	Packet	Packet
Service	Voice data	MMS internet	
Main network	PSTN	GSM TDMA	WCDMA
Hand off	Horizontal		

Tabulka 1 Tabulka parametrů 2/2.5/2.75G [4]

V tabulce lze přehledně vidět základní parametry a rozdíly mezi jednotlivými mezigeneračními skoky.

2.1.3 Ostatní 2G sítě

USA bylo na mezích kapacity jejich dosavadního AMPS analogového systému a kolem roku 1991 bylo rozhodnuto, že následující vývoj se bude ubírat digitálním směrem. USA ale chtělo digitální systém, který by udržel stávající mobilní zařízení v provozu, toho dosáhlo technologií TDMA. Jejich nový standard se nazýval IS-54, neoficiálně nazývaný Digital AMPS (D-AMPS). Stejně jako USA, další státy také začaly využívat technologii TDMA pro jejich celulární systémy, například Japonsko 1994 s jejich systémem Personal Digital Cellular (PDC). Kvůli neustále zvyšujícímu se počtu zákazníků mobilních sítí s nárůstem cca 200% za rok USA v roce 1993 opět docházela kapacita jejich D-AMPS systému. To byl také rok, kdy došlo k přechodu na technologii Code Division Multiple Access (CDMA) a systém nazývaný IS-95. O něco později vznikl standard IS-95A, který se nazýval cdmaOne. [1]

Po průniku GSM a dalších systémů do USA v letech 1994-1997 nastoupil na scénu v USA další standard IS rodiny. Byl to IS-136, který opět používal TDMA technologii a byl to nástupce předchozího IS-54. V roce 1995 spustili v Japonsku chytrý systém umožňující používat jedno zařízení jak v pohodlí domova, tak při cestování městem. Byl to systém na CDMA/IS-95 standardu a rozpoutal tak příští desetiletou nadvládu CDMA. [1]

2.1.4 Zabezpečení 2G sítí

Již od vzniku GSM standardu byla jeho bezpečnost neustále se opakujícím tématem. Většina rizik a problémů vznikala při end-to-end komunikaci užitelů, kteří používali SIM a Mobile equipment (ME), což je vlastně tak řečeno "mobilní zařízení". Vzhledem k obrovskému počtu uživatelů 2G sítí a značným množstvím datových přenosů skrze ně, jsou 2G sítě cílem pro potencionální útočníky. Systém byl vyvinut tak, aby poskytoval ochranu před odposloucháváním a ochraně identity zařízení, stejně jako tomu bylo u analogových přenosů. Takovéto ochrany lze dosáhnout ochranou jak mobilní sítě samotné, tak ochranou mobilního zařízení uživatele. [5]

2.1.4.1 Zabezpeční mobilní sítě

Před zahájením hovoru nebo před zahájením přenosu dat proběhne mezi mobilním zařízením (Mobile Station) a mobilní sítí množství autentizačních signálů. Proces začíná tím, že MS zašle svoje International Mobile Subscriber Identity (IMSI) základové stanici (BS). Ta je potom zaslána do subsystému Home Location Register (HLR). IMSI, které MS odešle do HLR, je namapováno ke korespondujícímu klíči K. S klíčem je poté provedena šifrovací operace pomocí hashovacího algoritmu A8 s parametry náhodné výzvy RAND a daného klíče K. Výsledek této operace je zaslán zpět na BS. [5]

2.1.4.2 Zabezpečení mobilního zařízení

Na mobilním zařízení je provedena šifrovací operace pomocí algoritmu A3 s přijatou RAND výzvou a klíčem K, která vytvoří očekávaný výsledek (XRES). Tento výsledek je poté zaslán zpět na BS, kde pokud se výsledky shodují, proběhne autentizace. Poté je algoritmem A8 SIM kartou vygenerován šifrovací klíč K_C, který slouží jako klíč pro šifrování užitelské komunikace pomocí algoritmu A5. [5]

2.1.4.3 Typy útoků na 2G sítě

Existuje spoustu způsobů, jak by se mohl potencionální útočník pokoušet získávat data z mobilních sítí. Pro názornost zde popíšu některé typů útoků, které byly a nebo by potencionálně mohly být provedeny na GSM sítě. [5]

Eavesdropping/Odposlouchávání

Při této technice útočník využívá zařízení pro zachytávání a naslouchání signálům cestujícím vzduchem kolem něj. Může poté získat přístup k signálům a datům, které zachytí. Této technice budeme nejblíže s pomocí našeho SDR. [5]

Impersonation of a User/Vydávání se za uživatele

Při tomto útoku používá útočník modifikované mobilní zařízení. Zasílá pomocí něho do sítě uživatelská data a snaží se při tom vypadat jako ten původní uživatel, na kterého útokem cílí. [5]

Impersonation of the Network/Vydávání se za síť

Při tomto útoku používá útočník upravené zařízení podobající se základové stanici. Cílem je zasílání signálů a dat cílenému uživateli, pokoušejíc se přimět užitele důvěrovat této falešné BS jako kdyby pocházela ze sítě. [5]

Man-in-the-middle/Prostředník

Toto je schopnost, kdy se útočník zvládne dostat mezi komunikaci uživatele a sítě. Získá tak možnosti odposlouchávat, modifikovat, mazat i měnit data zasílaná mezi těmito dvěma stranami. Zařízení k tomu potřebná jsou modifikovaná BS a modifikovaná MS. [5]

2.2 3G

V roce 2001 byla v japonsku spuštěna první 3G síť. Cílem 3G sítí bylo poskytnout kvalitnější mobilní služby než předchozí generace a také Internetové připojení. 3G sítě musely dodržet standard International Mobile Telecommunications-2000 (IMT-2000). Tento standard specifikoval mimo jiné i dodržení minimální přenosové rychlosti 200Kbit/s. Tohoto zrychlení se dosahovalo zdokonalováním a propojováním stávajících bezdrátových principů a technologií jako TDMA, CDMA a GSM. Používané módy přenosu dat byly Wideband CDMA (W-CDMA), CDMA2000 a Wi-Max, které byly všechny kompatibilní se standardy předchozí generace. [2; 6]

Sítě 3G se skládají z core network a Radio Access Network (RAN). Hlavní činností core network pro 3G sítě bylo využívání technologie packetů GPRS pro přenos dat a přepínání hlasových hovorů. RAN v 3G sítích sloužil pro nezavislý přístup mobilních zařízení a síťových terminálů. RAN obsahoval RAN controller, který fungoval na stejném principu jako BSC uvnitř 2G sítí. [6]

2.2.1 3.5G/3.75G

Klíčovou technologií, kterou se vyznačovaly 3G sítě byla technologie W-CDMA vyvinutá GSM komunitou pro použití právě na 3G sítích. W-CDMA byla využívána pro přenos dat skrze malé satelity a využívala technologie high-speed packet access (HSPA), jež se skládá z high-speed downlink packet access (HSDPA) a high-speed uplink packet access (HSUPA). HSDPA technologie označovaná jako 3.5G je packetová služba umožňující downlink přenosové rychlosti až 20Mbit/s. Spolu s ní je přímo propojená technologie HSUPA označovaná jako 3.75G, která svými uplink možnostmi pozvedávala 3G sítě tak, že bylo možné používat již mobilní internet v rychlostech až 5.8Mbps. [4; 6]

Generations	**3G**	**3.5**	**3.75**
Starts from	2001	2003	2003
Frequency	1.6-2.5GHz	1.6-2.5GHz	1.6-2.5GHz
Data capacity	384Kbps	2Mbps	30Mbps
Technology	Broad band /IP technology FDD TDD	GSM/ 3GPP	
Standard	CDMA/WCDMA/ UMTS/CDMA2000	HSDPA/HSUPA	1xEVDO
Multiplexing	CDMA	CDMA	CDMA
switching	Circuit ,packet	packet	packet
Service	High speed voice/data/video	High speed voice/data/video	High speed internet/multimedia
Main network	Packet network	GSM TDMA	
Hand off	Horizontal	Horizontal	Horizontal

Tabulka 2 parametry 3/3.5/3.75G [4]

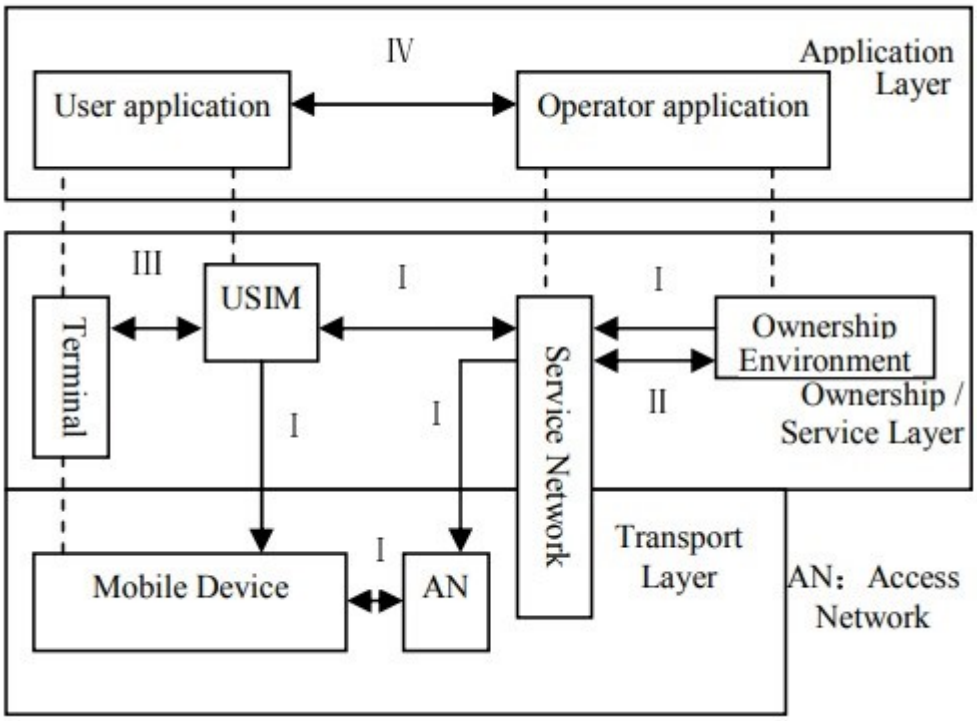
V tabulce lze vidět rozdíly mezi mezigeneračními postupy. Nejjasněji jde lze vidět rozdíl v používaných standardech pro přenos dat a v jejich přenosových rychlostech.

2.2.2 Zabezpečení 3G sítí

Kromě nových služeb a servisů, které jsou hlavním jádrem třetí generace mobilních zařízení, přinesla tato generace také spoustu nových rizik a ohrožení v oblasti zabezpečení těchto sítí a služeb, stejně jako mobilních zařízení. [7]

Značným rizikem, kterému čelila tato generace při jeho nástupu byl rapidní vývoj mobilních zařízení a jejich možností. Přínos mobility, roamingu, malé velikosti a jednoduchého ovládání s sebou přineslo také rizika. Mobilní zařízení se dalo lehce ztratit, jeho operační systém byl náchylnější proti útokům než například PC operační systém. Nedostatečné softwarové updaty nebo úplné vynechání antivirů v zařízení vedlo k náchylnosti proti útokům virů. [7]

3G systémy byly vyvinuty s logickou bezpečnostní infrastrukturou, která implementovala bezpečnostní prvky a mechanismy pro ochranu těchto sítí. [7]



Obrázek 1 Digram bezpečnostních vrstev 3G sítí [7]

Na diagramu můžeme vidět rozdělené vrsty infrastruktury 3G systémů. Nachází se zde transportní vrstva, servisní vrstva a aplikační vrstva. Římské číslice znázorňují jaký typ zabezpečení je zde použit při přenosu. [7]

- I (zabezpečený síťový přístup) Zde se nachází zabezpečení a ochrana proti přístupu do bezdrátové části sítě, což je nejnáchylnější část sítě k útokům. Některé bezpečnostní kroky, které se zde provádí jsou: ověřování uživatelské identity, ověřování užitelské lokace, zabezpečený přenos šifrovacího klíče, zašifrování přenášených dat a další. [7]
- II (zabezpečení síťové domény) Hlavní činnost této ochrané vrsty je zabezpečení přenosů signálů uvnitř core network a ochrana proti útokům na kabelovou část sítě. [7]
- III (zabezpeční uživatelské domény) Stará se o bezpečnost mobilních zařízení. Jedná se o ověřování identity mezi uživatelem a jeho čipovou kartou, dále také ověřování komunikace čipové karty s terminálem (mobilní zařízení/smartphone). Jedná se o ochranu uživatelských dat v rámci mobilního zařízení a jeho nejužší komunikace v rámci terminálu. [7]
- IV (zabezpečení aplikační domény) Tato vrstva ochrany zajišťuje bezpečný průchod dat mezi uživatelskou doménou (mobilní zařízení) a poskytovatelem služeb. To zajišťují postupy jako autentizace aplikace, detekce a prověřování aplikačních dat, ochrana aplikačních dat a další. [7]

2.3 4G

Hlavními cíly technologie 4G bylo dosažení vysokokapacitních přenosů dat pro rychle se pohybující uživatele, plynulé přepojování mezi základovými stanicemi bez prodlevy a další Quality of Service (QoS), což byly například propustnost sítě a její flexibilita. Cílem 4G bylo také integrování již vyvinutých technologií (GSM, GPRS, Wi-Fi, Bluetooth a další) na jejich společné a souvislé využívání na jednotné úrovni, kterou přinášela 4G. Na 4G bylo referováno slovem „MAGIC“, která znamenala **M**obile multimedia, **A**nywhere, **G**lobal mobility solutions over, **I**ntegrated wireless and **C**ustomized services. [4; 8]

Dvě beztrátové sítě, které dohromady tvoří 4G jsou Worldwide Interoperability for Microwave Access (WiMAX) a Long Term Evolution (LTE) standardizované organizací Third Generation Partnership Project (3GPP). WiMAX bylo ve vývoji již od roku 1999 a jeho 4G standard se na trh dostal v roce 2012. LTE bylo poprvé představeno v roce 2004 a v roce 2011 byla vydána verze LTE-Advanced, která byla považována za 4G standard.

