Masarykova univerzita
Fakulta informatiky


# Bezpečnostné aspekty 5G sietí

Bakalárska práca

**Valentína Monková**

Brno, jar 2021

Masarykova univerzita
Fakulta informatiky


# Bezpečnostné aspekty 5G sietí

Bakalárska práca

**Valentína Monková**

Brno, jar 2021

*Na tomto mieste sa v tlačenej práci nachádza oficiálne podpísané zadanie práce a vyhlásenie autora školského diela.*

# Vyhlásenie

Vyhlasujem, že táto bakalárska práca je mojím pôvodným autorským dielom, ktoré som vypracovala samostatne. Všetky zdroje, pramene a literatúru, ktoré som pri vypracovaní používala alebo z nich čerpala, v práci riadne citujem s uvedením úplného odkazu na príslušný zdroj.

Valentína Monková

**Vedúci práce:** Mgr. et Mgr. Jan Krhovják, Ph.D.

# Poďakovanie

Ďakujem svojmu vedúcemu, Mgr. et Mgr. Janovi Krhovjákovi, Ph.D., za odborné vedenie, rady a pripomienky, ktoré mi pomohli pri tvorbe tejto práce. Ďakujem tiež svojmu priateľovi, rodine a kamarátom za podporu a rady pri štúdiu a písaní práce.

# Zhrnutie

Práca sa v úvode zaoberá rekapituláciou bezpečnostných vlastností mobilných telekomunikačných sietí. Ďalej sa zameriava a dôkladne mapuje bezpečnostné aspekty a dopady novozavedených mobilných sietí piatej generácie (5G). Postupne cieli a analyzuje bezpečnostné požiadavky kladené na samotné siete a na mobilné terminály. Následne opisuje bezpečnostné vlastnosti ako autenticita, integrita, dôveryhodnosť v tzv. circuit-switched doméne, ale aj bezpečnostné vlastnosti v packet-switched doméne. V prípade mobilných sietí sa práca venuje bezpečnostným problémom, ktoré sú spôsobené danými protokolmi (v rámci danej generácie). Poukazuje aj na zbytočnú zložitosť niektorých týchto komunikačných protokolov. V prípade mobilných zariadení sa koncentruje na útoky spôsobené útočníkom s tzv. falošnou základovou stanicou.

# Kľúčové slová

5G, AKA, autentizácia, bezpečnosť, dôvernosť, integrita, LTE, mobilné siete, zachytávač IMSI

# Obsah

# 1 Úvod

Neustálym vývojom mobilných sietí a technológií sa zvyšujú aj obavy ľudí o bezpečnosť na internete. V roku 2019 začalo postupné nasadzovanie mobilných sietí piatej generácie a s nimi sa objavilo aj množstvo nových útokov a problémov. Niektoré útoky sú známe už zopár rokov a niektoré sa objavili s príchodom tejto generácie sietí.

Moja práca predstavuje základné vlastnosti sietí, ich postupný vývoj, venuje sa bezpečnostným vlastnostiam v daných doménach so zameraním na útoky s vytvorením falošnej základovej stanice. Vytvára prehľad hlavne všetkých nedostatkov a problémov. V úvode sa práca venuje prehľadu a rekapitulácii jednotlivých generácií sietí. Následne sa zameriava na novonasadené siete piatej generácie. Poukazuje aj na nové nedostatky a útoky spojené s touto generáciou ale aj na nové metódy a štandardy. Popisuje autentizačné protokoly, šifry a množstvo známych útokov. Cieľom práce bolo vytvoriť základný prehľad technológií a problémov, útokov v mobilných sieťach so zameraním na autentizáciu, šifrovacie algoritmy, útoky s falošnou základovou stanicou a zachytávače IMSI.

V prvej kapitole kapitole práce som sa venovala rekapitulácii postupného vývoja mobilných sietí. Od prvej generácie až po najnovšiu piatu generáciu. Zameriavala som sa primárne na dôležité štandardy, zlepšenie a nový prínos, bezpečnostné funkcie a služby v každej generácii. Následne popisujem v druhej kapitole proces autentizácie v packet-switched a circuit-switched doménach s primárnym zameraním na komplikovanosť daných autentizačných protokolov a na ich nedostatky. Šifrovacie algoritmy, dôvernosť, integritu a opäť raz problémy a možné útoky v týchto oblastiach popisujem následne v štvrtej kapitole. Piata kapitola je súhrnný opis útokov zameraných na vytvorenie falošnej stanice a následnej zachytávanie unikátneho čísla predplatiteľa. Posledná kapitola rekapituluje celý prehľad a mapovanie vybraných bezpečnostných oblastí.

# 2 Vývoj mobilných sietí

Celý vývoj mobilných sietí sa delí do takzvaných generácií (1G–5G), podľa toho kedy boli uvedené do funkčnosti a podľa toho, čo nové priniesli. Mobilné siete jednotlivých generácií sú založené na bezdrátových bunkových technológiách. Bunková alebo mobilná sieť je rádiová sieť rozložená do buniek, vysielače v danej oblasti majú svoj dosah a tým vytvárajú bunku. Dosah daného vysielača v bunke sa prekrýva s ostatnými dosahmi buniek a spolu tieto bunky vytvárajú akúsi oblasť, ktorá je pokrytá signálom. Každá bunka má aspoň jednu fixnú základovú stanicu, ktorá ju obsluhuje a riadi a zároveň spravidla využíva iné frekvencie oproti bunkám v určitej vzdialenosti aby nedochádzalo k narušovaniu prenosu medzi jednotlivými bunkami [53, 11].

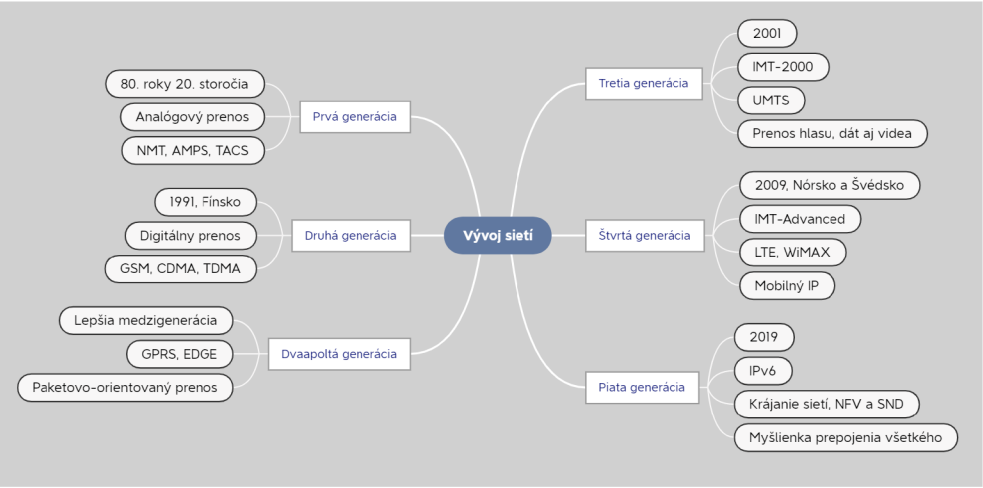
V nasledujúcich kapitolách sa predpokladá, že čitateľ pozná základy prenosových technológií na úrovni popísanej napríklad v knihe Wireless Communications & Networks [60] či obdobnej publikácii.

## 2.1 Prvá generácia (1G)

Prvá generácia mobilných sietí bola založená na štandarde analógového prenosu. Táto generácia sietí bola predstavená v 80. rokoch. Analógové systémy boli štandardy založené na technológií prepínania obvodov. Jediné služby v tejto generácii súviseli s prenosom reči, avšak tento prenos mal veľmi nízku kompatibilitu medzi viacerými zariadeniami. S využitím techniky FDMA (Frequency Division Multiple Access), bol hlasový hovor modulovaný na 150 MHz a potom sa prenášal medzi rádiovými vežami.

Prvá generácia sa bezpečnosťou vôbec nezaoberala, bola takmer nulová. Ktokoľvek s minimálnymi znalosťami a prístupom k celému pásmu dokázal odpočúvať akúkoľvek konverzáciu. Najväčším problémom bola krádež vysielacieho času.

Používané štandardy boli napríklad: NMT (Nordic Mobile Telephone), ktorý sa používal prevažne v škandinávských krajinách, Švajčiarsku, Holandsku, východnej Európe a Rusku, AMPS (Advanced Mobile Phone System), ktorý sa používal v Spojených štátoch a TACS (Total Access Communications System) v Spojenom kráľovstve [5, 53, 11].




Obr. 2.1: Vývoj mobilných sietí

## 2.2 Druhá generácia (2G)

2G je štandard, ktorý bol uvedený do behu v roku 1991 vo Fínsku. Oproti prvej generácii bola táto generácia založená nie na analógovom ale digitálnom prenose. Najznámejšou technológiou druhej generácie bola GSM (Global System for Mobile Communication). Vývoj GSM sa začal už v roku 1982. Spolu s GSM sa využívali rozhrania TDMA (Time Division Multiple Access) a CDMA (Code Division Multiple Access). Čo sa týka služieb, druhá generácia pokračovala v rozvoji služieb prvej generácie, orientovala sa na zlepšenie hlasových služieb, taktiež priniesla začiatky posielania krátkych správ, funkciu hlasových schránok, faxov a MMS (Multimedia Messages). Jedným z najväčších prínosom 2G bola možnosť využitia spektra viacerými používateľmi, čo sa dosiahlo pomocou efektívnejšej práce s prenosovým spektrom.

Oproti prvej generácii poskytuje druhá generácia aspoň minimálnu ochranu. Medzi mobilným telefónom a základovou stanicou sa zaviedlo digitálne šifrovanie mobilných konverzácií, avšak nie nutne v zvyšku siete [5, 53, 11].

### 2.2.1 Dvaapoltá generácia (2,5G)

S postupným napredovaním sietí sa zvyšovala aj potreba, aby siete boli rýchlejšie a lepšie, GSM siete už neboli dostatočne rýchle, preto vzinkali nové štandardy ako 2,5G. Dvaapoltá generácia je považovaná za prepojenie medzi druhou a treťou generáciou, oproti 2G má navyše aj paketovo orientovaný prenos dát. Dáta sa delia do paketov, ktoré ďalej putujú v sieti, nie je nutné vytvárať súvisle kanály pre prenos a príjem dát. Všeobecne známou technikou 2,5G sietí je GPRS (General Packet Ratio Services). V optimálnych podmienkach je možná maximálna rýchlosť prenosu dát s využitím GPRS až 160 kbps.