WiMAX měl sloužit jako alternativa k LTE, ale nenabyl takové popularity. Proto je hlavním nosičem 4G služeb hlavně LTE standard. [8]

Technologie používané ve 4G sítích jsou Orthogonal Frequency Division Multiple Access (OFDMA) a Multiple Inputs and Multiple outputs (MIMO). OFDMA umožňuje efektivní sdílení přenosového kanálu mezi více uživateli. MIMO umožňuje přenášet data z více antén současně, lze tak přenášet více datových proudů a pomocí multiplexu se šetří čas a zvyšuje přenosová rychlost. [6; 8]

Generations	4G
Starts from	2010
Frequency	2-8GHz
Data capacity	200Mbps-to- 1Gbps
Technology	LTE, Wi MAX
Standard	IP-broadband LAN/WAN/PAN
Multiplexing	MC-CDMA, OFAM
switching	Packet
Main network	Internet
Hand off	Horizontal &Vertical

Tabulka 3 parametry 4G [4]

2.3.1 Zabezpečení 4G sítí

LTE bylo navrhováno se silným důrazem na kryptografické techniky a vzájemnou autentifikací mezi prvky sítě. S nástupem plně na IP založené architektury s sebou LTE přineslo spoustu bezpečnostních rizik, které mohou potencionálně využít útočníci pro útok na 4G sítě a její uživatele. Některé útoky mohou být spam s potencionálně škodlivým obsahem, odposlouchávání, šíření malwaru, odposlouchávání IP adresy, krádež dat nebo také DdoS útoky a další. [9]

Pro ochranu před těmito a ostatními druhy útoků se organizace 3GPP již od začátku vývoje soustředila na pět bezpečnostních principů pro ochranu 4G sítí. Tyto principy jsou velmi podobné jako u 3G sítí. [9]

1. Zabezpečený přístup do sítě, poskytuje zabezpečený přístup uživateli k servisům poskytovaným 4G sítí [9]
2. Zabezpečení síťové domény, chránící síťové prvky a přenos signálů mezi uživateli a těmito prvky [9]

3. Zabezpečení uživatelské domény, poskytuje ochranu při přístupu k mobilnímu zařízení [9]
4. Zabezpeční aplikační domény, zajišťuje bezpečnou komunikaci skrze aplikační vrstu sítě [9]
5. Viditelnost a přístupnost k bezpečnostním prvkům poskytuje uživateli možnost zkontrolovat a ujistit se, zda jsou všechny bezpečnostní funkce v provozu [9]

2.4 5G

Pátá generace mobilních sítí, známá jako 5G, představuje zásadní krok vpřed v evoluci bezdrátových komunikačních technologií. Po 2G, 3G a 4G, které zásadně změnily způsob, jakým lidé komunikují a interagují s digitálním světem, 5G slibuje ještě rychlejší přenos dat, nižší latenci a větší spolehlivost. To otevírá dveře pro nové aplikace a služby, včetně pokročilých Internet of Things (IoT) řešení, autonomních vozidel a zcela nových způsobů mobilní komunikace. [6; 8]

5G síť je stavěna na zcela nové architektuře, která integruje technologie jako Masivní MIMO, beamforming a nové metody přístupu k rádiovému spektru. Tyto technologie umožňují efektivnější využití dostupného frekvenčního spektra a zvyšují hustotu přenosu dat, což je klíčové pro zvládnutí rostoucího počtu připojených zařízení a aplikaci vyžadujících vysokou šířku pásma. [6; 8]

Hlavní výhodou 5G sítí je její schopnost poskytovat velmi vysoké rychlosti datového přenosu. Oproti 4G sítím by se mohlo jednat až o stonásobné rychlosti. To umožňuje rychlejší stahování a streamování obsahu ve vysokém rozlišení, a také podstatně zlepší zážitek z online mobilních her a virtuální reality. Kromě toho by nízká latence 5G mohla také pomoct s využitím aplikací jako například řízení průmyslových strojů nebo jiné operace prováděné na dálku. [6; 8]

Přechod na nové generace s sebou vždy přináší také řadu výzev a bezpečnostních rizik. Nasazení nových antén a technologií je náročná záležitost, která vyžaduje velké přípravy a kontroly. Bezpečnost 5G sítí bude také velmi důležitým tématem. Kvůli zvýšeným přenosovým rychlostem a většímu počtu uživatelů vznikají nové potencionální prostory pro různé kybernetické hrozby. [6; 8]

Standard	4G	5G
Start Form	2010	2016
Data Rate	2 Mbps – 1Gbps	1Gbps and higher
Frequency Domain	2 – 8 GHz	3 – 300 GHz
Handover	Horizontal and Vertical	Horizontal and Vertical
Core network	All IP network	Flatter IP network, 5G network interfacing (5G-NI)
Multiple Access	CDMA	CDMA, BDMA

Tabulka 4 Tabulka porovnávající 4G a 5G [8]

3 CELULÁRNÍ RÁDIOVÁ SÍŤ

Celulární mobilní síťě jsou založeny na standardech a normách organizace 3GPP a spolu s GSM Association byly vytvořeny všechny aspekty a parametry pro mobilní sítě. To jsou například: rádiové rozhraní, operace na vyšších vrstvách architektury, mobilita sítě, mobilní bankovnictví, poskytované servisy, roaming a mnoho dalšího. [10]

3.1 GSM

Mobilní síť GSM se skládá ze dvou hlavních částí. Těmi jsou fyzická infrastruktura sítě a mobilní zařízení, která s touto sítí komunikují. Fyzickou infrastrukturu lze rozdělit na 3 podsítě a těmi jsou: Base Station Subsystem (BSS), Switching and Management Subsystem (SMSS) a Operation and Management Subsystems (OMSS). [11]

3.1.1 Radio Network – Base Station Subsystem (BSS)

Rádiová síť se skládá z Base Station Controller (BSC) a Base Transceiver Station/Base Station (BTS/BS). Tato BS bývá zpravidla umístěna uprostřed buňky. BS se skládá z vysokofrekvenčních přijímačů a vysílačů, kterých může být až 16 a každý z nich reprezentuje vlastní frekvenční kanál pro komunikaci. BS dále obsahuje komponenty pro zpracování protokolů a signálu. Hlavní úkoly BSC jsou přidělování frekvencí pro komunikaci a kontrola a správa přidružených BS. Hardware BSC může být umístěn na tom samém místě jako BS, strategicky umístěn samostatně, a nebo se může nacházet v MSC. [11]

3.1.2 Mobile Switching Network

Mobile switching subsystem (MSS) je složen z MSC a databází. MSC se v mobilní síti nazývá jako přepojovací uzel, protože provádí veškeré routovací funkce v síti jako jsou hledání routovací cesty a vedení signálu samotného. V databázích jsou uloženy všechny nutné informace pro routování a poskytování služeb. Veřejná mobilní síť může obsahovat více takovýchto MSC a každá z nich je zodpovědná za určitou oblast v síti. Množství BSC může být v base subsystému pod správou jediného MSC. [11]

3.1.2.1 Home and Visitor Location Registers

MSS obsahuje 2 funkční jednotky Home Location Register (HLR) a Visitor Location Register (VLR). Tyto dvě databáze slouží k synchronizaci registrovaných uživatelů s jejich aktuální polohou. Obecně bývá jeden HLR na jednu Public Land Mobile Network

(PLMN), což je vlastně jedna geograficky ohraničená oblast a podobně bývá jedna VLR pro jedno MSC. [11]

HLR ukládá uživatelská a identifikační data, jako jsou například IMSI, telefonní číslo, autentifikační klíč, seznam povolených servisů pro uživatele a dočasná data. Dočasná data mohou obsahovat adresu současného VLR, telefonní číslo, na které mají být převedeny hovory a další. [11]

VLR ukládá data o všech mobilních zařízeních, která se nachází v administrativní oblasti náležícího MSC. Mobilní zařízení jsou samozřejmě volně se přemisťující, takže mohou být zaregistrována buďto ve své domovské síti a nebo v cizí síti. [11]

3.2 UMTS

Celulární sítě třetí generace byly vyvinuty se zájmem přinést odběratelům vyšší přenosové rychlosti dat a zpřístupnění multimediálních služeb skrze mobilní sítě. [11]

Síť UMTS se skládá ze tří částí, to jsou: Core Network (CN), UMTS Terrestrial Radio Access Network (UTRAN) a User Equipment (UE). UE je složen z mobilního zařízení a Universal SIM karty (USIM). USIM karta drží více informací o uživateli a také poskytuje více autentifikačních a bezpečnostních procesů při komunikaci v síti. Zařízení může komunikovat buďto v módu spínání okruhů (Circuit Switched - CS), přepínání paketů (Packet Switched) a nebo kombinovaně. Každý mód připojení pracuje s jinou částí sítě a poskytuje tak jiné služby uživateli. [11]

Komponenty RAN jsou podobné jako u GSM sítí, pouze s vylepšeními a změnami. Jsou to Base Stations (BS) nebo také Node B, Radio Network Controllers (RNCs). BS v sítích odpovídá za kódování fyzického kanálu, modulaci/demodulaci, přenos dat skrze vzduchové rozhraní, opravu errorů a další. RNC odpovídá za kontrolu a přidělování zdrojů, přidělování komunikačních kanálů, kontrola přístupu, šifrování a další. [11]

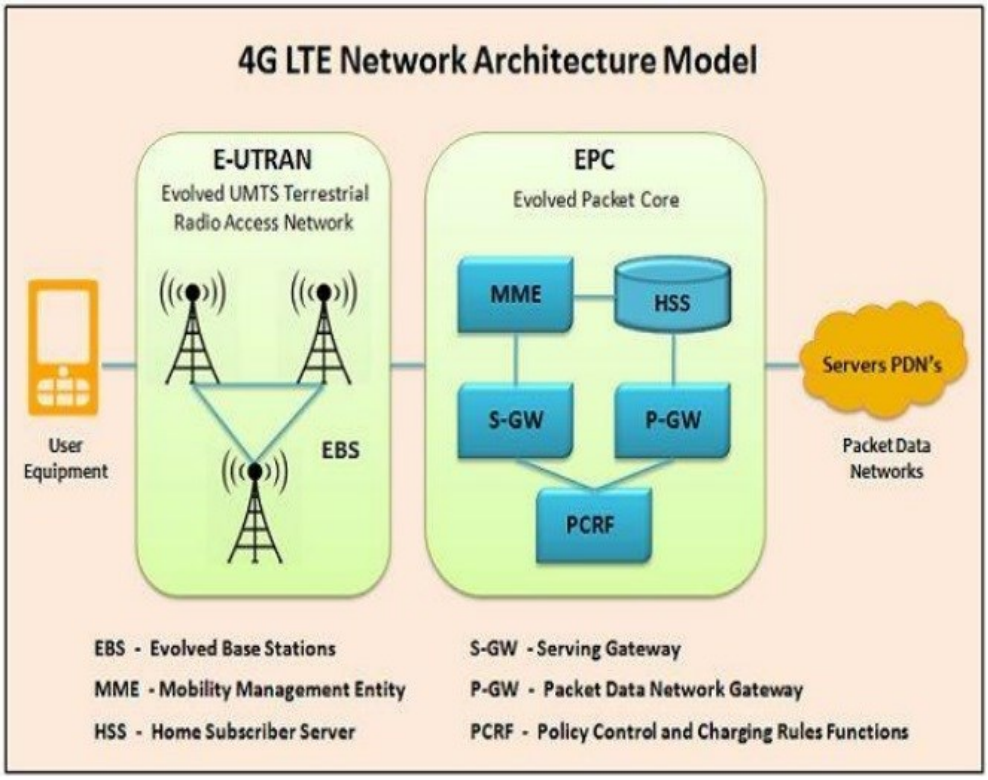
Hlavní funce CN jsou přepojování, routování a poskytování fyzického média pro přenos dat mezi uživateli. CN také obstarává síťovou správu a databáze k tomu potřebné. UMTS architektura je postavená na GSM síti s prvky GPRS, ale veškeré vybavení musí být upgradováno pro podmínky použití pro UMTS standardy. CN také obsahuje databáze HLR a VLR jak jsem popsal v části GSM. [11]

3.3 LTE

Nástup čtvrté technologie se snažil sjednotit rozpolcený trh zaplněný různými spolu nespolupracujícími technologiemi z druhé a třetí generace. Je postavený na plně IP založené architektuře a přináší spoustu navýšení v přenosových rychlostech a menšímu zpoždění. LTE je založený na množství moderních a složitých technologií, které jsou postavené na původních 3G sítích. [12]

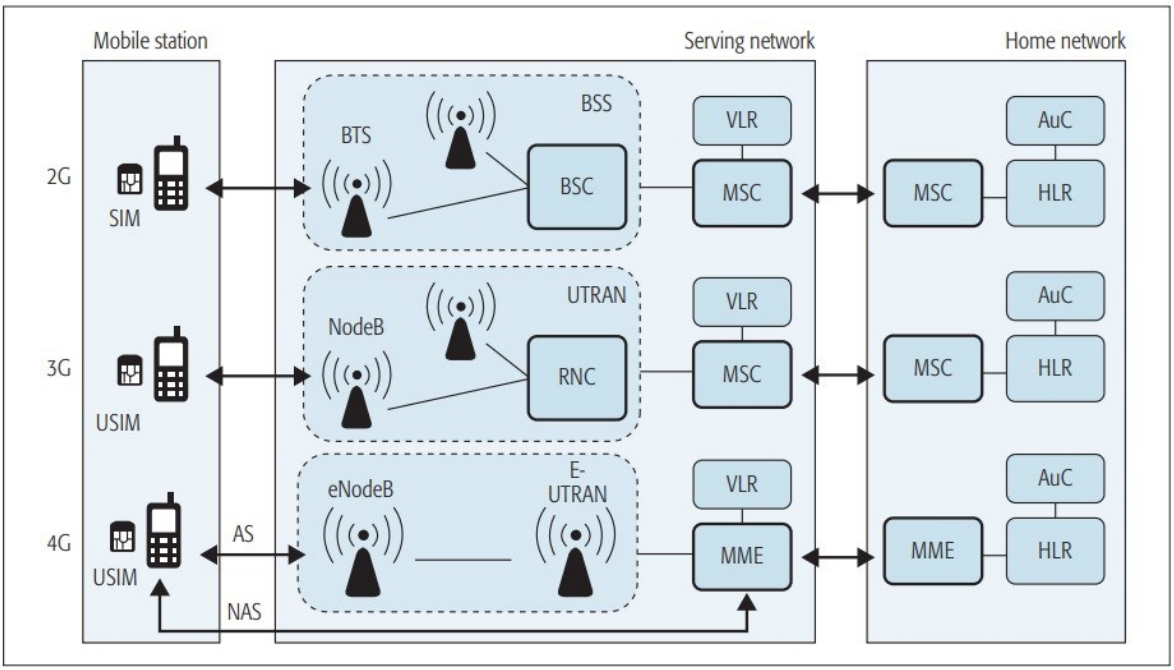
LTE celulární systém je složený z tísíců buněk, která každá vysílá na stejné rádiové frekvenci a používá OFDMA pro downlink a Single Carrier Frequency Division Multiple Access (SC-FDMA) pro uplink. SC-FDMA je náhrada W-CDMA u 3G sítí. [12]

LTE síť je složená z UE (který je zpětně kompatibilní), nejedná se o náhradu zařízení za nová. Dále rádiová část sítě Evolved – UTRAN (EUTRAN) a Evolved Packet Core (EPC). EUTRAN je zjednodušený 2G BSS systém a 3G UTRAN, integrovaný do jedné sítě používající eNodeB základové stanice s použitím optických vláken k jejich propojení používající IP protokoly. EPC používá plně na IP založené protokoly, což této architektuře dává technický náskok oproti minulým generacím. Přináší nižší zpoždění celé sítě, ale hlavně také umožňuje propojení již funkčních sítí jako jsou eNode BS, sítě různých mobilních operátorů, pevných linek a ta nejdůležitější Internetu. [12]



Obrázek 2 Digram 4G LTE architektury sítě [12]

Na digramu vidíme, že hlavní důraz je zde věnován části EPC, která tvoří průchody pro komunikaci všech spolupracujících sítí dohromady. Děje se tak díky propojovacím "gateways" mezi sítí LTE a ostatními sítěmi.



Obrázek 3 Přehledný diagram celulárních sítí 2G/3G/4G sítí [13]

Na digramu sítí vidíme postupné vývoje technologií mezi generacemi. Místo klasické SIM karty je u 3G a 4G sítí používaná USIM. Při GSM používané BSS bylo vyvinuto na UTRAN a později ještě na E-UTRAN. Posledním na diagramu významným rozdílem byla správní složka komunikace v síti. Oproti MSC uvnitř 2G a 3G sítí používají 4G sítě Mobile Management Entity (MME). [13]

4 SDR

4.1 Co to je Softwarově definované rádio (SDR)

Software Defined Radio (SDR) nemá žádnou globálně uznávanou definici. Někdy také nazýváno Software Based Radio, Reconfigurable Radio či Flexible Architecture Radio. Je to zařízení, které může přijímat a zpracovávat různé rádiové vlny o určité vlnové délce, frekvenci nebo modulaci pouhou změnou softwarového nastavení, bez žádné změny hardwaru nebo změnou platformy na které SDR operuje. Pomocí komplexních operací je SDR schopno tyto přijaté rádiové vlny převést zpět do formátu informace pro člověka čitelné. Software SDR se může nacházet na PC, ale v dnešní době i na mobilním zařízení nebo jiném tomu uzpůsobeném hardwaru. Ideální SDR by bylo schopné přijímat jakoukoliv frekvenci, šířku pásma, modulaci i datovou rychlost. [14; 15]

4.2 K čemu slouží SDR

SDR bylo ve vývoji již od sedmdesátých let dvacátého století a po mnoho let se investuje do jeho používání například ve vojenském sektoru, kde je po zařízeních požadováno delší funkční období než v komerčním sektoru. Komerční sektor také využívá stále více schopností SDR řešení, například logika SDR je používána jako ovládací software pro základové stanice. Hlavní motivací pro používání SDR je jeho jednoduchost používání a nízká cena případné výměny nebo vylepšení používaného softwaru oproti výměně celého HW zařízení. Další příklady použití SDR mohou být v oblasti bezpečnosti mobilních dat, kde jej profesionálové používají pro monitorování a kontrolování sítí. [14; 15]

Software Communications Architecture (SCA) představuje klíčový milník ve snaze o standardizaci v oblasti SDR. Tento architektura je zásadní pro zajištění kompatibility a interoperability mezi různými SDR systémy. SCA definuje sadu standardizovaných rozhraní a komponent, což umožňuje vývojářům tvořit software, jež lze snadno přenášet mezi různými platformami. SCA také podporuje širší kompatibilitu mezi zařízeními od různých výrobců, což je zásadní pro vytváření robustních a flexibilních komunikačních systémů. [14]

4.3 Modely SDR zařízení na trhu

Spoustu společností se rozhodlo začít vyrábět SDR a ceny jednotlivých SDR se liší hlavně jejich vlastnostmi. Některá populární SDR jsou RTL-SDR, HackRF a BladeRF. RTL-SDR

je jedna z nejlevnějších a nejvíce rozšířených možností na trhu. Tato SDR běžně operují v rozsahu 24MHz-1766MHz a mohou pracovat pouze jako přijímače. HackRF je používaný profesionály pro monitorování mobilních sítí za účelem ochrany osob, sledování osob a mnoho dalšího. HackRF pracuje v rozsahu 30MHz-6000Mhz, BladeRF pracuje s rozsahem 300MHz-3800MHz. [15]

4.4 Typy SDR zařízení

SDR založené na General Purpose Processor (GPP) jsou SDR zařízení využívající obecné mikroprocesory, které jsou běžně využívány například v osobních počítačích. Jejich výhodou je jejich univerzálnost a široká dostupnost, proto jsou ideálním řešením pro vývoj a testování nových komunikačních protokolů a technologiím. Mohou bežet na standardním operačním systému a využívat běžné programovací jazyky jako například C++ nebo Python. Hlavní nevýhodou je ale omezený výkon a efektivita oproti více specializovaným typů SDR jako jsou DSP a FPGA. [16]

SDR založené na Digital Signal Processor (DSP) jsou optimalizované pro operace zpracování signálu, jako je filtrace, kódování a modulace. Jsou velmi efektivní pro úlohy vyžadující vysoký výpočetní výkon v reálném čase, což má využití v oblastech vojenství a bezpečnostních aplikacích. Tyto systémy bývají často dražší než GPP kvůli jejich specializovanému hardwaru a větší náročnosti na programování. [16]

SDR založené na Field-Programmable Gate Array (FPGA) poskytují vysokou úroveň flexibility a přizpůsobení, protože umožňují přeprogramování a rekonfiguraci hardwarové logiky po jejich vyrobení. To může být obzvlášť užitečné pro vývoj komplexních rádiových systémů, které mohou vyžadovat pravidelné úpravy pro optimalizaci výkonu nebo přidání nových funkcí. FPGA-based SDR jsou schopna dosahovat vysokého výkonu při nízkém zpoždění, což je dělá ideálními kandidáty pro využití vy aplikacích jako radarové zpracování signálu nebo pokročilé komunikační systémy. FPGA jsou kvůli svým možnostem také náročnější a nákladnější na vývoj. [16]

4.5 RTL-SDR

RTL-SDR je nejpopulárnější typ SDR zařízení na trhu. Je tomu tak kvůli jeho širokému rozsahu použití k různým účelům. Zařízení je postaveno na Realtek RTL2832U čipu, který byl původně využíván v DVB-T TV tunerových donglech. Běžná RTL-SDR mohou signál pouze přijímat a nikoliv vysílat. [15; 17]

SDR se kterým budu pracovat v této BP se nazývá Nooelec NESDR SMArTee v2 SDR. Je to RTL-SDR, které je postaveno na čipu RTL2832U. Při jeho vývoji se výrobci snažily dosáhnout co nejnižších úrovní šumu a co nejlepšímu odvodu tepla. Jeho operační frekvence je přibližně 25-1750MHz. Toto SDR je naceněno za 34 amerických dolarů, což je v přepočtu téměř 800Kč. [18]

Obrázek 4 Nooelec SMArTee v2 SDR (RTL-SDR) [18]

5 MOŽNOSTI ZACHYTÁVÁNÍ DAT A JAKÁ DATA LZE ZACHYTIT

Veškeré informace v 2/3/4G sítích přenesené vzduchem jsou rádio-frekvenční signály. Způsobů jakými lze zachytit tyto signály je více, ale v mé práci se budu primárně soustředit na ty, které jsou dosažitelné s pomocí cenově dostupného RTL-SDR, které bude sloužit pouze jako přijímač. [15]

5.1 Zachytávání GSM dat mobilního zařízení

Všechna odemčená mobilní zařízení používají SIM kartu pro komunikaci skrze hovory nebo SMS zprávy. Takovéto informace musí být vzduchem komunikovány k nejbližší BS pomocí RF signálů. Teoreticky lze tyto pakety zachytit, dekódovat a zjistit tak jejich obsah. Ke zpracování těchto paketů lze použít software Wireshark, který umožňuje dekódování a překlad paketů pro uživatele čitelnou formu. Některé informace o uživateli, které takto lze zachytit jsou: Temporary Mobile Subscriber Identity (TMSI), dále také informace o lokalitě uživatele Mobile Country Code (MCC), Mobile Network Code (MNC), Location Area Code (LAC). V paketu se také nachází systémové informace Cell Broadcast Channel (CBCH), Location Area Identity (LAI) a Random Access Channel (RACH). [15; 19]

5.2 Pasivní IMSI Catcher

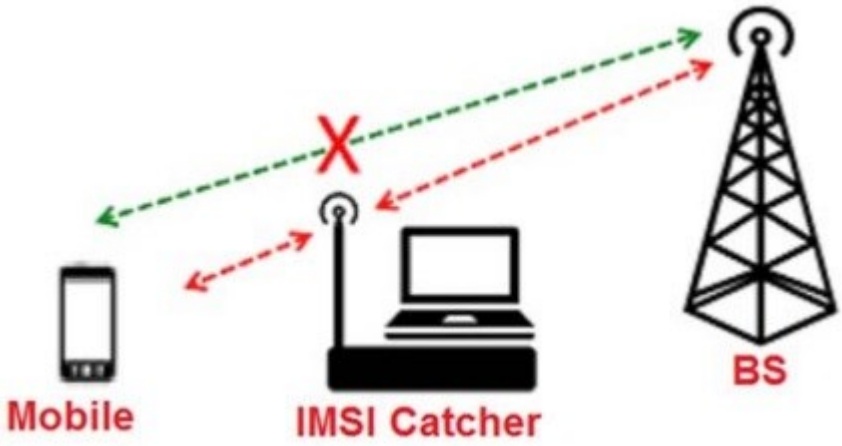
IMSI Catcher je pasivní technika, při které se snažíme zachytit občasné zaslání IMSI uživatele k BS pro jeho ověření. IMSI je unikátní identifikační číslo, které má každý uživatel používající mobilní sítě přiřazené. IMSI je složeno ze tří částí, MCC, MNC a Mobile Subscription Identification Number (MSIN) a celkem může mít max 15 číslic. IMSI může být použito k sledování polohy uživatele a také získávání dat o uživateli například jeho historie hovorů. Zachytávání IMSI ze vzduchu může být provedeno pomocí nástroje grgsm_livemon, který v reálném čase monitoruje GSM síť. Následně s pomocí nástroje Wireshark lze z paketů získat ještě více informací. [15]