Ďalšou nadstavbou sietí druhej generácie po GPRS je EDGE (Enhanced Data Rates for GSM Evolution). Považuje sa za generáciu 2,75G, ktorá priniesla ďalšie možnosti a zlepšenie hlavne v oblasti rýchlosti prenosu dát. S využitím služby EDGE sa rýchlosť prenosu dát pohybuje až do 384 kbps. Táto je rýchlosť je umožnená vďaka 8PSK (Eight-Phase Shift Keying) [53, 11].

## 2.3 Tretia generácia (3G)

3G je generácia, ktorá ako prvá spĺňa štandardy IMT-2000 (International Mobile Telecommunications for the 2000). IMT-2000 je prvotná skupina štandardov vytvorená z IMT konceptu. IMT štandardy nie sú špecifické technológie, sú to špecifikácie a požiadavky na vysokorýchlostné mobilné širokopásmové pripojenie, definujú, ktoré vlastnosti a podmienky by mali byť splnené v príslušnom časovom rámci. Za využívanie IMT-2000 štandardov pri ponúkaní 3G mobilných služieb boli vydávané licencie daným operátorom po celom svete.

Je to štandard založený na širokopásmovej bezdrôtovej sieti, využíva paketovo orientovaný prenos dát, rovnako ako druhá generácia, a poskytuje bezdrátovú službu s rýchlosťami prenosu dát od 144 kbps až do 384 kbps.

V Českej republike sa prvé zakúpené licencie datujú na rok 2001, ktoré vydražili mobilní operátori Eurotel a Radiomobil [62].

Siete tretej generácie sa obdobne ako predchádzajúce dve zameriavajú hlavne na dátové služby. V 3G sa už objavila vysoká kvalita hlasových hovorov. Taktiež sa služby tejto generácie posunuli oveľa ďalej a priniesli nové funkcie ako: mobilná televízia, internetový prí-

stup, rýchlejší prenos dát, videohovory a rôzne ďalšie multimediálne služby.

UTMS (Universal Mobile Telecommunication Mobile System) je príkladom najlepšieho štandardu v tretej generácii. UMTS pochádza z Európy a v optimálnych podmienkach dosahuje rýchlosť až 1920 kbps. Hlavným cieľom UMTS je, aby sa 3G technológie využívané naprieč celým svetom s rôznymi obmenami dali spravovať z akéhokoľvek vzdialeného miesta. Toto je možné dosiahnuť využitím prepojených satelitov a pozemných sietí. S pomocou VHE (Virtual Home Enviroment) by zabezpečovali použitie 3G sietí aj v roamingu.

Hlavným zámerom bolo, aby dôverné informácie používateľov boli adekvátne chránené proti krádeži alebo zneužitiu. Medzi hlavné požiadavky, ktoré riešila a zabezpečovala tretia generácia patria: dôvernosť identity používateľov, dohodu pre autentizáciu a výmenu kľúčov, dôvernosť dát a ochranu integrity signalizačných správ. Často dochádzalo k sprenevere týchto citlivých informácií, práve preto, že domáca sieť, služby a zdroje poskytované príslušnou sieťou neboli dostatočne chránené. Tento problém sa riešil a medzi jednu z najužitočnejších zmien 3G sietí už patrí aj overenie, či je príslu3ná sieť autorizovaná voči domácemu prostrediu na začiatku a počas využívania siete. Výmena dát a citlivých informácií v sieti už musela byť chránená voči neautorizovaným zmenám. Používatelia mali možnosť overenia, či daná sieť je chránená v akomkoľvek okamihu používania siete, či už pri telefonovaní alebo pri prenose daných dôverných údajov o používateľovi [5, 53, 11, 67].

## 2.4 Štvrtá generácia (4G)

Štvrtá generácia sietí je následníkom skupín štandardov 2G a 3G. Dva najznámejšie štandardy, ktoré sa využívali v 4G sieťach, sú WiMAX (World Interoprability For Microwave Access) a LTE (Long Term Evolution). WiMAX je bezdrôtová technológia, prýkrát použitá v roku 2007 v Južnej Kórei. Je to architektúra, ktorá má slúžiť na vytváranie doplnkových a alternatívnych sietí. Podporuje väčšie rýchlosti na väčšie vzdialenosti pre väčší počet používateľov. Využíva sa taktiež na propagáciu vzájomnej spolupráce medzi produktami, napríklad od iných výrobcov, pokiaľ spĺňajú daný level certifikácie a profil. LTE pri-

niesla zrýchlenie 4G sietí, nepovažuje sa ale nutne za technológiu, ale skôr cestu, ktorá k tejto väčšej rýchlosti prenosu dát smerovala. Dnes už celosveto známy a využívaný štandard LTE bol prvýkrát komerčne predstavený v roku 2009 v Nórsku a Švédsku. Prvý štandard, ktorý rieši všetky funkcie ako prácu s dátami a nerozlišuje konkrétny typ dát. [57]. Signál LTE sa šíri vysielacími a prijímacími frekvenčnými pásmami. V Českej republike sú pre LTE pridelené pásma 1, 3, 7, 8 a 20 [56][1].

Oproti predchádzajúcim dvom generáciam, 4G podporuje technológiu celointernetového protokolu (all-Internet Protokol alebo IP), protokol založený na paketovo-orientovanom prenose. 4G predstavuje rôznorodú architektúru, ktorá využíva viacero rôznorodých bezdrátových sietí naraz a preto sa aj nazýva multi-systém. Hlavný zámerom tohto štandardu je bezproblémové odovzdanie v rámci prechodu viacerých sietí a garancia tej najlepšie mobility pre mobilné uzly [31].

Rýchlosť prenosu v 4G je až 100 Mbps pri pokrytí veľkej oblasti s vysokou mobilitou a až 1 Gbps pri optimálnych podmienkach v lokálnych sieťach. Práve preto, že prenos dát v tejto genrácii dosahuje až takéto vysoké hodnoty, posielanie obrovských dát medzi zariadeniami už vôbec nie je problém a stáva sa niečím úplne bežným a jednoduchým. 4G má väčšiu šírku pásma, vyššiu prenosovú rýchlosť, je plynulejšia a zabezpečuje rýchlejšie doručenie dát. Podobne ako 3G aj 4G musí spĺňať koncepty vydané ITU (International Telecommunication Union), pre túto generáciu boli vyvinuté štandardy nazývané IMT Advanced.

Jedným zo základnych nutností 4G bezdrátových systémov sa stáva prispôsobivosť. 4G prináša ešte lepšiu kvalitu služieb ako 3G, vďaka využitiu základných protokolových vrstiev. Prináša nové a zlepšené služby ako: mobilný prístup na webové stránky, IP telefónia, herné

1. Frekvenčné pásma alokované pre LTE sú rozlišné v každej krajine. Každé pásmo má pridelené svoje špecifické číslo, ktoré ho definuje. Napríklad pásmo 20, ktoré je pridelené aj Českej republike, je časť FDD (Frequency Division Duplex, duplex s frekvenčným delením) LTE pásma, to znamená, že potrebuje dva spárované samostatné pásma na simultánny prenos na dvoch frekvenciách. Toto pásmo má odlišné downlinkové (od siete k zariadeniu 791–821 MHz) a uplinkové (od zariadenia do siete 832–862 MHz) frekvencie, šírku pásma 30 MHz, duplexné rozostupy $-41MHz$ a pásmovú medzeru 71 MHz.

služby, mobilná televízia s vysokým rozlíšením, videokonferencie a 3D televízie.

Čo sa týka bezpečnosti, k zlepšeniu došlo v oblastiach prístupu k ineternetu z fixnej lokácie. V zaistení bezpečnosti pri pridaní nového zariadenia alebo aplikácií do 4G. Taktiež boli pridané unikátne identifikátory pri obojstrannej autentizácii kvôli zlepšeniu a vytvoreniu bezpečnejšej šifry ako v predchádzajúcich štandardoch [57].

## 2.5 Piata generácia (5G)

5G, alebo piata generácia mobilných sietí, je nasledovníkom štandardom 4G. Je to ďalší krok vo vývoji mobilných bezdrátových sietí. 5G je navrhnutá pre WWWW (World Wide Wireless Web) a využíva IP protokol rovnako ako 4G, avšak 5G využíva hlavne ďalšiu generáciu IP protokolu a to IPv6. Táto generácia má umožnovať pripojenie všetkého, či už sa jedná o stroje, objekty, zariadenia alebo čokoľvek iné, čo sa dá do takejto siete pripojiť, má umožniť úplne nový druh siete a nový pohľad na to, čo všetko môže spolu koexistovať v jednej sieti. Hlavnou myšlienkou je zjednotiť používateľskú skúsenosť všetkým používateľom, okrem toho by mala priniesť aj vyššiu rýchlosť, nižšiu latenciu, väčšiu spoľahlivosť, kapacitu siete a zvýšenú dostupnosť aj na odľahlejšie miesta. Efektívnosť tejto generácie sietí pripojila nových používateľov a nové priemysly [63].

Začiatkom roku 2019 začalo predstavenie 5G sietí. V roku 2020 veľa krajín očakávalo celonárodné 5G mobilné siete, avšak tento rozvoj pozastavilo infekčné ochorenie COVID-19. Všetky veľké mobilné spoločnosti začali vyrábať nové mobilné zariadenia s podporou 5G, aby priniesli nové siete viacerým používateľom a sprístupnili nové možnosti a služby takmer všade a všetkým. 5G bola spustená už vo viac ako 35 krajinách, vrátane Českej republiky.

Všetky predošlé generácie sa zameriavali predovšetkým na zvýšenie rýchlosti mobilného širokopásmového pripojenia oproti tomu, čo bolo možné v predchádzajúcich generáciách. Avšak hlavným cieľom 5G nie je priniesť rýchlejšie siete, samozrejme to k tomu patrí, no zameriava sa hlavne na zjednotenie všetkých služieb. 5G má byť platforma, ktorá má spájať a sprostredkovávať nové služby, ale aj komunikáciu v kritických misiách a masívny internet vecí. 5G má prirodzene podpo-

rovať všetky typy spektier, pásiem, väčšinu modelov nasadenia a nové spôsoby vzájomného pripojenia ako zariadenie-zariadenie.

Technológií využitých na umožnenie 5G sietí je veľmi veľa, tie najzásadnejšie z nich sú technológie milimetrových vĺn, masívne MIMO (Multiple Input Multiple Output), technológia malých bunkových sietí, plný duplexný režim. Technológie milimetrových vĺn riešia problémy, ktoré vznikajú následkom toho, že dnes pri obrovskom počte zariadení sa frekvencie, ktoré tieto zariadenia využívajú, stávajú preplnené a prenášač nemôže prijať viac dát, takže začína dochádzať k spomaľovaniu zariadení a poklesu pripojenia. Riešením je práve rozšírenie šírky pásma, avšak tieto frekvencie mimo bežné pásmo sa oslabujú prechodom budov alebo ich pohltia aj rastliny. Práve preto je užitočná technológia malých bunkových sietí, ktorá fuguje na princípe využitia tisícok malých základových staníc, ktoré slúžia ako sprostredkovatelia signálu. Takže v prípade nejakej prekážky sa automaticky využije menšia základová stanica na prechod singálu v sieti. Masivné MIMO slúži na zlepšenie internetového prenosu. Táto technológia zlepšuje práve latenciu a robustnosť sietí. Plný duplexný režim je implementovanie spôsobu, ktorý využíva prenos dát v oboch smeroch na jednom prenášači v rovnakom čase, bez toho aby sa vzájomne rušili [51, 65].

Budúce 5G služby sa môžu rozvíjať do všetkých smerov, už teraz sa neustále objavuje enormný počet nových služieb, ako napríklad: hologramy, 360-stupňové videá, strojová komunikácia, inteligentná preprava a ďalšie. 5G sa môže ďalej zaoberať vylepšením nasledujúcich faktorov ako nové typy mobilných zariadení, udržateľné zdroje energie, neobmedzený prenos dát a obrovský počet aktívnych pripojení.

5G služby sú rozdelené podľa vlastností do nasledujúcich piatich kategórií.

1. Pohlcujúce 5G služby: teleprezencia, virtuálna/rozšírená realita (VR/AR), streamovanie masívneho obsahu

2. Inteligentné 5G služby: výpočty zamerané na používateľov, služby v preplnených oblastiach

3. Všadeprítomné 5G služby: Internet vecí

4. Autonómne 5G služby: teleoperácie, inteligentná preprava, drony, roboty

5. Verejné 5G služby: monitorovanie katastrof, verejná bezpečnosť (safety), súkromná bezpečnosť (security), pohotovostné služby [68]

Prvá mobilná architektúra, ktorá dokáže podporovať viaceré, špecifické prípady použitia, kde rôzne prípady použitia majú svoje unikátne kyberbezpečnostné požiadavky, je 5G. Dobrý spôsob, ako niečo takéto uskutočniť a zároveň znížiť bezpečnostné riziká, je segmentácia siete, tá je napríklad v zábavnom IT priemysle úplne bežná a využívaná.

Krájanie 5G sietí je rozdelenie jedného sieťového spojenia do viacerých, odlišných virtuálnych spojení, ktoré dokážu poskytnúť rozlišné množstvo zdrojov rozlišným typom sieťovej prevádzky. Na uskutočnenie tejto segmentácie siete sa využívajú technológie SDN (Software Defined Networking) a NFV (Network Functions Virtualization). SDN je nová inteligentná architektúra, ktorá umožňuje kontrolu údajov a separáciu preposielana dát pomocou externej komponenty nazývanej ovládač. SND poskytuje jednoduché abstrakcie pre všetky malé komponenty a funkcie, je umožnený vzájomný prístup medzi odlišnými časťami heterogénnych sietí. NFV je architekrúra, ktorá naopak slúži na virtualizáciu celého uzla siete a jeho funkcií.

Avšak aj napriek tomu s príchodom nových možností a všetkého, čo dokážu nové 5G siete, prichádzajú aj obavy o bezpečnosť týchto sietí a užívateľov. Najčastejšie a najviac diskutované problémy s príchodom 5G sietí sú napríklad: náhly nárast sieťovej prevádzky (v rovnaký moment sa prudko zvýši), bezpečnosť rádiových rozhraní (šifrovacie kľúče týchto rozhraní sa posielajú nezabezpečenými kanálmi), bezpečnosť pri roamingu (používateľské bezpečnostné požiadavky sa neaktualizujú počas roamingu), signalizačné búrky, odmietnutie služby na zariadeniach koncových používateľov a ďalšie [3, 61].

| Generácia | 1G | 2G | 3G | 4G | 5G |
|---|---|---|---|---|---|
| Frekvencia | 800-900 Mhz | 850 - 1900 MHz | 1.6 - 2.5 GHz | 2 - 8 GHz | 3 - 30 GHz |
| Šírka pásma | 1.9 kbps | 384 kbps | 2 Mbps | 2 Mbps - 1 Gbps | 1 Gbps a viac |
| Typ prepínania | Obvody | Obvody, Pakety | Obvody, Pakety | Pakety | Pakety |
| Multiplexing | FDMA | TDMA, CDMA | CDMA | CDMA | CDMA, MIMO |
| Služby | Analógový prenos | Digitálny prenos, vyššia kapacita | Vyššia kvalita dát, videa a hovoru | Dynamický prístup k dátam, nositeľné zariadenia, streamovanie v HD | Dynamický prístup k dátam, nositeľné zariadenia, streamovanie v HD, prepojenie všetkých zariadení, globálny roaming |

Obr. 2.2: Porovnanie generácií sietí

# 3 Autentizácia v sieťach

Autentizácia je proces overovania identity používateľa alebo informácie. Overuje, či niečo alebo niekto je to alebo ten/tá, za čo/koho sa vydáva. Hlavným cieľom autentizácie je povoliť prístup overeným používateľom alebo sieťam a zároveň zabrániť prístup neautorizovaným sieťam a užívateľom. Na autentizáciu v sieťach sa prevažne využívajú rozšírenia EAP (Extensible Authentication Protocol) protokolu alebo v novších generáciach EAP s kombináciou AKA (Authentication and Key Agreement) protokolu.

## 3.1 Circuit-switched doména

V starších generáciách sietí sa prevažne využívali verzie EAP. Je to autentizačný rámec, ktorý slúži na zabezpečenie prenosu dát a používanie parametrov a dát EAP metódami. EAP sa používa najčastejšie v bezdrátových sieťach. Je definovaný, aj všetky jeho rozšírenia, v RFC (Request for Comments) špecifikáciách, kde ma každé takéto rozšírenie svoje špecifické číslo, podľa ktorého je ho možné nájsť. EAP je definovaný v RFC 3748 a neskôr jeho novšia verzia ako RFC 5247.

### 5.1.1 EAP-SIM protokol

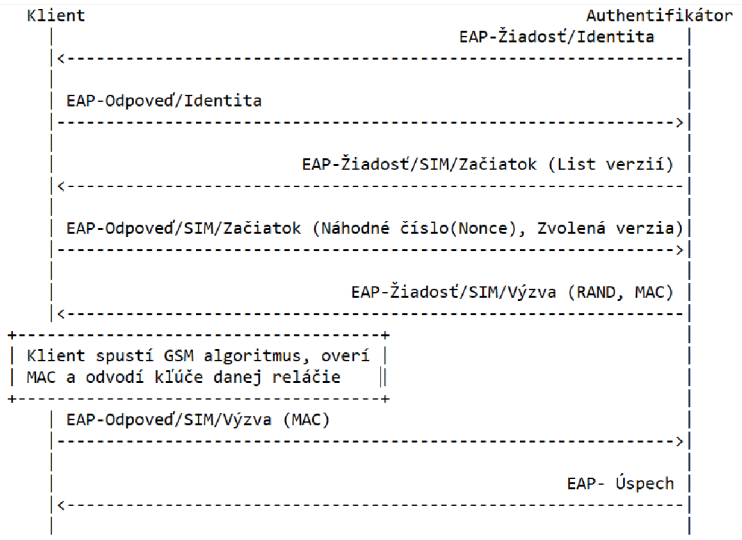
EAP-SIM (Extensible Authentication Protocol-Subscriber Identity Module) je jeden z prvých z rady EAP protokolov, podobne ako EAP-AKA. Slúži na autentizáciu medzi GSM (Global System for Mobile Communications) a danou WLAN (Wireless Local Area Network). Prepojenie týchto dvoch sietí umožnilo zlepšiť kvalitu GSM sietí a možnosť viacerých pripojených klientov v danej oblasti. GSM je mobilný štandard v druhej generácii sietí. Autentizácia v tomto protokole je založená na princípe výzva-odpoveď. EAP-SIM funguje na podobnom mechanizme ako autentizácia v GSM, avšak bola vylepšená, aby sa predošlo známym útokov v GSM sieťach. Jednou zo zmien je napríklad využitie až 128-bitového kľúča oproti 64-bitovému, ako tomu bolo v GSM. Obrovským krokom vpred bola aj vzájomná autentizácia, autentizovať iba klienta sa rýchlo ukázalo ako nedostačujúce.