5.3 False Base Station Attack / Aktivní IMSI Catcher

Při pasivní technice IMSI Catcher se snažíme zjistit frekvenci na které vysílá BS, abychom mohli zachytit IMSI, které je komunikováno pro ověření uživatele. False Base Station Attack využívá zařízení, které se chová stejně jako základová stanice v síti. Někdy také nazýváno StingRay, cell site simulator nebo cell site emulator. Využívá známé techniky

nazvané Man-in-the-middle a vysílá do okolí falešnou výzvu pro mobilní zařízení, aby se ověřily stejně jako u běžných BS. Mobilní zařízení se poté této falešné BS prokáže svou identitou a tím prozradí své IMSI. Tento typ útoku funguje pro 2/3/4G, protože zabezpečovací procedury pro ochranu identity se spustí až po odeslání uživatelských IMSI, proto může tento útok fungovat. Dosah takovéto falešné BS se pohybuje kolem 100m. Dřív byla takováto zařízení těžce dostupná a exklusivně ji používaly pouze vládní složky pro sledování podezřelých cílů a ochraně společnosti. V dnešní době už jsou ale tato zařízení běžně dostupná na trhu a jsou používána kýmkoliv, kdo si k nim získá přístup. Může se jednat o teroristy, kriminálníky nebo i rádio-amatérské fanoušky pro různé důvody. [20; 13]

Pokud se útočníkovi povede dostat se mezi komunikaci BS a mobilního zařízení, může nyní provádět téměř jakoukoliv operaci s přijatým a vysílaným signálem. Může odposlouchávat hovory, nahrávat je, také zachytávat, číst, měnit a přesměrovávat SMS zprávy, sledovat polohu zařízení, získávat soubory z mobilního zařízení nebo i zapínat mikrofon nebo kameru na zařízení. [20]



Obrázek 5 Grafické zobrazení použití aktivního IMSI Catcher [20]

5.4 IMSI Paging Attack

Tento typ útoku využívá neověřovaného komunikačního řídícího kanálu Common Control Channel (CCCH) pojmenovaného paging type 1. Paging procedura je běžně používaná pro nalezení MS, aby mu mohla být doručena služba, například SMS nebo hovor. Takováto paging zpráva je rozeslána všem MS v dané oblasti a obsahuje požadované TMSI. Pokud ale mobilní síť nezná aktuální TMSI daného MS, může místo toho dotazovat jeho IMSI.

Když MS obdrží zprávu od pagingu obsahující jeho IMSI nebo TMSI, odešle nazpět své aktuální TMSI. [13]

Tento typ útoku dokazuje, že MS lze lokalizovat i v oblastech o velikostech až 100km^2 odposloucháváním pagingových zpráv dané mobilní sítě. IMSI pagingová procedura může být spouštěna odesíláním chybných SMS zpráv nebo pomocí metody přerušených hovorů. Tento typ útoku bylo také možné provést na 2/3/4G sítích. [13]

5.5 Zachytávání hovorů a SMS zpráv uvnitř GSM sítí

Podobně jako při „živém“ sledování GSM sítě, lze zachytit a později dekódovat a dešifrovat hovory a SMS zprávy zachycené pomocí našeho SDR. Při této technice se používá modul grgsm a příkazem grgsm_capture. grgsm_capture bude dle nastavených parametrů ukládat do souboru formátu .cfile zachytávané pakety. Dalším důležitým krokem je zjistit TMSI zařízení, jehož SMS zprávy nebo hovory se budeme snažit dekódovat a rozšifrovat. K rozšifrování bude také potřeba zjistit šifrovací klíč KC, který je pro šifrování A5/1 nebo A5/3 použitý. Když se nám podaří všechny tyto kroky splnit, bude potom možné nahrát tento náš .cfile soubor do programu wireshark pomocí příkazu grgsm_decode. Dekódování SMS zpráv i hovorů funguje skrze grgsm_decode na podobném principu. Mohlo by se také stát, že při hovoru byla aktivována technika „channel hopping“ na základové stanici, ze které byl hovor přijat. To by znamenalo, že hovor by probíhal na více měnících se kanálech kvůli větší bezpečnosti a rušení. Museli bychom poté využít příkazu grgsm_channelize, který umí zachytit data na více různých přenosových kanálech zároveň. Tuto možnost, ale bohužel, nemáme se zařízením RTL-SDR, protože maximální šířka pásma, kterou jsme schopni zachytit je maximálně cca. 3.2MHz. [21; 22]

5.6 AKA Protocol Linkability Attack

AKA je protokol pro vzájemnou autentizaci a navázání autentizovaného klíče mezi mobilní sítí a mobilním zařízením. Tento protokol pracuje na 3G sítích a v mírné obměně i ve 4G mobilních sítích jako EPS-AKA, ale princip útoku je stejný. [13]

Princip fungování je takový, že AKA mobilní sítě zašle autentifikační požadavek mobilnímu zařízení a zařízení odešle nazpět autentifikační odpověď. Při přijetí požadavku ověří mobilní zařízení platnost daného požadavku a tím si ověří platnost mobilní sítě, naopak si zase prověří síť mobilní zařízení. [13]

Ověřovací proces mobilní sítě na mobilním zařízení probíhá ve dvou krocích. V první fázi ověřuje mobilní zařízení Message Authentication Code (MAC) a v druhé ověřuje zda se přijaté Sequence Number (SQN) nachází ve správném rozsahu. Pokud neprojde mobilní síť autentifikací pro mobilní zařízení, mobilní zařízení odešle nazpět autentifikační chybovou hlášku nebo sychronizační chybovou zprávu s identifikací problému. [13]

Útok na tento protokol využívá chybových zpráv zasílaných daným protokolem. Pokud útočník zachytí nešifrovanou autentifikační žádost odeslanou sítí určitému mobilnímu zařízení, může ji opětovně odeslat a mohou nastat dvě možnosti. Pokud byla zpráva určena pro toto zařízení, zařízení odešle nazpět hlášení o selhání SQN (protože toto SQN bylo již přijato). Pokud zpráva nebyla určena pro toto zařízení, zařízení odpoví nazpět s hlášením o nesprávné hodnotě MAC. Tento exploit v AKA protokolu může sloužit útočníkům pro sledování mobilního zařízení a narušovat tak garantovanou "nesledovatelnost" mobilních zařízeních v síti. [13]

	Can be used in			Collects user IDs		User can detect it
	2G	3G	4G	TMSI	IMSI	
IMSI catchers	✓	✓	✓	–	✓	✓
IMSI paging attack	✓	✓	✓	✓	–	–
AKA err msg attack	–	✓	✓	–	–	–

Tabulka 5 Přehled využití útoků na 2/3/4G sítě [13]

V tabulce je jednoduše zobrazen přehled posledních tří uvedených typů útoků na sítě. Můžeme například vidět, že útok na AKA protokol necílí na získávání dat o uživateli, ale slouží primárně pro trasování jeho polohy. „IMSI catchers" je zde myšleno jako „False Base Station Attack" jak mám uveden nadpis v práci.

5.7 Paging attack on LTE

Tento typ paging útoku probíhá na stejném principu jako paging attack uvnitř GSM sítí. Využije se při tom zařízení SDR, které bude zachytávat vysílané signály z okolí. Cílem tohoto útoku je místo IMSI podobně fungující Globally Unique Temporary Identifier (GUTI), který je používán pro lokalizaci uživatelských zařízení. [23]

Jedná se tedy o zachytávání dotazů LTE sítě, které nesou hodnotu GUTI a jsou mířené pro daného uživatele. GUTI hodnota zařízení se nemění ani když se uživatel přesune do jiné MME oblasti, proto lze tento typ útoku využít i pro sledování uživatelské polohy. [23]

Tento experiment byl proveden s využitím zařízení Ettus B200 mini SDR. Software tohoto zařízení bylo pro provedení pokusu nutné přeprogramovat a frekvenční rozsah zařízení se pohybuje mezi 70MHz – 6GHz jak uvádí stránky výrobce. Na tento typ útoku se tedy nebudu v praktické části soustředit, protože se zaměřuji spíše na metody, které jsou proveditelné pomocí cenově dostupného „RTL-SDR“. [23; 24]

5.8 Odposlouchávání rádiových signálů veřejných složek

Pokud v našem okolí vysílají policejní vysílačky, záchranářské komunikační kanály nebo jiné veřejně známé služby je možné je pomocí SDR zachytit a signál zpracovat. Většina států již ale tyto přenosové kanály zašifrovala, bylo to nutné kvůli obrovskému rozmachu levně dostupných SDR zařízení, která by pro tento typ komunikace mohla znamenat ohrožení. Na internetu lze nalézt různé odkazy, kde jsou uvedené frekvence, na kterých jaká služba vysílá. Tyto frekvence se liší oblast od oblasti a je velmi těžké se je pokoušet efektivně zachytit. [15]

5.9 Popis použitých pojmů

TMSI je dočasná identita přiřazená uživateli proto, aby nemusela být po síti komunikována jeho IMSI. Slouží tak pro ochranu jeho identity. TSMI má hodnotu pouze v oblasti zpracovávané jednou VLR databází a tato identita existuje pouze, když se uživatel nachází v dané oblasti. Identita může být také po dobu pobytu uživatele změněna. [11]

MSIN je identifikační číslo uživatele uvnitř jeho domovské sítě. MCC je mobilní číselný znak státu. Je to mezinárodně standardizované třímístné číslo. MNC mobilní číselný znak sítě. Je to dvoumístné číslo pro jednoznačnou identifikaci mobilní sítě uvnitř státu. [11]

Každá oblast má své vlastní identifikační číslo, to je LAI. LAI je složeno hierarchicky a mezinárodně unikátní. Skládá se z Country Code (CC), MNC a Location Area Code (LAC). CC je 3místné označení státu a LAC je maximálně 5místné označení lokální oblasti. LAI je regulérně vysíláno skrze kontrolní kanál Broadcast Control Channel (BCCH). To také znamená, že každá BS vysílá své unikátní identifikační parametry skrze kanál BCCH. Tento kanál umožňuje pohybujícím se mobilním zařízením zachytit nové LAI, pokud se přemístí do jiné oblasti. Když se takto přemístí, mobilní operátor dostane o

této změně informaci, aby mohl v případě mobilního hovoru správně nalézt mobilní zařízení ve své síti. [11; 17]

RACH je rádiový kanál sloužící pro mobilní zařízení, aby mohla zažádat o aktualizaci své polohy. Tento kanál funguje pouze jako uplink. [11]

II. PRAKTICKÁ ČÁST

6 POUŽITÉ NÁSTROJE

Praktickou část mé práce jsem po konzultaci s vedoucím práce začal tvořit a vypracovávat v operačním systému Linux Debian verze „bookworm“ 64bit neboli verze 12.5. [1 INSTALACE] Na mém domácím pracovním počítači jsem měl nainstalovaný OS Windows 11. Použil jsem proto program VirtualBox verze 7.0.16 [2 INSTALACE], kde jsem si vytvořil virtuální počítač s operačním systémem Linux.

Pracoval jsem se zařízením Nooelec NESDR SMArTee v2 SDR, které se do PC zapojovalo pomocí USB portu. Zpřístupnění USB portů domovského zařízení pro virtuální počítač jsem docílil instalací VirtualBox Extension Pack verze 7.0.13 [2 INSTALACE]. Ihned po nainstalování Linuxu jsem si vytvořil profil a nastavil si pro něj administrátorská práva. Toto byl velmi důležitý krok, protože mi to ulehčilo spoustu instalačních procesů a některé programy také nefungují správně, pokud nejsou inicializované v “sudo“ administrátorském režimu.

```
dan@Daniel:~$ su - root
Password:
root@Daniel:~# usermod -aG sudo dan
root@Daniel:~# reboot
```

Obrázek 6 Příkazy pro nastavení administrátorských práv pro profil „dan“

Poté jsem musel do systému nainstalovat ovladače pro mé SDR. Provedl jsem následující sérii příkazů.

```
dan@Daniel:~$ sudo apt install build-essential git
[sudo] password for dan:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
build-essential is already the newest version (12.9).
git is already the newest version (1:2.39.2-1.1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
dan@Daniel:~$ git clone https://github.com/osmocom/rtl-sdr.git
cd rtl-sdr
mkdir build
cd build
cmake ../ -DDETACH_KERNEL_DRIVER=ON
make
sudo make install
sudo ldconfig
```

Obrázek 7 Příkazy pro instalaci ovladačů SDR 1

A aby mohlo být USB zařízení používáno bez root práv. Přidal jsem „udev“ pravidlo a restartoval počítač.

```
dan@Daniel:~/SDRPlusPlus/build$ sudo cp ../rtl-sdr.rules /etc/udev/rules.d/
sudo reboot
```