Účastníkmi v EAP-SIM autentizácii sú mobilný klient, bezdrátový router, GSM sieť a AAA server. Prvým krokom je štandardne v takýchto protokoloch výzva-odpoveď o zaslanie a overenie identity. Odpoveď používateľa obsahuje buď jeho unikátne číslo IMSI (International Mobile Subscriber Identity) alebo pseudonym (napr. TMSI[1]). Nasleduje overenie parametrov SIM, kde server zasiela list možných verzií, ktoré podporuje, a klient následne zasiela vybranú verziu a náhodné číslo (nonce). Server zároveň obdrží *n* GSM trojíc. Tieto trojice získava kontaktovaním Autentifikáčného Centra, výhodou využitia tohto centra je to, že server a klient nepotrebujú vopred stanovené heslo. Z týchto trojíc server odvodí všetky dôležité informácie a kľúče. Server posiela novú výzvu, ktorá obsahuje niekoľko RAND výziev a všeobecný MAC, ktorý pokrýva dané výzvy. Klient následne spustí GSM algoritmus (je založený na autentizačných algoritmoch A3 a A8[2]), odvodí kľúče danej relácie (dané autentizačné trojice sa kombinujú na vytvorenie silnejších kľúčov relácie ako boli individuálne trojice) a vypočíta kópiu daného MAC kódu (ten sa počíta z náhodného čísla a EAP paketov, tieto pakety zapuzdrujú dané parametre vo formáte: typ, dĺžka, hodnota). Ak MAC hodnoty nie sú rovnaké, posiela chybovú hlášku. V opačnom prípade nasleduje poslanie MAC atribútu, ktorý pokrýva SRES. SRES je 32-bitová odpoveď, ktorá sa vytvára pomocou danej funkcie RAND a tajného kľúča uloženého na SIM karte využitím A3/A8 algoritmu. Server tento MAC overí, a ak je správny, posiela správu o uspešnej autentizácii [32].

### Slabiny EAP-SIM

Jedným zo závažných útokov na tento protokol je napríklad vydávanie sa za daný GSM server. Potrebné informácie na uskutočnenie tohto útoku môžeme získať napríklad obrdžaním SIM karty, z ktorej by sa dali zistiť potrebné trojice na vzájomnú autentizáciu alebo využitím

1. Temporary Mobile Subscriber Identifier je dočasný pseudonym, ktorý sa začal využívať na zlepšenie bezpečnosti už v GSM sieťach. TMSI je valídne iba v určitej oblasti a zasiela sa namiesto IMSI čísla. Avšak nebráni IMSI útokom, pretože je možné si dané IMSI číslo vyžiadať aj po zaslaní TMSI.
2. A3 a A8 sa v praxi implementujú spolu a vytvárajú A3/A8 algoritmus. Tento algoritmus je implementovaný na SIM karte a využíva sa v GSM autentizačnom protokole na vytvorenie SRES.




Obr. 3.1: Priebeh autentizácie v protokole EAP-SIM [32]

škodlivého softvéru. Ďalšou možnosťou na získanie týchto trojíc je aj využiť zraniteľnosti danej GSM siete hacknutím alebo aj zneužitie neexistujúcej počiatočnej autentizácie medzi AAA serverom a daným prístupovým bodom. Ak útočník nejakým spôsobom získa dané trojice, vie sa vydávať za GSM sieť, dostať sa do WLAN siete a získať ďalšie množstvo informácií. Daná falošná GSM sieť bude autentizovaná ako legitímna sieť, dokým sa nezmenia dané trojice, tie sa však menia vtedy keď sa mení kľúč, ktorý ich generuje, čo niekedy trvá aj zopár rokov [7, 32, 35].

### 5.1.2 EAP-AKA protokol

EAP-AKA (Extensible Authentication Protocol-Authentication and Key Agreement) sa využíva na autentizáciu uživaľeského zariadenia (UE) a Nie-3GPP (nie preto, lebo neboli špecifikované dané prístupy v 3GPP -The 3rd Generation Partnership Project) siete, ako napríklad WLAN (Wireless Local Area Network).

Funguje na princípe vzájomnej autentizácie a výmeny kľúča medzi 3GPP a Nie-3GPP, takže medzi UE a AAA serverom (Authentication,

Authorization and Accounting server). Prvým krokom je nadviazanie spojenia medzi UE a AP (Prístupový bod, Access Point). Nasleduje EAP výzva-odpoveď na zistenie identity zariadenia, buď vo forme IMSI čísla, alebo dočasnej identity. Server obrdží autentizačný vektor na overenie predplatiteľa. Po tomto kroku nasleduje EAP-AKA výzva-odpoveď na opakované zaslanie identity (zároveň klientovi posiela aj doplňujúce informácie ako unikátne jednorazové číslo, inicializačný vektor, MAC...), ktorá musí byť rovnaká, je to akási kontrola toho, či dané číslo nebolo zmenené počas výmeny. Následne AAA server overí, či sa používateľ môže pripojiť na danú WLAN (pomocou rozhrania HSS, Home Subscriber server) a zároveň si odvodí hlavný kľúč (MK), kľúč integrity (IK) a šifrovací kľúč (CK) z daného autentizačného vektora. Pokiaľ UE má prístup, nasleduje ďalšia výzva od AAA servera. Táto výzva obsahuje RAND funkciu, AUTN (autentizačný token) a MAC hodnotu (tento MAC kód pokrýva EAP pakety, slúži na ochranu daných EAP správ). UE potom overí, že token je správny a v správnom rozmedzí. Ak áno, generuje s využitím symetrického kľúča $K$ autentizačný výsledok (RES), kľúč integrity (IK) a šifrovací kľúč (CK). UE odpovedá poslaním RES a novej MAC hodnoty. Server následne porovná svoj vygerovaný autentizačný token XRES a MAC. Ak sú rovnaké, odvodí sa hlavný kľúč relácie (MSK), ten sa uloží do AP a slúži na ochranu pri ďalších komunikáciách.

### Zraniteľnosti EAP-AKA

Pri nadviazaní spojenia UE posiela IMSI v čistom texte, čo je klasický problém zachytenia IMSI a následného sledovania. Taktiež typ útokov man-in-the-middle, ako napríklad: zmena IMSI čísla útočníkom alebo pri posielaní MSK prístupovému bodu bez nejakého predchádzajúceho overenia, sa útočník môže vydávať za AP a potom tento kľúč zneužiť.

Veľkým problémom je aj využitie symetrickej kryptografie a rovnakého kľúča $K$ pre generovanie a šifrovanie všetkých ostatných kľúčov a čísel. Ak by bol tento kľúč prezradený, znamenalo by to vlastne odhalenie prenášaných hodnôt v EAP-AKA protokole [43, 8, 47].


Obr. 3.2: Priebeh autentizácie v protokole EAP-AKA [43]

## 3.2 Packet-switched doména

Čoraz viac ľudí využíva mobilné siete po celom svete a s tým rastie aj počet útokov na dané mobilné zariadenia a potreba chrániť súkromie mobilných používateľov. Najviac využívané sú stále siete štvrtej a tretej generácie, ktoré využívajú na autentizáciu AKA (Authentication and Key Agreement) protokol, o ktorom vieme, že nie je úplne bezpečný. AKA protokol bol navrhnutý skupinou 3GPP (3rd Generation Partnership Project) a má slúžiť na vzájomnú autentizáciu mobilného zariadenia, špecificky jeho USIM (Universal Subscriber Identity Module) karty a siete, ku ktorej sa snaží pripojiť. USIM karta je univerzálny identifikačný modul účastníka, oproti bežným SIM kartám poskytuje viac lepších služieb[3]. Existuje aj verzia AKA pre 5G siete [37]. Tieto protokoly fungujú na princípe výzva-odpoveď, sú založené na symmetrickej kryptografii s využitím náhodného sekvenčného čísla (SQN), ktoré zabraňuje hlavne opakovaným útokom.

Medzi najčastejšie využitie slabostí AKA protokolu sa považuje nechránený mechanizmus vyžiadania identity, s využitím napríklad medzinárodného zachytávača identity mobilného predplatiteľa (IMSI zachytávač), čo je telefónne odpočúvacie, ktoré slúži na zachytávanie prenosu z mobilného zariadenia a taktiež sa využíva aj na sledovanie polohy používateľov mobilných telefónov. Druhým veľkým problémom je aj získavanie súkromných informácií zo správ o zlyhaní autentifikácie. Nastal aspoň menší pokus o vyriešnie týchto známych problémov v AKA protokole pre 5G siete, v ktorom sa už zaviedlo náhodné asymetrické šifrovanie.

Avšak vyskytol sa ďalší a omnoho závažnejší typ útokov, ktorý dokonca dokáže aktívne monitorovať používateľa aj mimo rozsah falošnej stanice a dozvedieť sa množstvo súkromných informácií bez jeho vedenia. Ochranný mechanizmus využitím sekvenčného čísla nie je až tak nepreniknuteľný. Keďže na vytváranie tohto čísla sa využíva exkluzívny-OR (XOR) a nie veľká miera náhodnosti, pomocou špecifických opakovaných útokov sa dá táto ochrana prelomiť. Útočník potom vie efektívne odsledovať, kedy zariadenie opustilo danú oblasť

3. Oproti SIM umožňuje: viac kontaktov v telefónnom zozname vrátane emailov, iných mien, používa bezpečnejšie algoritmy: napríklad KASUMI (je popísaný v štvrtej kapitole), oproti SIM taktiež na šifrovanie hovorov a dát nasadzuje silnejšie kľúče, aplikuje vzájomnú autentizáciu, ... [66]

falošnej stanice alebo sa naučiť postupne jeho typické vzorce ako: kedy posiela správy alebo počet telefonátov v danom čase [14].

### 5.2.1 5G-AKA

Bunková sieť sa skláda väčšinou z troch hlavných častí, prvou a najdôležitejšou je uživateľské vybavenie (UE), čo zahŕňa predplatiteľov a ich mobilné zariadenia s USIM kartou. Každá USIM s kryptografickými schopnosťami uchováva aj unikátne číslo predplatiteľa IMSI v LTE-AKA protokole alebo trvalý identifikátor predplatného SUPI (Subscription Permanent Identifier) v 5G-AKA, unikátny a tajný kľúč $K$, ktorý sa využíva pri autentizácii s domácou sieťou a 48-bitové sekvenčné číslo. Ďalšou častou je spomínaná domáca sieť (HNs), ktorá slúži ako databáza na overovanie USIM kariet a ich používateľov v domácom prostredí. Avšak často sa uživateľské zariadenia ocitnú mimo oblasť svojej domáce siete, takže posledná komponenta je obsluhujúca sieť (SN), ku ktorej sa následne zariadenie pripája.