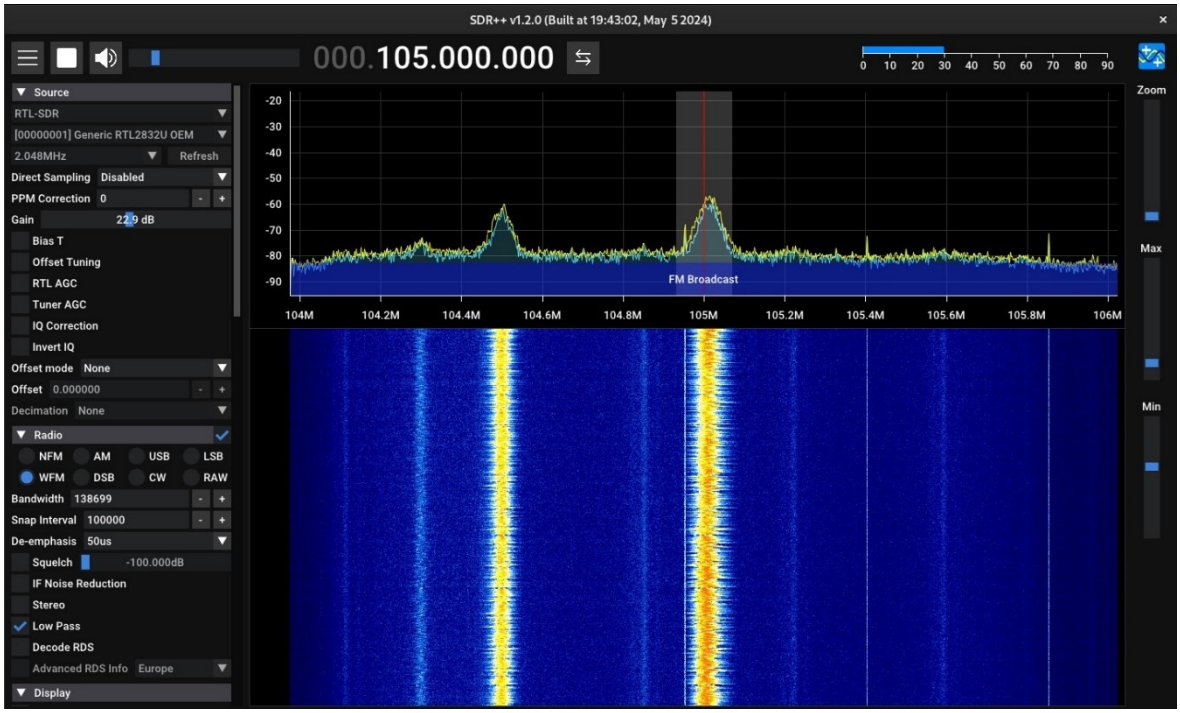
Obrázek 8 Příkazy pro instalaci ovladačů SDR 2

Další krok pro mě bylo nainstalování programu SDR++. Tento program jsem používal při své práci jako takový základní “benchmark“ pro zjištění, zda je mé SDR správně inicializováno, je propojeno s anténou a přijímá signál.

```
dan@Daniel:~$ sudo apt install "required dependencies"
git clone https://github.com/AlexandreRouma/SDRPlusPlus.git
cd SDRPlusPlus
mkdir build
cd build
cmake ..
make
sudo make install
```

Obrázek 9 Příkazy pro instalaci programu SDR++

SDR++ jsem využil, protože je to multi-platformní open source software schopné práce s velkou spoustou SDR zařízeních. Poskytoval pro mě všechno, co jsem pro základní analýzu a vyzkoušení zachytávání signálu potřeboval a díky přehlednému UI bylo jeho ovládání velmi pohodlné. Přečetl jsem si část manuálu na jeho používání a byl jsem schopný úspěšně naladit rádiovou FM stanici Frekvence 1 ve Zlínském kraji (105.0 FM). [25]



Obrázek 10 Prostředí programu SDR++ s naladěnou frekvencí 105Mhz (rádio Frekvence1)

Kalibrate-rtl je další program, který jsem si nainstaloval. Kalibrate je nástroj pro identifikování okolních dostupných GSM kanálů. [17]

```
dan@Daniel:~$ git clone https://github.com/steve-m/kalibrate-rtl.git
sudo apt-get install libtool libfftw3-dev
cd ~/kalibrate-rtl/src
cd kal-v0.4.1
./bootstrap && CXXFLAGS='-W -Wall -O3' ./configure && make
src/kal -h
```

Obrázek 11 Příkazy pro instalaci programu Kalibrate-rtl

Základními příkazy pro používání nástroje kalibrate jsou „kal -h“ a „kal -s GSM900“. Atribut „-h“ otevírá nápovědu pro používání daného nástroje. „kal -s GSM900“ proskenuje okolí a bude vyhledávat dostupné GSM stanice v pásmu 900MHz.

```
dan@Daniel:~$ ~/bin/kal -s GSM900
Found 1 device(s):
  0:  Generic RTL2832U OEM

Using device 0: Generic RTL2832U OEM
Detached kernel driver
Found Rafael Micro R820T tuner
Exact sample rate is: 270833.002142 Hz
[R82XX] PLL not locked!
kal: Scanning for GSM-900 base stations.
```

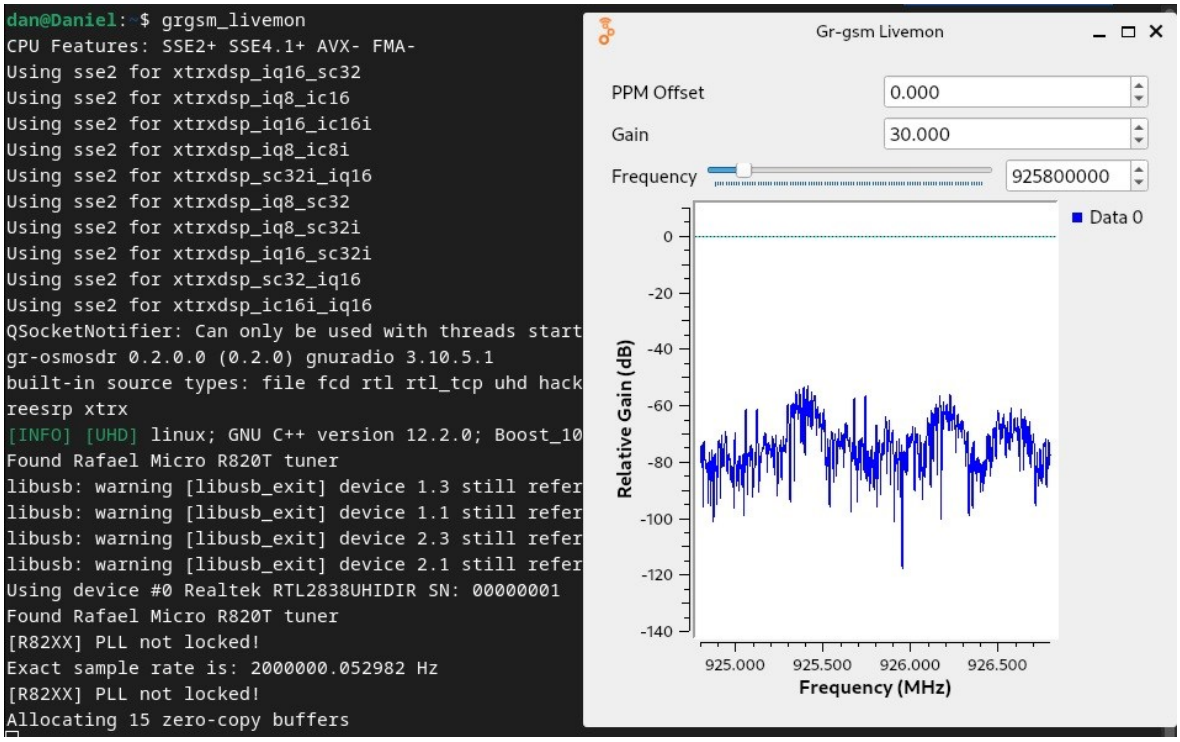
Obrázek 12 Použití základního příkazu „kal“ pro vyhledání GSM stanic v okolí

Dalším důležitým nástrojem pro zachytávání GSM signálů ze vzduchu byl gr-gsm. Tento nástroj se nachází jako modul programu GNU Radio. Při instalaci se mi nainstalovalo jak GNU Radio tak i můj žádaný modul gr-gsm. [17]

```
dan@Daniel:~$ sudo apt install cmake libboost-all-dev libusb-1.0-0-dev
git clone https://github.com/ptrkrysik/gr-gsm.git
cd gr-gsm
mkdir build
cd build
cmake ..
make
sudo make install
sudo ldconfig
```

Obrázek 13 Instalace modulu gr-gsm

Jedním ze základních příkazů, kterých budu využívat pro skenování GSM sítě bude příkaz „grgsm_livemon“, livemon jako zkratka pro monitorování aktuálního přenosu přes síť.

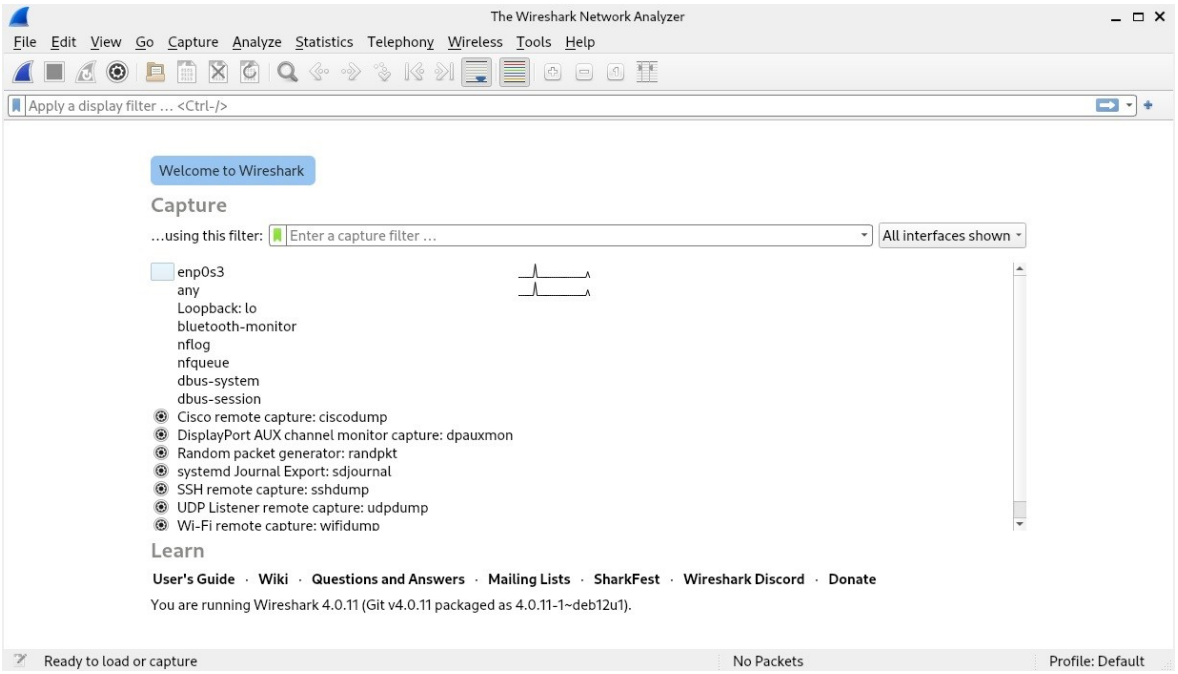


Obrázek 14 Příklad použití příkazu grgsm_livemon

Posledním programem co jsem instaloval je program Wireshark. Wireshark je nástroj pro analýzu paketů v reálném čase a zobrazuje je uživateli v čitelné formě. Multiplatformní nástroj velmi často využívaný ve spoustě případů, kdy chce uživatel dekódovat signály zachycené z mobilní sítě. Příkazy použité po samotné instalaci programu jsou konfigurační příkazy pro nastavení práv programu wireshark na uživatelském účtu dan. Bez nastavení těchto práv nemůže wireshark bez problémů pracovat. [17]

```
dan@Daniel:~$ sudo apt install wireshark
sudo dpkg-reconfigure wireshark-common
sudo usermod -aG wireshark dan
```

Obrázek 15 Instalace programu Wireshark



Obrázek 16 Úvodní obrazovka programu Wireshark

7 MONITOROVÁNÍ SÍTĚ A ZÍSKÁVÁNÍ DAT

V této části mojí bakalářské práce se pokusím prakticky aplikovat některé metody získávání dat, které jsem teoreticky popsal v teoretické části. Budu ale zde omezen některými okolnostmi, jako jsou hardwarové limity mých periferií například: maximální zachytitelná frekvence mého SDR, příjem antény, ale také legislativa, protože odposlouchávání nebo zachytávání uživatelských hovorů a dalších dat je nelegální činnost.