V momente, keď sa chce uživateľské vybavenie pripojiť k obsluhujúcej sieti, je nutné, aby bol vytvorený bezpečný kanál na komunikáciu alebo posielanie správ. Tento kanál sa vytvorí až po autentizácii zariadenia k jeho domácej sieti a autentizácii samotnej domácej siete. V 5G-AKA zariadenie a jeho domáca sieť medzi sebou zdieľajú tajný a unikátny kľúč a SUPI. Podobne ako predchádzajúce generácie AKA-protokolov, aj 5G využíva jednosmerné kryptografické funkcie, všetky využívajú tajný, unikátny klúč $K$ a používajú sa na zachovanie integrity a dôvernosti. Obrovským prínosom bolo využitie asymetrickej kryptografie, tá sa využíva na zabránenie odhalenia identity UE. V predchádazjúcich generáciách protokolu sa posielal identifikátor v čistom texte. Po úšpešnom priebehu protokolu domáca sieť dostáva novú globálnu dočasnú identitu GUTI (Globally Unique Temporary Identity) pre UE. Používa sa namiesto šifrovaného SUPI, pretože použitím GUTI sa vyhneme jednému asymetrickému šifrovaniu, avšak GUTI môže byť použité najviac raz, mení sa po každom použití. Realizácia AKA protokolu vyzerá takto:

1. UE sa identifikuje HN a tým spúšťa protokol. Identifikuje sa použitím dočasného GUTI alebo zaslaním asymetricky šifrovaného SUPI.

2. HN dešifruje správu a získava sekvenčné číslo domácej siete a kľúč $K$, ktorý je unikátny pre dané SUPI. HN vygeneruje nové jednorázové číslo $n$ a použitím kryptograficke funkcie $f^5$ ho zašifruje, toto číslo sa potom použitím XOR-u ďalej šifruje so sekvenčným číslom domácej siete ($SQN_N$). Následne pomocou inej funkcie $f^1$ zašifruje aj dvojicu $n$ a $SQN_N$. HN potom naspäť UE zasiela n-ticu (jednorázové číslo $n$, $SQN_N$ XOR $f^5(n)$, zašifrovanú dvojicu $n$ a $SQN_N$)

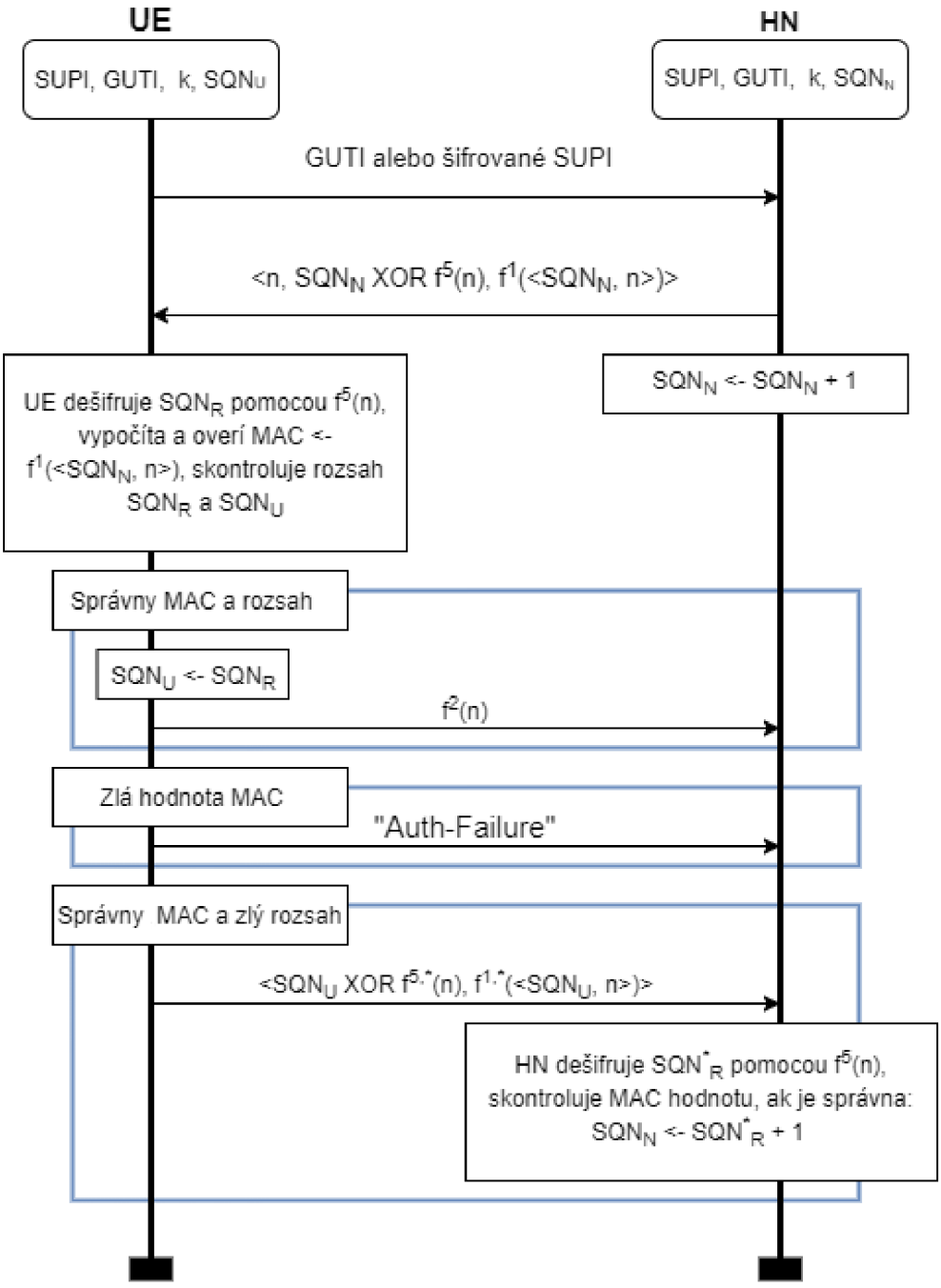
3. UE si po obdržaní čísla $n$, vytvorí znovu pomocou rovnakej funkcie $f^5$ zašifrované $n$ a to použije na dešifrovanie dočasného sekvenčného čísla $SQN_R$. Následne zopakuje posledný krok a zhotoví rovnakou kryptografickou funkciou $f^1$ dvojicu $n$ a $SQN_R$ a overí, že sa to rovná posledému číslu v n-tici od HN a zároveň či $SQN_R$ aj sekvenčné číslo používateľského zariadenia ($SQN_U$) sú v správnom rozmedzí. Ak áno, UE zmení $SQN_U$ na $SQN_R$ a posiela HN novou kryptografickou funkciou $f^2$ znovu zašifrované $n$, aby dokázalo svoju znalosť kľúča $K$. Ak sa to nepodarí, posiela sa správa o zlyhaní ("Auth-Failure").

4. Ďalším krokom je re-synchronizácia, kde UE zašifruje $SQN_U$ XOR-ovaním so zašifrovaným $n$, na šifrovanie $n$ sa použila funkcia $f^{5,*}$. Následne sa táto správa ešte overí MAC (message authentication code) funkciou. Taktiež sa podobne ako v prvom kroku vytvorí zašifrovaná dvojica $SQN_U$ a $n$ použitím jednomernej funkcie $f^{1,*}$. Následne HN dešifruje $SQN_R^*$ a skontroluje MAC. Ak sa overenie úspešne podarí, tak HN zmení hodnotu $SQN_R^*$ na $SQN_U + 1$. Tento proces slúži na posunutie sekvenčného čísla, aby sa nachádzalo v správnych hraniciach pri následnej prvej správe ďalšieho priebehu 5G-AKA protokolu.

5. Posledným krokom je vygenerovania novej dočasnej identity GUTI, ktorú si domáca sieť uloží a spojí s daným zariadením v databázi. Čerstvé GUTI následne zamaskuje a posiela UE.

### 5.2.2 Známe útoky na AKA protokoly

Väčšinu z týchto útokov poznáme už z predchádzajúcich generácií AKA. Bolo pridaných niekoľko úprav týchto chýb a známych útokov,




Obr. 3.3: Priebeh autentizácie v protokole 5G-AKA [37]

avšak stále aj v 5G-AKA je množstvo slabín, ktoré sa dajú využívať na získavanie súkromných informácií. Podľa 3GPP špecifikácií by mal kanál medzi domácou sieťou a obsluhujúcou sieťou zabezpečovať dôvernosť, integritu, autentizáciu a ochranu pred opakovaným útokom. Avšak kanál medzi zariadením a obsluhujúcou sieťou je bezdrôtový a práve preto často predmetom rôznych útokov škodlivých tretích strán. Domáca sieť je pre dané zariadenia dôveryhodná, avšak to nie nutne platí pre obsluhujúcu sieť, práve preto musí prebiehať vzájomná autentizácia, na overenie identity či už siete alebo zariadenia a na zabezpečenie následnej komunikácie medzi zariadením a sieťou. Avšak protokoly na túto autentizáciu bývajú často chybové. Obsahujú slabosti, ktoré sa dajú využiť. Aby sa takýmto útokom zabránilo, pridáva sa do daných protokolov nová funkcionalita, avšak často nie dostatočná a autentizačné protokoly sa tak stávajú viac komplikovanými a stále rovnako zraniteľnými.

### Zachytávač IMSI

Všetky predchádzajúce verzie AKA až na 5G-AKA sú zraniteľné voči tomuto útoku, ktorý sa považuje za jeden z najviac bežných a najľahšie uskutočniteľných. Je založený na tom, že medzinárodná identita mobilného účastníka (IMSI) sa nijako nešifruje, posiela sa v čistom texte. Je možné získavať permanentnú identitu užívateľského zariadenia a podľa toho potom získavať informácie o danom používateľovi. Je potrebné na tento útok ale mať vlastnú základnú stanicu, čo bolo v minulosti problematické, avšak teraz je to možné s takmer bežným vybavením [42].

### Útoky na zistenie polohy zariadenia

Tieto útoky zväčša fungujú v dvoch fázach. V prvej útočník odpočúva úspešný priebeh autentizácie medzi domácou sieťou a zariadením. Pri tomto odpočúvaní si uloží autentizačnú správu, ktorú posiela domáca sieť. V druhej fáze sa už útočník snaží využiť danú odpočutú informáciu.