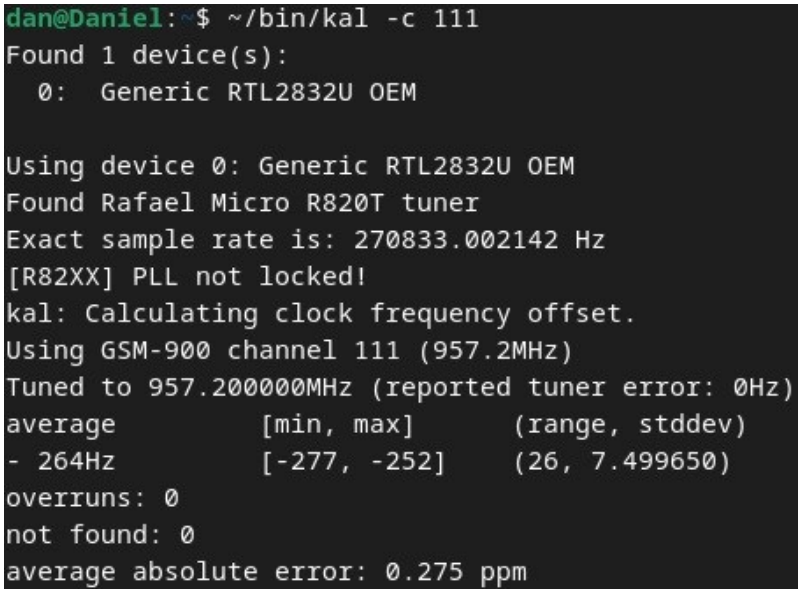
7.1 Sledování dat GSM sítí / Paging Request Attack

Jako první krok zde použiji nástroj Kalibrate pro zjištění okolních operujících GSM kanálů. V příkazovém řádku použiji příkaz „kal -s GSM900“, který spustí sken okolních GSM kanálů v prostoru 900MHz.

```
    chan:   22 (939.4MHz + 147Hz)    power:   28808.82
    chan:   23 (939.6MHz - 168Hz)    power:   29149.17
    chan:   26 (940.2MHz + 582Hz)    power:   37052.85
rtlsdr_demod_write_reg failed with -9
r82xx_write: i2c wr failed=-9 reg=17 len=1
r82xx_set_freq: failed=-9
Tuning to 940600000 Hz failed!
rtlsdr_demod_write_reg failed with -9
r82xx_write: i2c wr failed=-9 reg=17 len=1
r82xx_set_freq: failed=-9
Tuning to 940800000 Hz failed!
```

Obrázek 17 část získaných kanálů z příkazu „kal -s GSM900“

Většina kanálů v tomto příkazu selže, protože nemáme dostatečně silnou anténu, abychom měli široko-geografický rozsah. Nám ale stačí zjistit frekvenci jednoho z kanálů, na který máme dosah a s tím budeme pracovat v dalším kroku.

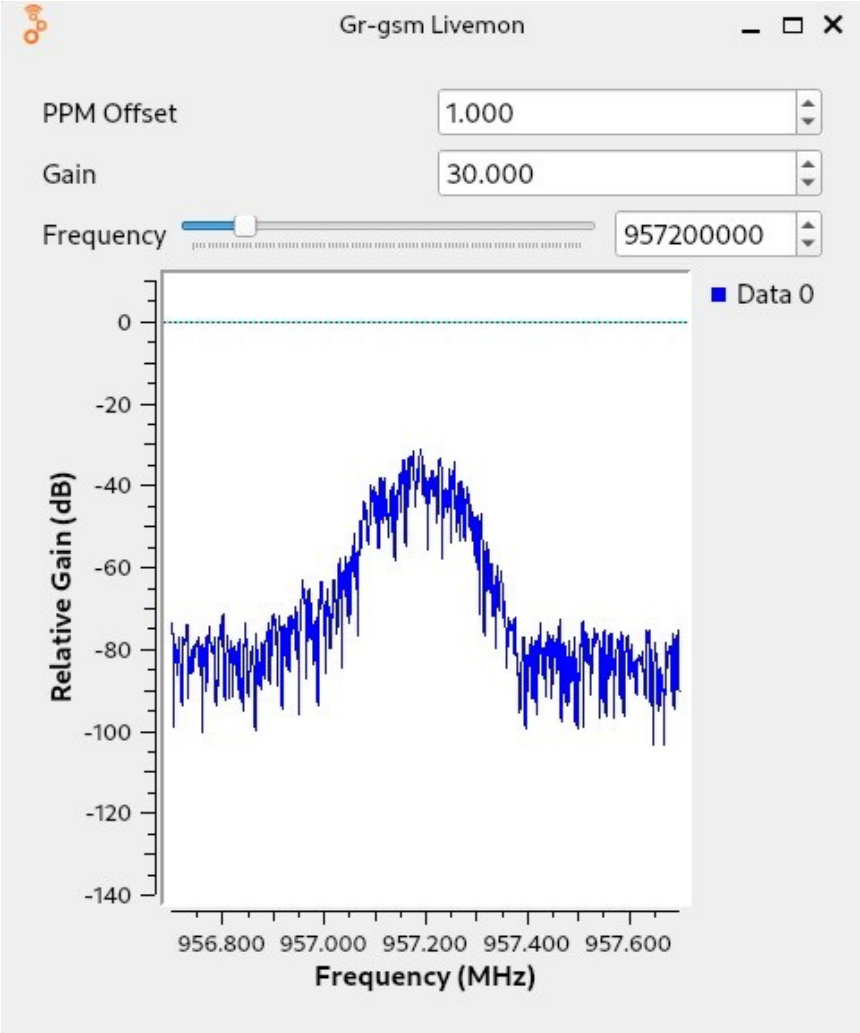


Obrázek 18 Výkonostní specifika zvoleného kanálu 111

Zvolil jsem kanál 111 s frekvencí 957.2MHz, protože byl přijat s nejvyšší přijatou energií signálu a průměrnou odchylkou v přijaté frekvenci pouze -264Hz. Nyní využiji tento kanál a budu zachytávat downlink paketů na vysílacím řídícím kanálu BCCH. Zaprvé si zapnu program wireshark „sudo wireshark“ na kterém budu zachytávané pakety číst a analyzovat v čitelném formátu pro člověka. Druhý krok bude otevření si dalšího okna příkazového řádku. V něm spustím příkaz „grgsm_livemon -f 957.2M -s 1e6 -g 30 -p 1“.

- grgsm_livemon -> je příkaz, který spustí živé snímání paketů ze zadané frekvence
- atribut -f -> nastaví frekvenci jakou bude livemon sledovat. Jedná se o náš zjistěný kanál
- atribut -s -> nastaví „sample rate“ jakým bude daný signál zpracováván
- atribut -g -> nastaví „gain“, který bude signálu přidán. Pro mě byla hodnota 30 optimální řešení, protože signál jsem přijímal v dost slabém stavu a při 0 gain signál nebyl téměř rozlišitelný od šumu okolí
- atribut -p -> je nastavení „offsetu“ signálu. Je to korekce odchylky přijímaného signálu způsobené naším SDR

S tímto nastavením se mi spustilo okno grgsm_livemon a příjem dat začal. Tento program bude snímat data do nekonečna, dokud otevřené okno nezavřeme nebo nepoužijeme klávesovou zkratku Ctrl + C.



Obrázek 19 grgsm_livemon přijímá signál s nastavenými parametry

Nyní se přesunu do programu wireshark a budu sledovat rozhraní „Loopback: Lo“ na portu 4729, na které grgsm_livemon posílá přijímané pakety. To je lokální adresa na PC 127.0.0.1.

Pakety zasílané mezi základovými stanicemi a mobilními zařízeními jsou pojmenované jako Paging Request nebo System information. Každý z těchto typů paketu nese mírně rozličnou informaci. V krátkosti popíšu rozdíly mezi některými z nich a poté uvedu příklady toho, jaké typy jsem vlastním SDR také zachytil. [17]

System Information Message

Toto jsou zpravidla typy zpráv, které mobilní zařízení potřebuje pro správnou komunikaci se sítí. Tyto zprávy jsou vysílány na BCCH a mají více typů: [17]

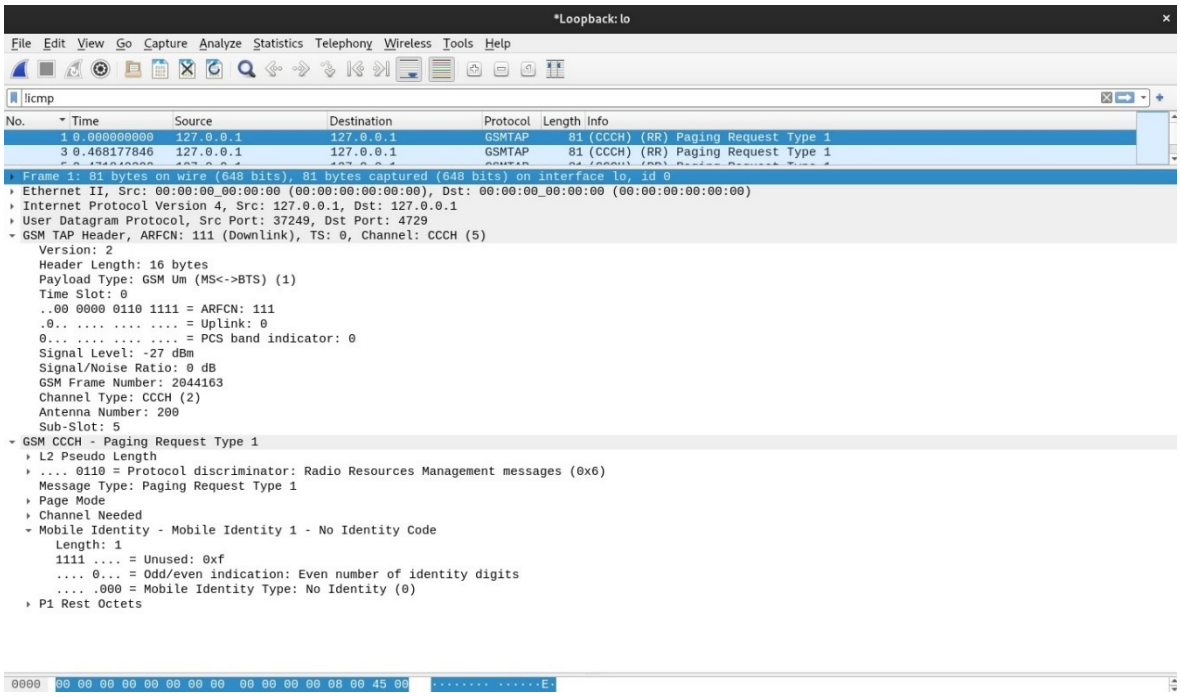
- Type 1 -> Obsahuje list ARFCN kanálů dané BS a RACH parametrů [17]

- Type 2 -> Obsahuje list ARFCN kanálů sousedící BS a list frekvencí BCCH [17]
- Type 3 -> Obsahuje dekódované ID BS, také LAI (MCC, MNC, LAC) a některé GPRS informace [17]
- Type 4 -> Obsahuje dekódované LAI, RACH parametry a některé GPRS informace [17]
- Type 2quater -> Tento typ je 3G zpráva, obsahuje informace o sousedící 3G BS [17]
- Type 13 -> Obsahují všechny důležité informace o GPRS [17]

Paging Request Message

Téměř naprostá většina paging requestů je vysílána typu 1 a je bez identifikace mobilního zařízení. Některé potom obsahují TMSI nějakého mobilního zařízení v dané LAI oblasti.

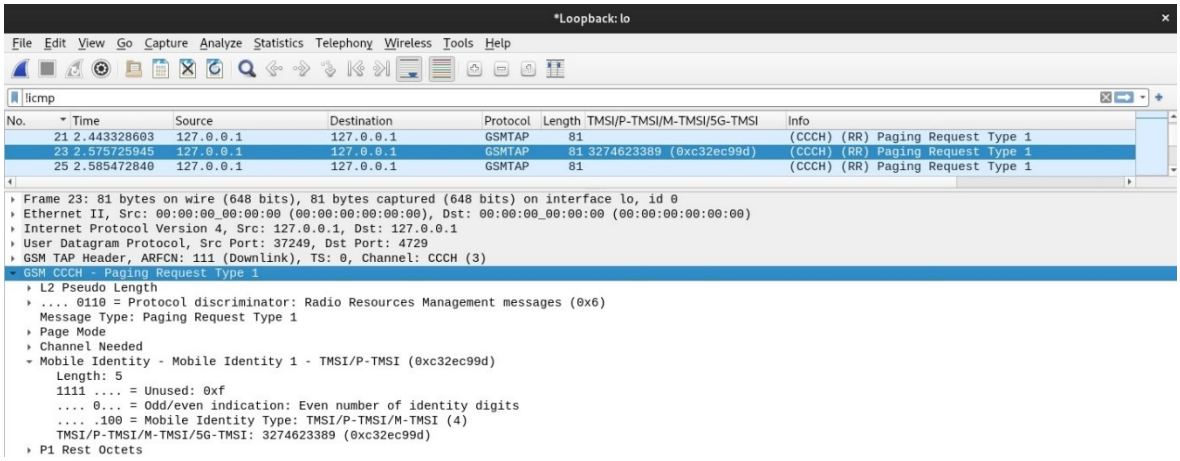
- Type 1 -> Většina těchto requestů je vysílána prázdná. Aktivní paket ale obsahuje buďto IMSI nebo TMSI/P-TMSI mobilního zařízení [17]
- Type 2 -> Obsahuje TMSI/P-TSMI nebo IMSI [17]
- Type 3 -> Obsahuje TMSI/P-TMSI [17]



Obrázek 20 Zachycený paket Paging Request typu 1

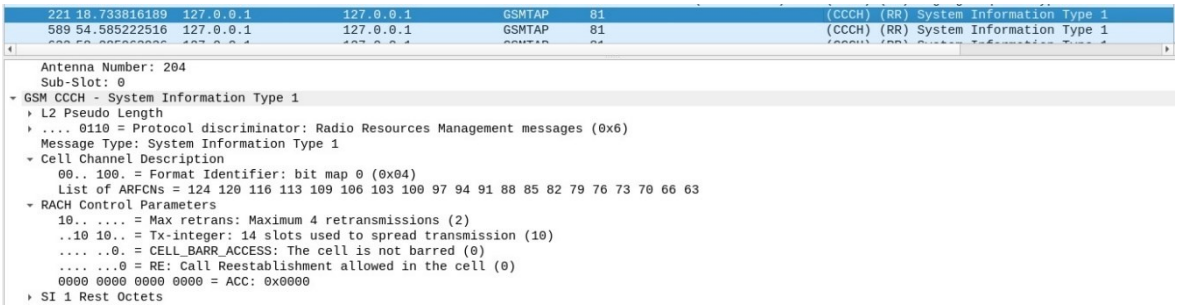
Ve vrchní části v textovém řádku lze vidět, že jsem použil filtr pro zobrazované pakety „!icmp“. Protokol ICMP nás v tuto chvíli nezajímá, protože slouží pouze pro identifikaci errorů při pracování s na IP založenými sítěmi, takže jsem ho tímto vyřadil ze zobrazování v okně přehledu přijatých paketů. Poté již lze vidět pouze přijaté pakety protokolu GSMTAP přijaté na UDP portu 4729. GSMTAP je protokol, který slouží pro přemisťování přijatých GSM paketů na interní UDP port 4729. GSMTAP přidává přijatému paketu pseudo-header, což je hlavička paketu přidaná před zprávu/obsah paketu samotného. Tato hlavička obsahuje pouze základní informace o paketu a zbytek zprávy je obsažen v těle paketu. [26]

Vidíme, že se jedná o Paging Request Type 1 uvnitř CCCH na kanálu číslo 5, který nenesl žádnou hodnotu TMSI. Uvnitř GSMTAP Header, kde lze vidět, že přijímáme base station downlink, se o paketu dozvíme Absolute Radio Frequency Channel Number (ARFCN), což je 111. Také zjistíme úroveň jeho signálu, která je na úrovni -27dBm, to je hodnota, které maximálně dosahuje náš přijatý signál. [17]



Obrázek 21 Zachycený paket Paging Request typu 1 nesoucí hodnotu TMSI

Tento paket je téměř v každém parametru stejný jako ostatní vysílané pakety typu Paging Request Type 1. Tento byl ale obohacen o hodnotu TMSI. Tak lze předpokládat, že jeho cílem bylo identifikovat nějaké mobilní zařízení s daným TMSI. To mohlo být z důvodu navázání hovoru, přemístění zařízení do jiné oblasti, nebo vyhledání zařízení kvůli poskytnutí jiných datových služeb.



Obrázek 22 Zachycený paket System Information Type 1

Kvůli repetitivnosti a špatné čitelnosti screenshotů zde nebudu vkládát další. Zmíním ale, že za dobu testování zachytávání těchto paketů jsem zachytil pouze Paging request type 1 a 2, a také jsem zachytil System Information typu 1, 13, 2, 2quater, 3 a 4.

V této části práce se mi podařilo nasimulovat situaci podobně, jako to udělali různé zdroje a studie přede mnou. Povedlo se mi zachytit data z komunikačních GSM kanálů a zobrazit je ve svém linuxu v čitelné formě pro člověka. Podařilo se mi zachytit data jak o uživatelích, tak i o základových stanicích v mém dosahu a potvrdil jsem, že je možné použít IMSI paging attack.

7.2 Zachytávání a dekódování hovoru/SMS na GSM síti

Jako první věc bych se zde chtěl zmínit, že odposlouchávání a narušování celulární komunikace uživatelů se základovými stanicemi je nelegální. Uvedu zde pouze něco jako „dummy postup“, jak by princip zachytávání a dešifrování hovorů a SMS zpráv fungoval při použití SDR v mém případě.

Používaný software bude stejný jako u zachytávání ostatních GSM signálů. Budu používat program Wireshark pro zobrazování a analýzu paketů ve čitelné formě pro člověka a také modul grgsm, u kterého budeme využívat příkaz „grgsm_capture“.

Navazuji zde na již používané příkazy v kapitole 7.1, takže je již nebudu znovu opakovat kvůli redundanci. Poté co zjistíme pomocí nástroje kalibrate na jaké frekvenci operuje nejvýkonnější základová stanice, přesuneme se do příkazového řádku. Naším cílem bude zachytávat a ukládat probíhající komunikaci po tomto kanále do souborů s příponou .cfile a poté tyto soubory analyzovat.

Pro udržení přehlednosti v našem systému si založíme složku, kam budeme ukládat průběžně zachycené .cfile soubory. V terminálu příkazem „mkdir nazev_slozky“ takovou složku vytvoříme v aktuálním adresáři, kde se nacházíme. Já ji vytvořil uvnitř mého

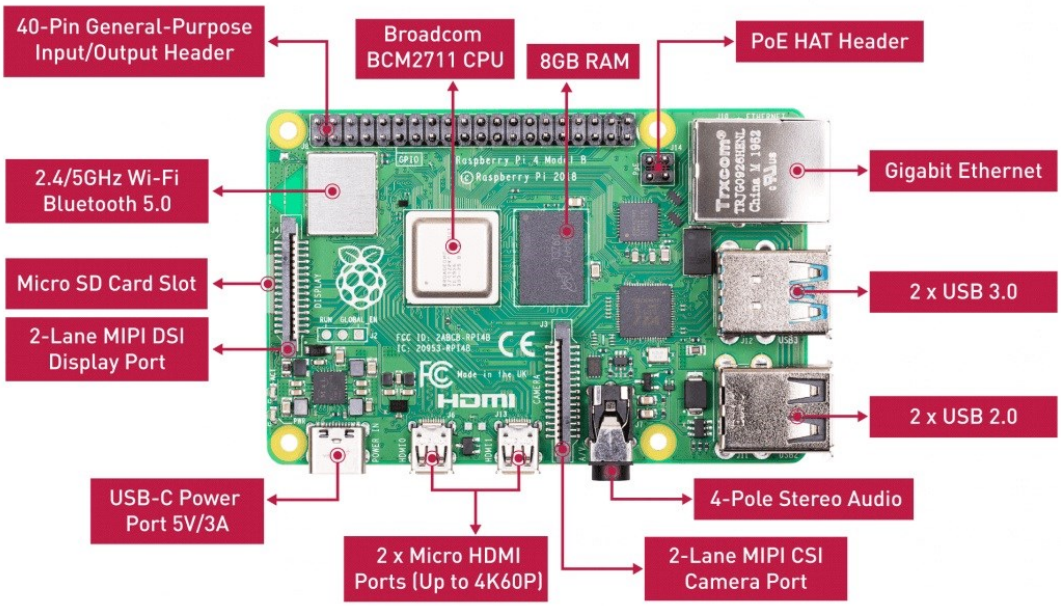
domovského adresáře a pomocí „cd“ příkazu se do ní přesunul. Poté použiji příkaz „grgsm_capture -f 957.2M -g 30 -s 1e6 -p 1 -T 20 zachycenegsm.cfile“, který začne zachytávat a ukládat veškerou komunikaci na frekvenci 957.2MHz. Atributy tohoto příkazu jsou téměř stejné jako u „grgsm_livemon“ jenom je přidaný atribut T, který definuje po jak dlouhou dobu bude signál ukládán. 20 sekund by pro reálné využití příliš praktické nebylo, ale podle vytíženosti sledovaného kanálu by velikosti těchto souborů mohly vystoupat až do výšin GB, kdyby byl čas zachytávání dostatečně dlouhý.

Kdybych znal potřebné údaje o uživateli, typu šifrování na aktuálním kanále, šifrovací klíč a měl zachycenou tu část přenosu dat, kdy probíhal hovor nebo byly zasílány zprávy SMS, tak bych byl schopný touto metodou opravdu dešifrovat hovor nebo SMS. Byl by k tomu použit příkaz „grgsm_decode“ s odpovídajícími parametry. Tento příkaz pracuje se soubory .cfile, které zachytáváme a dekóduje je s pomocí programu wireshark.

8 BUDOUCÍ MOŽNOSTI TÉTO PRÁCE

Můj projekt je nyní značně omezen schopnostmi mobility, jelikož se nachází na jedné geografické poloze. Aktuální možnosti přesunu by bylo přemístění celého PC a dalšího potřebného hardware pro jeho ovládání nebo překopírování a přesun „image“ Linux Debian, který funguje na virtuálním PC. Ani jedna z možností ale není příliš praktická. PC a ostatní hardware jsou těžké a křehké a přemisťovat je není nikdy příjemná záležitost. Za druhé přesun „image“ linuxu například přes USB flash disk je sice přívětivější možnost, ale musíme se zde zamyslet také nad více okolnostmi. Flash disk můžeme ztratit, může mít poruchu, musí mít dostatečnou paměť. Také musíme mít druhé PC, kde bychom linux instalovali, k tomu bychom zase potřebovali Virtual Box a ještě by musel být proveden celý instalační proces.

Raspberry Pi je název jednodeskového počítače vyráběného firmou Raspberry Pi Foundation. Raspberry Pi je malé a levné zařízení, které je používáno lidmi z různých oborů a různých úrovní znalostí. Kompaktní zařízení, jehož operační systém je postaven na OS Linux. Lze k němu pomocí I/O portů jednoduše připojit periferie jako klávesnice, myš, monitor a také pomocí GPIO portů téměř jakékoliv další elektronické komponenty. Pro mou práci nejzajímavější fakt u Raspberry Pi je to, že jeho OS je nahraný na SD kartě, kterou lze z počítače vyjmout a přeprogramovat dle potřeby. Samozřejmě Raspberry Pi je omezeno hardwarovými vlastnostmi, které ale v dnešní době dosahují možností až čtyřjádrového procesoru a 8GB RAM. [27; 28]



Obrázek 23 Periferie Raspberry Pi 4 Model B [29]

Již i na oficiálních stránkách distribuce Linux Debian existuje popis postupu, jak přeinstalovat původní OS Raspberry Pi na vlastní zamýšlenou distribuci. Jelikož je Raspberry Pi OS založený na Linux Debian, pro daný hardware není poté problém pracovat přímo s distribucí Debian. Z aktuální relace Linux Debian na které jsem pracoval na projektu, je možné vytvořit „image“ systému. Ten bych poté nahrál na SD kartu místo původního OS. [30]

Raspberry Pi by po řádné instalaci a provedení nastavení systému vyžadovala pouze napájení, jinak by bylo zařízení připraveno k práci. Pomocí dostupných portů bych mohl připojit například LCD displej pro zobrazování sledované frekvence, nebo připojit tlačítka pro lazení frekvence. Díky Wi-Fi/Bluetooth modulu bych mohl informace z Raspberry komunikovat do dalších zařízení a mít tak víceúčelný systém pro zachytávání mobilních sítí i jiných dat. Takovýto více kompaktní a přenosnější systém by mohl být použitelný pro rádio-amatérské nadšence za dostupnou cenu potřebného hardwaru. Věřím, že tento postup by mohl být tématem pro zadání budoucí navazující práce ve stejném oboru, například pro diplomovou práci.

ZÁVĚR

V této bakalářské práci byly detailně prozkoumány mobilní sítě druhé, třetí a čtvrté generace a byly představeny různé metody a techniky pro jejich sledování, s důrazem na využití softwarově definovaného rádia (SDR). Díky kombinaci teoretického popisu a praktických experimentů byla práce schopna poskytnout vhled do možností a fungování těchto sítí.

Praktická část práce potvrdila, že RTL-SDR je extrémně užitečné zařízení pro zachytávání a analyzování signálů z mobilních sítí. Výsledky praktických experimentů potvrdily metody sledování dat diskutované v teoretické části. Navíc práce pouzkázala na několiv výzev a omezení související s použitím SDR, což naznačuje směry pro další studium. Mezi tyto výzvy patří zlepšení schopností zachytávání signálů při vyšších frekvencích a zlepšení efektivity analýzy dat.

Vzhledem k neustálému vývoji mobilních technologií a rostoucí závislosti na bezdrátové komunikaci, bude klíčové pokračovat ve výzkumu a vývoji metod pro monitorování a analýzu telekomunikačních sítí. Budoucí práce by mohly zahrnovat rozšíření aplikací SDR na sítě páté generace (5G), což by přineslo další inovace v oblasti telekomunikací a zabezpečení sítí. Tato práce tak představuje základní kamen pro budoucí studie zabývajícím se využití SDR při monitorování telekomunikačních sítí.

SEZNAM POUŽITÉ LITERATURY

[1] FARLEY, Tom. Future Mobile Phones. Online. *Future Mobile Phones*. 2005, roč. 1, č. 3, s. 12. ISSN 0085-7130. Dostupné z: https://d1wqtxts1xzle7.cloudfront.net/30805674/T05_3-4-libre.pdf. [cit. 2024-05-13].

[2] MSHVIDOBADZE, Titanin. Evolution mobile wireless communication and LTE networks. Online. *Https://ieeexplore.ieee.org/abstract/document/6398495*. 2012, roč. 1, č. 1, s. 7. Dostupné z: https://ieeexplore.ieee.org/abstract/document/6398495. [cit. 2024-05-13].