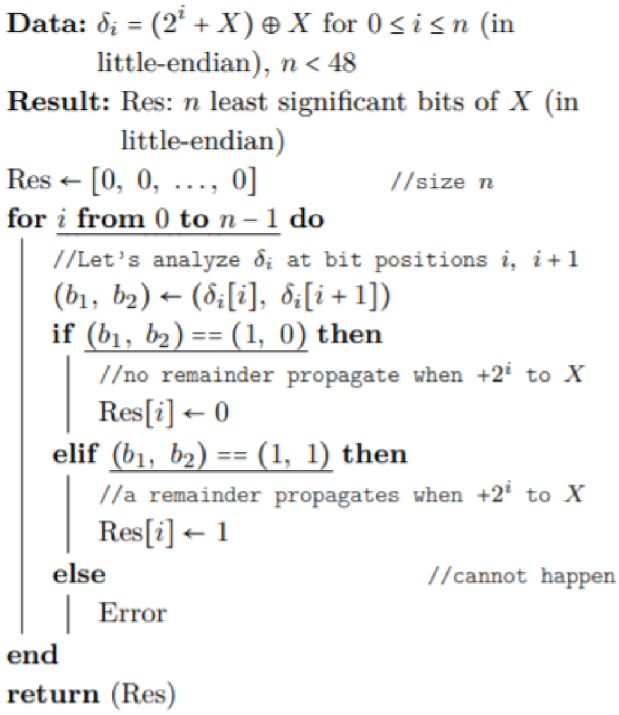
Napríklad na zistenie polohy mobilnej stanice konkrétnej obete. Útočník cielene odpočúva prvý beh protokolu. Zamerá sa v tomto prípade hlavne na autentizačnú výzvu (RAND, AUTN). Túto informáciu

si uloží a následne postupne simuluje nový beh protokolu v rôznych oblastiach. Ak dané zariadenie nie je hľadané mobilné zariadenie danej obete, dostane správu o zlyhaní MAC, ak je, tak odpoveďou bude re-synchronizačná správa, pretože MAC test uspel ale test rozsahu už nie. Práve tým, že odpoveď pri nepodarení danej autentizácie je v každom prípade iná, vieme presne určiť polohu mobilnej stanice. Takže s využitím a postavením zopár falošných staníc by sa dal sledovať konkrétny pohyb daného zariadenia. Čo popiera bezpečnostnú požiadavku nevystopovateľnosti v sieti.

Taktiež ďalším ohrozením je aj útok, ktorý využíva na sledovanie polohy šifrované IMSI číslo. V prvej fáze rovnako odpočúva úspešný priebeh protokolu, avšak teraz si uloží šifrované IMSI číslo. To využije na sledovanie tak, že vždy keď chce zistiť či dané zariadenie je to zariadenie, ktorého zašifrované IMSI si uložil, preruší priebeh protokolu a namiesto šifrovaného IMSI, ktoré malo posielať zariadenie, pošle to svoje uložené a tým dokáže zistiť, či je to to isté zariadenie. Ak to nie sú rovnaké zariadenia, dostane správu o zlyhaní, ak sú rovnaké, dostane správu o úspešnej autentizácii. Avšak IMSI číslo sa šifruje vždy inak, nestačí si raz zašifrované IMSI číslo uložiť a následne ho sledovať. Mení sa každým použitím.

#### Prelomenie sekvenčného čísla

Tento útok je založený na už predošlom zistení identity daného zariadenia, či už trvalej, dočasnej alebo zašifrovanej. Po úspešnom odchytení identity je útočník taktiež schopný zistiť niekoľko najmenej významných bitov sekvenčného čísla domácej siete. Prvým krokom pri tomto útoku je vygenerovanie a uloženie $2^n + 2$ úspešných, nových autentizačných výziev pre dané cielené mobilné zariadenie. To je možné až po identifikácii a práve preto potrebujeme dopredu zistiť aspoň jednu identitu zariadenia. Následne danému mobilnému zariadeniu spustí všetky tieto výzvy. Pre zariadenie sú všetky tieto výzvy valídne a nové. Po prvej úspešnej výzve útočník zašle znovu prvú výzvu (v prvom behu je to tá istá, ale kontrola na novosť už neprejde, pretože sa sekvenčné číslo po predchádzajúcej výzve zvýšilo o jedna) aby navodil zlyhanie synchronizácie. Následne pošle ďalšiu novú výzvu, ktorá opäť bude úspešná, aby aj zariadenie aktualizovalo svoje sekvenčné číslo. Po tejto úspešnej výzve opäť opakujeme



**Data:** $\delta_i = (2^i + X) \oplus X$ for $0 \leq i \leq n$ (in little-endian), $n < 48$
**Result:** Res: $n$ least significant bits of $X$ (in little-endian)
Res $\leftarrow [0,\ 0,\ \ldots,\ 0]$ //size $n$
**for** $i$ **from** $0$ **to** $n-1$ **do**
  //Let's analyze $\delta_i$ at bit positions $i,\ i+1$
  $(b_1,\ b_2) \leftarrow (\delta_i[i],\ \delta_i[i+1])$
  **if** $(b_1,\ b_2) == (1,\ 0)$ **then**
    //no remainder propagate when $+2^i$ to $X$
    Res$[i] \leftarrow 0$
  **elif** $(b_1,\ b_2) == (1,\ 1)$ **then**
    //a remainder propagates when $+2^i$ to $X$
    Res$[i] \leftarrow 1$
  **else** //cannot happen
    Error
**end**
**return** (Res)

Obr. 3.4: Algoritmus na zistenie sekvenčného čísla z kolekcie dát [14]

iniciálnu výzvu za účelom neúspechu. Postupne pokračujeme pre všetky výzvy. Po dokončení poslednej výzvy vezmeme všetky výsledky ($2^n + 2$ vygenerovaných autentizačných správ), ktoré zároveň tvoria aj vstup algoritmu, ktorý spočíta niekoľko posledných bitov sekvenčného čísla. Myšlienka daného algoritmu je analýza šíriacich sa zvyškov po daných výzvach. Vstup $\delta_i$ predstavuje 48 bitov posladaných z autentizačných správ a hodnoty X (pole 48 bitov, hodnota iniciálneho sekvenčného čísla domácej siete zvýšenej o číslo 1) v kódovaní little-endian. Postupne algoritmus prechádza hodnoty dvoch susediacich bitov z $\delta_i$ a podľa hodnôt daných bitov vytvára postupnosť najmenej významných bitov sekvenčného čísla domácej siete. Tento algoritmus je následne možné vykonávať na zozbieraných dátach aj offline [37, 14, 34].

# 4 Dôvernosť a integrita v sieťach

Dôvernosť znamená, že zdroje, objekty a dáta sú chránené pred neautorizovanými prístupmi. Jej cieľom je to, aby iba autorizované osoby mali prístup k daným informáciám. Je to pojem, ktorý sa využíva najmä v organizáciách pri riadení bezpečnosti. V praxi sa toto uplatňuje prostredníctvom delenia právomocí, najlepšie je využiť princíp najnižšieho privilégia. Princíp založený na tom, že každý modul má právo pristupovať len k informáciám, ktoré nevyhnutne potrebuje k splneniu svojho zámeru.

Integrita je pojem, ktorý vyjadruje, že dáta alebo dané informácie neboli neautorizovane zmenené. Zabezpečuje sa tak, že tieto informácie sú spoľahlivé a správne. Nežiadúca zmena dát nemusí byť vždy úmyselná, no o to viac škôd môže spôsobiť, ak nie je dostatočne včas odhalená. Preto je vhodné sledovať zmeny dát, aby bolo jasné, či sa stala nejaká takáto chyba a kto ju spôsobil, aby sa predošlo budúcim problémom.

## 4.1 Circuit-switched doména

Kvôli zvýšenému dopytu po aplikáciách založených na reči a celkovému pokroku v oblasti vývoja sieti sa kladie aj väčší dôraz na oblasť bezpečnosti. Za účelom zabezpečiť, aby informácie neboli zverejnené alebo neoprávnene zmenené pri prenose reči nezabezpečenými kanálmi, vznikli šifrovacie algoritmy.

V GSM sieťach sa prvoplánovo autentizoval iba telefón danej základovej stanici, no stanica sa už naspäť neautentizovala. Stačí si vytvoriť falošnú stanicu, ku ktorej sa pripojí obeť a keďže stanica vyberá šifrovací algoritmus, ktorý sa na danú komunikáciu použije, môže ho rovno vypnúť a všetky informácie dostane v čistom texte. Telefón by mal upozorniť na tento útok, avšak v danej dobe obsahovala SIM karta bit, ktorým sa dala deaktivovať táto výstraha. Bol to algoritmus nazývaný A5/0 [29].

Následne sa začali využívať algoritmy A5/1 a A5/2. A5/1 je šifra, ktorá sa používala vo väčšine európskych krajinách na zabezpečenie vzájomnej rečovej komunikácie tiež v GSM. V ostatných častiach sveta sa používal algoritmus A5/2. Využíva 64-bitový kľúč a 22-bitové číslo,

ktoré je verejne známe. Tento 64-bitový kľúč sa v oboch šifrách derivuje ako súčasť autentizácie na SIM karte. Konverzácia v tomto algoritme sa prenáša v rámcoch. Každý rámec sa využitím funkcie XOR šifruje so sekvenciou, ktorú vytvára generátor bežiaceho kľúča (running-key generator).

A5/1 kombinuje 3 posúvne registre s lineárnou spätnou väzbou (Linear Feedback Shift Register)[1]. Všetky tieto registre fungujú na taktovacom algoritme, ktorý sa počíta v každom kroku. Rozhodnutie o taktovaní je založené na jednom bite z každého registra. Dané bity sa podľa určitých parametrov v každom kroku vyberú a následne sú vybrané dané registre, kde sa vyskytoval tento bit vo väčšine, dva alebo tri registre sú následne taktované [12, 15].

Táto šifra bola prelomená prvýkrát R. Andersonom v roku 1994, odhalilo sa množstvo slabostí daného algoritmu a poznáme množstvo útokov na túto šifru. Častý útok na túto šifru je hrubou silou, kde sa útočník pokúša náhodne uhádnúť obsah prvých dvoch registrov a následne podľa kľúčového prúdu zistiť obsah tretieho registra. Takéto skúmanie nám následne odhalí vnútorný stav šifry a kľúč danej relácie. Využíva hárdvér ako COPACOBANA (Cost-Optimized Parallel COde Breaker) [18], čo je mechanizmus optimalizovaný na beh kryptoanalytických algoritmov [6, 27, 38].

Ďalším častým útokom je Time-Memory Trade-Off (TMTO) útok[2]. Na tento útok je tiež vhodné využiť hardvér ako COPACOBANA, alebo implementovať vlastné pole malých nezávislých procesových jednotiek. Každá z týchto jednotiek následne počíta jeden riadok v danej TMTO tabuľke. Takýmto postupných počítaním a generovaním je možné získať úspešne a s celkom dobrou pravdepodobnosťou kľúč danej relácie behom pár minút. v tomto konkrétnom útoku sa využíva metódy tenkých dúhových tabuliek a rozlišujúcich bodov (distinguished points) [30, 38].

---

1. LFSR je register, ktorého výstup je lineárne závislý na predchádzajúcich výstupoch a stavoch. Používa sa najčastejšie ako generátor pseudonáhodnych čísiel [16]
2. Time-memory trade-off je technika, ktorá slúži na prelamovanie rôznych šifier a systémov v reálnom čase v praxi. Základné metódy TMTO sú: kryptoanalýza pomocou Hellmanových tabuliek a kryptoanalýza pomocou dúhových tabuliek. Tieto metódy kombinujú akési dva rôzne mechanizmy prelamovania šifier a to: mechanizmus útokov hrubou silou, prechádzaním cez takmer všetky možnosti a hľadaním v už vopred pripravenej tabuľke údajov [30, 40].

Známymi útokmi na šifrovací algoritmus A5/1 či A5/2 sú aj algebraické útoky. Základnú techniku týchto útokov prvýkrát predstavili N. T. Courtois a W. Meier [19]. Metóda týchto útokov má štyri základné kroky:

- Nájdenie systému nezávislých algebraických rovníc, ktoré budú spájať počiatočný stav s kľúčovým prúsom, ktorý je viditeľný počas útoku.
- Zmenšenie stupňa daných rovníc, čím menší stupeň rovníc, tým lepšie a ľahšie na vyriešenie.
- Hromadenie a zbieranie dostatočného počtu bitov kľúčového prúdu na dosadenie do rovníc.
- Vyriešenie danýc algebraických rovníc.

Týmto postupom si vygenerujeme systém rovníc pre lineárne registre a následne vyriešením získáme kľúč danej relácie. Často sa avšak stanovuje aj akási horná hranica stupňa daných rovníc pre rýchlejší algebraický útok [19, 33, 52].

A5/2 bola odzačiatku považovaná za slabšiu šifru, obe využívajú rovnaký kľúč a fungujú takmer rovnako. A5/2 využíva až štyri registre s lineárnou spätnou väzbou. Taktovanie prvých troch registrov je kontrolované štvrtým. V tomto algoritme sa vyberajú bity pre taktovací algoritmus iba zo štvrtého registra. Práve preto sa tento algoritmus považuje za slabší, akonáhle zistíme iniciálny stav štvrtého registra, doážeme zistiť takmer všetko. Obe tieto verzie, A5/1 aj A5/2 sa dajú prelomiť v reálnom čase. Medzi najväčšie slabosti patrí malá veľkosť tajného kľúča alebo málo možností iniciálneho stavu. A5/2 sa už v sieťach nevyskytuje [52, 24].

## 4.2 Packet-switched doména

V packet-switched doméne nasleduje nasadenie A5/3 blokovej šifry nazývanej KASUMI. Je vytvorená modifikovaním verzie MISTY kryptosystému[3], konkrétne zjedodušením kľúčového rozvrhu a upravením

3. MISTY1 je bloková šifra, ktorá bola navrhnutá v roku 1995 M. Matsuim. Je dizajnovaná tak, aby sa nedala prelomiť diferenciálnou a lineárnou kryptoanalýzou.

niektorých komponent. Touto zmenou sa KASUMI šifra stala dokonca slabšou ako pôvodná MISTY a preto bola v roku 2010 prelomená pri špecifických podmienkach. Kombinuje viacero metód: metóda príbuzných kľúčov, bumerangová metóda, ... Pri danom útoku sa skúmajú kvartety textu zašifrovaného štyrmi diferenciálne príbuznými, ale rozdielnými kľúčmi [13]. Avšak tieto podmienky sa dosahujú pri bežnom používaní tejto šifry veľmi zložito a preto tento útok na A5/3 nie je možné aplikovať. Šifra A5/4 sa tiež nazýva KASUMI a oproti predchádzajúcej verzii sa namiesto 64-bitovej dĺžky kľúča používa 128-bitová. KASUMI sa využíva v štandardoch ako UMTS, GSM a GPRS. v UTMS sú na tejto šifre založené kryptografické funkcie na dôvernosť a integritu. Daný inicializačný vektor pre túto šifru zasiela AAA serve pri opakovanej žiadosti na zaslanie identity [23, 29, 50].

V ďalších generáciách sietí sa objavuje nová šifra SNOW. SNOW 3G je slovne orientovaná šifra, ktorá generuje sekvencie 32-bitových slov. SNOW 3G sa skladá z posúvneho registra s lineárnou spätnou väzbou a nekonečného stavového automatu. Tento register je zložený zo šestnástich stavov a každý tento stav obsahuje 32 bitov. Stavový automat je zložený z 3 registrov. Do týchto registrov sa v počiatočnej fáze uloží šifrovací klúč a inicializačný vektor (nazýva sa aj nonce, akési jednorázové unikátne číslo, v 5G-AKA ho generuje už spomínaná HN). Celý tento šifrovací algoritmus funguje v dvoch režimoch, v inicializačnom a následne v režime, ktorý slúži na generáciu kľúčového prúdu. Algoritmus sa využíva aj v sieťach štvrtej (LTE) či piatej generácie a sú na nej taktiež založené kryptografické funkcie pre dôvernosť a integritu. Nahradila tak v týchto funkciách KASUMI šifru. Dosiaľ táto šifra nebola prelomená [45].

V packet-switched doméne sa taktiež vyskytuje množstvo rôznych útokov využívajúcich nedostatky rôznych častí služieb a protokolov a tým porušujú základné bezpečnostné požiadavky v oblasti integrity a dôvernosti. Takýmito útokmi sú napr. ReVolte útok, útok na IMSI pomocou VoWi-Fi či aLTEr útok a podobne.

---

Dokáže realizovať vysokorýchlostné šifrovanie na hardvérových aj softvérových prostrediach [49].

### ReVoLTE útok

Ešte stále sa v enormnom počte na mobilnú komunikáciu využíva v sieťach štandard LTE (Long Term Evolution). Oproti vyšším rýchlostiam, ako v predchádzajúcich generáciách, poskytuje aj službu VoLTE (Voice over LTE). VoLTE je štandard pre bezdrôtovú komunikáciu pre mobilné telefóny, terminály, zariadenia Internetu Vecí (IoT) a taktiež aj pre nositeľné doplnky, ako inteligentné hodinky a podobne. Tento štandard implementovali takmer všetci poskytovatelia telekomunikácií po celom svete.

Nedávno sa však objavilo množstvo úspešných útokov na VoLTE, a keďže je používaný takmer celosvetovo, môže ovplyvniť veľký počet ľudí. Útok, ktorý dokáže obnoviť zašifrovanú VoLTE komunikáciu a odpočúvať ju. Nazýva sa ReVoLTE a využíva to, že kľúčový prúd je predvídateľný. Kľúčový prúd je akýsi tok pseudonáhodných znakov, tieto znaky sa spájajú so správami v obyčajnom texte a výstupom je zašifrovaný text. Avšak využívajú sa práve pseudonáhodne znaky, ktoré sa dajú predvídať a útočník s takmer minimálnimi zdrojmi dokáže takýto útok zinscenovať a odpočúvať. Čo je veľký zásah do súkromia daných používateľov. Video názornej ukážky [4].

Úspešné vytvorenie VoLTE komunikácie zabežpečujú hlavne niektoré dôležité komponenty z LTE sietí. Medzi tieto zložkou je používateľské zariadenie (UE), základová stanica v LTE sieťach (eNodeB), Vyvinuté jadro paketu (EPC) a IP Multimediálny Podsystém (IMS). EPC je rámec, ktorý slúži na autentifikáciu a dohodu o kľúči, riadenie mobility, smeruje dopravu na používateľskej rovine ku správnej paketovej dátovej sieti, čo je napríklad v tomto útoku IMS a hlavne jeho funkcia, ktorá spravuje prichádzajúce a odchádzajúce VoLTE telefonáty.

VoLTE využíva na vytváranie hlasových telefonátov a videohovorov paketovú LTE a modifikované IP protokoly. Patria tam protokoly ako protokol o začatí relácie (SIP), protokol na prenos dát v reálnom čase (RTP) a protokol na kontrolu RTP pripojenia (RTCP). Cieľom úspešného útoku je práve dešifrovať tieto RTP pakety a ich obsah. Na prenos hlasových údajov medzi základovou stanicou a UE VoLTE využíva priradený nosič. Práve tento nosič slúži na prepravu RTP balíkov.

---

4. `https://www.youtube.com/watch?v=FiiELuFvwu0`

Vždy pri pripojení UE do základovej stanice by sa pre rádiové pripojenie mal vytvárať nový kľúč. Avšak keď priebehajú dva VoLTE rozhovory v rámci jedného rádiového spojenia, dochádza k takzvanému znovupoužitiu daného kľúčového prúdu. Čo znamená, že prvý hovor (cieľový hovor) aj druhý hovor (kľúčový hovor) sú šifrované rovnako. Túto informáciu o znovupoužití potom môže útočník následne využiť na získanie kľúčového prúdu z druhého telefonátu a ten potom aplikuje funkciu XOR na odpočúvaný text z prvého telefonátu.