[3] GU, Guifen a PENG, Guili. The survey of GSM wireless communication system. Online. *The survey of GSM wireless communication system*. 2010, roč. 1, č. 1, s. 4. Dostupné z: https://ieeexplore.ieee.org/abstract/document/6141552. [cit. 2024-05-13].

[4] MONDAL, Sarmistha; SINHA, Anindita a ROUTH, Jayati. A Survey on Evolution of Wireless Generations 0G to 7G. Online. *A Survey on Evolution of Wireless Generations 0G to 7G*. 2015, roč. 1, č. 1, s. 6. Dostupné z: https://d1wqtxts1xzle7.cloudfront.net/33394352/A_Survey_on_Evolution_of_Wireless_Generations_0G_to_7G-libre.pdf. [cit. 2024-05-13].

[5] SIMATE, Zilole. Evaluation of mobile network security. Online. *Evaluation of mobile network security*. 2013, roč. 1, č. 1, s. 6. Dostupné z: https://ieeexplore.ieee.org/abstract/document/7055108. [cit. 2024-05-13].

[6] A Review on Mobile Technologies: 3G, 4G and 5G. Online. *A Review on Mobile Technologies: 3G, 4G and 5G*. 2017, roč. 1, s. 5. Dostupné z: https://ieeexplore.ieee.org/abstract/document/8057566. [cit. 2024-05-13].

[7] YU, Wenqiong. The Network Security Issue of 3G Mobile Communication System Research. Online. *The Network Security Issue of 3G Mobile Communication System Research*. 2010, roč. 1, č. 1, s. 4. Dostupné z: https://ieeexplore.ieee.org/abstract/document/5532739. [cit. 2024-05-13].

[8] HAJLAOUI, Emna; ZAIER, Aida; KHLIFI, Abdelhakim; GHODHBANE, Jihed; BEN HAMED, Mouna et al. 4G and 5G technologies: A Comparative Study. Online. *4G and 5G technologies: A Comparative Study*. 2020, roč. 1, č. 1, s. 6.

Dostupné z: https://ieeexplore.ieee.org/abstract/document/9231605. [cit. 2024-05-13].

[9] BHASKER, Daksha. Journal of Cyber Security & Information Systems. Online. *Journal of Cyber Security & Information Systems*. 2013, roč. 1, č. 1, s. 32. Dostupné z: https://csiac.org/wp-content/uploads/2021/06/CSIAC_V1N4_FINAL_2.pdf. [cit. 2024-05-13].

[10] J. KIM, Byoung-Jo a S. HENRY, Paul. Directions for future cellular mobile network architecture. Online. *Directions for future cellular mobile network architecture*. 2012, roč. 1, č. 1, s. 9. Dostupné z: https://firstmonday.org/ojs/index.php/fm/article/view/4204. [cit. 2024-05-13].

[11] R. MISHRA, Ajay. *Advanced cellular network planning and optimisation: 2G/2.5 G/3G... evolution to 4G*. Online. John Wiley, 2007. ISBN 978-0-470-01471-4. Dostupné z: https://d1wqtxts1xzle7.cloudfront.net/12699672/Advanced_Cellular_Network_Planning_and_Optimisation__Misha-libre.pdf. [cit. 2024-05-13].

[12] ALI ALMAZROI, Abdulaleem. Performance analysis of 4G broadband cellular networks. Online. *Performance analysis of 4G broadband cellular networks*. 2018, roč. 1, č. 1, s. 6. Dostupné z: https://d1wqtxts1xzle7.cloudfront.net/97722036/03_202018-5-9-pp.12-17-libre.pdf. [cit. 2024-05-13].

[13] BOJIC, Iva; YOSHIMURA, Yuji a RATTI, Carlo. Opportunities and Challenges of Trip Generation Data Collection Techniques Using Cellular Networks. Online. *Opportunities and Challenges of Trip Generation Data Collection Techniques Using Cellular Networks*. 2017, roč. 1, č. 1, s. 6. Dostupné z: https://ieeexplore.ieee.org/abstract/document/7876983. [cit. 2024-05-13].

[14] ULVERSOY, Tore. Software Defined Radio: Challenges and Opportunities. Online. *Software Defined Radio: Challenges and Opportunities*. 2010, roč. 1, č. 1, s. 20. Dostupné z: https://ieeexplore.ieee.org/abstract/document/5462981. [cit. 2024-05-13].

[15] BABU SAJJA, Surendra; PRANEETH AVAPATI, Sai; NATH JAGARLAMUDI, Narendra; KAMRUDDIN SHAIKH, Khalid a BHARGAVI MADIREDDY, Bindu. A Generic Overview of Software Defined Radio in the

Security Realm. Online. *A Generic Overview of Software Defined Radio in the Security Realm*. 2021, roč. 1, č. 1, s. 5. Dostupné z: https://ieeexplore.ieee.org/abstract/document/9688353. [cit. 2024-05-13].

[16] AKEELA, Rami a DEZFOULI, Behnam. Software-defined Radios: Architecture, state-of-the-art, and challenges. Online. *Software-defined Radios: Architecture, state-of-the-art, and challenges*. 2018, roč. 1, č. 1, s. 20. Dostupné z: https://www.sciencedirect.com/science/article/pii/S0140366418302937. [cit. 2024-05-13].

[17] PARMAR, Arjunsinh a M. PATTANI, Kunal. Sniffing GSM Traffic Using RTL-SDR And Kali Linux OS. Online. *Sniffing GSM Traffic Using RTL-SDR And Kali Linux OS*. 2017, roč. 1, č. 1, s. 6. Dostupné z: https://d1wqtxts1xzle7.cloudfront.net/51881876/IRJET-V4I1323-libre.pdf. [cit. 2024-05-13].

[18] *Nooelec NESDR SMArTee v2 SDR - Premium RTL-SDR w/ Aluminum Enclosure, Bias Tee, 0.5PPM TCXO, SMA Input. RTL2832U & R820T2-Based*. Online. Nooelec. 2024. Dostupné z: https://www.nooelec.com/store/nesdr-smartee-sdr.html. [cit. 2024-05-13].

[19] MARTOYO, Ihan; SETIASABDA, Paul; Y. KANALEBE, Herman; P. URANUS, Henri a PARDEDE, Marincan. Software Defined Radio for Education: Spectrum Analyzer, FM Receiver/Transmitter and GSM Sniffer with HackRF One. Online. *Software Defined Radio for Education: Spectrum Analyzer, FM Receiver/Transmitter and GSM Sniffer with HackRF One*. 2018, roč. 1, č. 1, s. 5. Dostupné z: https://ieeexplore.ieee.org/abstract/document/9084568. [cit. 2024-05-13].

[20] ALRASHEDE, Hamad a AHMED SHAIKH, Riaz. IMSI Catcher Detection Method for Cellular Networks. Online. *IMSI Catcher Detection Method for Cellular Networks*. 2019, roč. 1, č. 1, s. 6. Dostupné z: https://ieeexplore-ieee-org.proxy.k.utb.cz/document/8769507. [cit. 2024-05-13].

[21] TALHA CHOUDARY, Muhammad; YASEEN, Arish; A JAVAID, Muhammad; R KHAN, Abeer; A KHAWAJA, Bilal et al. Sniffing, Decoding and Decryptionof GSM signals using Open Source Software and Low Cost Hardware. Online. *Sniffing, Decoding and Decryptionof GSM signals using Open Source*

Software and Low Cost Hardware. 2017, roč. 1, č. 1, s. 4. Dostupné z: https://d1wqtxts1xzle7.cloudfront.net/79104273/2nd_IEEC_2017_paper_13-libre.pdf. [cit. 2024-05-13].

[22] KRYSIK, Piotr. *Gr-gsm*. Online. Github. 2017. Dostupné z: https://github.com/ptrkrysik/gr-gsm/wiki/Usage. [cit. 2024-05-13].

[23] YEE, Nathan. Performing a Practical Paging Attack on the LTE Network. Online. *Performing a Practical Paging Attack on the LTE Network*. 2017, roč. 1, č. 1, s. 4. Dostupné z: https://digitalcommons.calpoly.edu/cgi/viewcontent.cgi?article=1124&context=cscsp. [cit. 2024-05-13].

[24] *USRP B200mini*. Online. Ettus. 2024. Dostupné z: https://www.ettus.com/all-products/usrp-b200mini/. [cit. 2024-05-13].

[25] *SDR++ USER GUIDE*. Online. Sdrpp. 2022. Dostupné z: https://www.sdrpp.org/manual.pdf. [cit. 2024-05-13].

[26] MOHAMMED, Nasibeh a KISORE, N. Raghu. Experimental evaluation of security in 2G cellular networks in India. Online. *Experimental evaluation of security in 2G cellular networks in India*. 2015, roč. 1, č. 1, s. 5. Dostupné z: https://ieeexplore.ieee.org/abstract/document/7154797. [cit. 2024-05-13].

[27] *What is a Raspberry Pi?* Online. Opensource. 2024. Dostupné z: https://opensource.com/resources/raspberry-pi. [cit. 2024-05-13].

[28] *What Is Raspberry Pi? Models, Features, and Uses*. Online. BASUMALLICK, Chiradeep. Spiceworks. 2022. Dostupné z: https://www.spiceworks.com/tech/networking/articles/what-is-raspberry-pi/. [cit. 2024-05-13].

[29] WU, Elaine. *Meet The Brand New Raspberry Pi 4 8GB*. Online. Seeedstudio. 2020. Dostupné z: https://www.seeedstudio.com/blog/2020/05/28/meet-the-brand-new-raspberry-pi-4-8gb-ram/. [cit. 2024-05-13].

[30] *RaspberryPiImages*. Online. Wiki.debian. 2024. Dostupné z: https://wiki.debian.org/RaspberryPiImages. [cit. 2024-05-13].

[31] *Download VirtualBox (Old Builds): VirtualBox 7.0*. Online. Virtual Box. 2024. Dostupné z: https://www.virtualbox.org/wiki/Download_Old_Builds_7_0. [cit. 2024-05-13].

[32] *Installing Debian 12.5*. Online. Debian. 2024. Dostupné z: https://www.debian.org/releases/bookworm/debian-installer/. [cit. 2024-05-13].

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

3GPP	Third Generation Partnership Project
AMPS	Advanced Mobile Phone Service
ARFCN	Absolute Radio Frequency Channel Number
BCCH	Broadcast Control Channel
BS	Base Station
BSC	Basic System Controller
BSS	Basic Station Subsystem
BTS	Basic Transceiver System
BTS	Base Transceiver Station
CBCH	Cell Broadcast Channel
CC	Code Country
CCCH	Common Control Channel
CDMA	Code Division Multiple Access
CN	Core Network
CS	Circuit Switched
D-AMPS	Digital AMPS
DDoS	Distributed Denial of Service
DNS	Domain Name System
DSP	Digital Signal Processor
EDGE	Enhanced Data rates for Global Evolution
EPC	Evolved Packet Core
E-UTRAN	Evolved UTRAN
FDD	Frequency Division Duplex
FPGA	Field-Programmable Gate Array
GPP	General Purpose Processor

GPRS	General Packet Radio Services
GSM	Global System for Mobile Communications
GUTI	Globally Unique Temporary Identifier
HLR	Home Location Register
HSDPA	High-Speed Downlink Packet Access
HSPA	High-Speed Pakcet Access
HSUPA	High-Speed Uplink Packet Access
IMSI	International Mobile Subscriber Identity
IMT	International Mobile Telecommunications
IoT	Internet of Things
LAC	Location Area Code
LAI	Location Area Identity
LTE	Long Term Evolution
MAC	Message Authentication Code
MAGIC	Mobile multimedia Anywhere Global mobility solutions over Integrated wireless and Customized services
MCC	Mobile Country Code
ME	Mobile Equipment
MIMO	Multiple Inputs and Multiple Outputs
MME	Mobile Management Entity
MNC	Mobile Network Code
MS	Mobile System
MSC	Mobile-Services Switching Center
MSIN	Mobile Subscription Identification Number
NNS	Network and Switching Subsystem
OFDMA	Orthogonal Frequency Division Multiple Access

OMC	Maintenance Centre
OMSS	Operation and Management Subsystems
OSS	Operation Support Subsystem
PDC	Personal Digital Cellular
PLMN	Public Land Mobile Network
QoS	Quality of Service
RACH	Random Access Channel
RAN	Radio Access Network
RF	Radio Frequency
RNC	Radio Network Controller
RTL- SDR	Realtek SDR
SCA	Software Communications Architecture
SC-FDMA	Single Carrier Frequency Division Multiple Access
SDR	Software Defined Radio
SIM	Subscriber Identity Module
SMS	Short Messaging Services
SMSS	Switching and Management Subsystem
SQN	Sequence Number
TACS	Total Access Comunications System
TDMA	Time Division Multiple Access
TMSI	Temporary Mobile Subscriber Identity
UI	User Interface
UMTS	Universal Mobile Telecommunications System
USIM	Universal SIM
UTRAN	UMTS Terrestrial Radio Access Network
VLR	Visitor Location Register

W-CDMA	Wideband CDMA
WiMAX	Worldwide Interoperability for Microwave Access

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: BAKALÁŘSKÁ PRÁCE NA CD

CD disk - obsahuje soubor BP_Janak_Daniel.pdf