Na to, aby útočník dokázal zachytiť daný rozhovor, stačí dostupný hardvér (aspoň jedno komerčné mobilné zariadenie, notebook na ovládanie downlinkového odpočúvača a daný dowlinkový odpočúvač (napríklad Ettus USRP B210 [25])) a aspoň minimálna znalosť ako odpočúvať downlinkový prenos v rádiovej vrstve. Na to sa využíva downlinkový odpočúvač (downlink sinffer) a konfiguráciu danej eNodeB stanice. Pri druhom telefonáte je taktiež nutná znalosť pozície danej obete, jej/jeho telefonné číslo a komerčný telefón. Dôležité je aj to, aby sa kľúčový nasledujúci útok odohrával tesne po tom iniciálnom. Na zistenie, kedy skončil prvý hovor, aby útočník mohol vykonať druhý, sa využije taktiež spomínaný downlikový odpočúvač, ktorý dokáže zasielať informácie práve o tom, či ešte stále prebieha prvý telefonát sledovaním dedikovaného nosiča. Práve kvôli tomu, že nastavenie hovoru je rovnaké, časové rozmedzie minimálne, využíva sa rovnaké rádiové pripojenie, sa obnoví počet dedikovaných nosičov, čo vyústi v rovnaké vstupné parametre ako v prvotnom hovore. To znamená, že aj kľúčový prúd bude rovnaky a všetky RTP dátove pakety budú zašifrované rovnako. Hneď potom, čo nazbiera dostatočný počet dát, môže takýto hovor ukončiť, pretože má všetko potrebné na odpočúvanie tohto telefonátu.

V realite zaleží aj na tom, koľko poskytovateľov využíva nesprávnu implementáciu a aký veľký majú títo poskytovatelia rozsah svojich staníc. Z prieskumu 15 eNodeB až u 12 možných staníc sa dá tento útok zrealizovať, pretože využívalo znovupoužitie kľúčového prúdu. LTE síce využíva na šifrovanie bezpečné algoritmy (SNOW, AES (Advanced Encryption Standard) [20], ...), avšak GSM siete ponúkajú šifrovacie algoritmy ako A5/1 a A5/2. A5/1 nie je dostačujúca a dá sa aj napriek jej existencii odpočúvať konverzácie (ako ukazuje tento útok). Práve v miestach, kde poskytovatelia nepodporujú VoLTE, sa stále využívajú GSM rozhovory [55].

Väčšími detailami, rôznymi útokmi, špecifikáciami a bezpečnostnými aspektami LTE sa už zaoberala diplomová práca [39].

### Zachytávač IMSI pre VoWi-Fi

V oblastiach so zlým signálom je zložité vyhnúť sa prerušeným hovorom, miestam bez signálu či zložitým prepojením do inej siete. Na vyriešenie týchto problémov sa začalo využívať Voice over Wi-Fi (VoWi-Fi). VoWi-Fi umožnňuje namiesto uskutočnenia hovoru pomocou siete daného používateľa uskutočniť tento telefonát pomocou Wi-Fi siete. Dokonca uskutoční tento rozhovor s rovnakým telefónnym číslom a bez akejkoľvek potreby inej aplikácie.

VoWi-Fi architektúra je zložená z užívateľského zariadenia (UE), rádiovej prístupovej siete (RAN) a vyvinutým jádrom paketu (EPC). Pod RAN spadá aj prístupový bod a ten sa stará o rádiový signál a komunikáciu medzi zariadením a EPC. EPC je základný rámec pre riadenie hlasových služieb v LTE. Na podporu Wi-Fi hovorov a na vytvorenie akejsi brány medzi internetom a EPC sa však začala používať vyvinutá paketová dátová brána (Evolved Packet Data Gateway, ePDG). Je zodpovedná najmä za autentizáciu daným UE v sieti.

Na zabezpečenie dôvernosti a integrity v týchto Wi-Fi hovoroch sa využívajú dva protokoly Internet KeyExchange (IKEv2) a IP Security (IPSec). Spolu tieto protokoly vytvárajú virtuálnu súkromnú sieť (Virtual Private Network, VPN). VPN protokol slúži na zabezpečené sifrované pripojenie medzi dvomi sieťami alebo medzi používateľom a sieťou. Avšak tieto protokoly sa navyužívajú aj pri výmene IMSI čísla počas autentizácie a tak je možné získavať IMSI pomocou Man-in-the-middle útoku.

Man in the middle (MITM) je veľmi známy typ útoku, kde útočník tajne ovláda komunikáciu medzi dvomi zariadeniami. Odpočúva správy, mení ich, alebo ich nahradzuje inými správami bez vedomia daných používateľov, ktorý sa snažia o komunikáciu na sieti. Ich cieľom je získať skutočné dáta, ktoré sú zasielané medzi dvomi koncovými zariadeniami a tie následné využiť vo svoj prospech. To porušuje dôveryhodnosť a integritu daného rozhovoru na sieti, pričom komunikanti veria v to, že ich výmena informácií je bezpečná [17].

Objavujú sa MITM útoky na zistenie IMSI čísla cez Wi-Fi. Tieto útoky začínajú odpočúvaním Wi-Fi komunikácie a telefonátov daného

cieľového zariadenia. Na tento útok potrebujeme v dohľadnej vzdialenosti od cieľa umiestniť falošný prístupový bod s falošným IPSec serverom. Potom čo sa cieľ pripojí k prístupovému bodu je možné zachytávať a manipulovať so všetkými jeho dátovými paketmi. Následne útočník obrdží IP adresu a číslo portu z daného používateľského ePDG. Následne prebieha postupná výmena kľúčov a autentizácia v EAP-AKA, už spomínaná v predchádzajúcej kapitole. Zaiadenie posiela zašifrované IMSI, avšak to si útočník dešifruje veľmi ľahko kľúčami, ktoré sám vygeneroval pre túto reláciu [9, 48].

### Útok aLTEr

Častým diskutovaným útokom nie len v už známych 4G sieťach, ale aj novonasadzovaných 5G sieťach, je práve spomínaný aLTEr útok. Tento útok využíva techniku Man-in-the-middle, a to, že používateľské dáta v LTE sa v niektorých prenosových kanáloch síce šifrujú, no nie je zabezpečená ich integrita. Je možné tieto dáta modifikovať bez vedomia obete a následne ich využiť vo svoj prospech či vytvoriť úplne nové dáta a vydávať sa za obeť.

Manipulovať s dátami v šifrovanom kanáli je trochu zložitejšie, pretože útočník musí meniť obsah správ tak, aby po dešifrovaní mali požadovaný obsah. Toto je možné vykonávať vďaka tomu, že útočník pozná nezašifrovanú časť správ, s ktorými chce komunikovať. Cieľom útoku je DNS (Domain Name System) spoofing. To znamená, že tento domenový server vráti nesprávny záznam výsledku, konkrétne IP adresu. Hlavnou úlohou DNS je preklad doménových mien a IP adries.

Na začiatku útoku sa komerčné zariadenie pripojí a autentizuje do siete AKA protokolom. Následne sa snaží vyvolať DNS požiadavku (napr. navštívenie webovej adresy). Túto požiadavku zašifruje a posiela tento paket konkrétnemu DNS serveru pomocou pôvodnej IP adresy. Útočník následne túto komunikáciu preruší, rozozná DNS pakety a pomocou maskovania zmení pôvodnú IP adresu na adresu falošného DNS servera. Následne sa táto pozmenená požiadavka posiela do komerčnej siete. Sieť túto požiadavku dešifruje a posiela nie na pôvodný DNS server, ale ten falošný. Taktiež sa maskuje aj downlinkové spojenie, aby pôvodná IP adresa bola rovnaká ako cieľová pre

daný paket a komunikácia ostala nezistená. Takto môžme následne používateľov presmerovať na falošné a škodlivé stránky [54].

# 5 Útoky s tzv. falošnou základovou stanicou

Mobilné siete nie sú vôbec tak bezpečné ako si ľudia myslia. Častokrát majú ľudia strach sprístupniť nejakej aplikácii informácie o polohe svojho mobilného zariadenia, to však nevedia, že ak by niekto ich polohu zistiť chcel, tak to dokáže aj bez ich súhlasu. Jedným z najväčších problémov v sieťach ešte stále sú zachytávače IMSI (International Mobile Subscriber Identities).

IMSI je pätnásťmiestne číslo, ktoré pri pripájaní a autentizovaní do akejkoľvek siete jednoznačne definuje používateľa. Dostáva ho klient od svojho operátora a je pridelené k SIM karte. Toto číslo sa skladá z troch dôležitých častí

- trojmiestny mobilný kód krajiny (Mobile Country Code)[1]
- dvoj alebo trojmiestny mobilný sieťový kód (Mobile Network Code)[2]
- posledných 9 až 10 číslic je už konkrétna mobilná identita používateľa (Mobile Subscriber Identity).

Zachytávače IMSI sú sledovacie zariadenia, ktoré poukazujú a využívajú nedostatky v autentizácii, a to má za následok nežiadúce účinky či už na dôveryhodnosť mobilných operátorov alebo komunikačné služby. Znižujú dôveru ľudí, pretože nedokážu ochrániť ich súkromie v sieťach. Rádiové zariadenie, ktoré je schopné zachytávať tieto IMSI čísla, je navrhnuté so špecialnými funkciami, ktoré mu umožňujú odpočúvať komunikáciu mobilných zariadení. Zachytávač IMSI sa dokáže prejaviť ako falošná základová stanica, aby využila nedokonalosti v 2G/GSM, 3G/UMTS, 4G/LTE a 5G sieťach. Práve tým tieto aktívne útoky porušujú jednu z dôležitých podmienok definovanú v medzinárodných požiadavkách na ochranu súkromia, a to nevysledovateľnosť používateľa. Tieto zachytávače IMSI využívajú známy spôsob útoku, man-in-the-middle [4].

---

1. Pre Česko je to číslo 230, pre Slovensko zase 231, kde prvá dvojka v oboch číslach značí Európu.
2. Toto čísla sa už špeciálne rozlišuje podľa operátora v Česku je pre kód 01 vyhradený operátor T-Mobile, na Slovensku pre Orange.

Na zostrojenie takéhoto útoku, napríklad kvôli odpočúvaniu telekomunikácie konkrétnej osoby, útočník nepotrebuje žiadne programovacie schopnosti. Stačí mu základné komerčné vybavenie a použiť program, ktorý už existuje, a ktorý nie je potrebné nijako upravovať. Existuje množstvo open-source softvérových projektov, vymenovaných nižšie, z ktorých sa dá tento kód použiť. Avšak po úspešnom zachytení je potrebné túto komunikáciu aj dešifrovať (aké šifry sa používajú v ktorej generácii je popísané v úvode tejto kapitoly). Najjednoduchším riešením je prinútiť dané 3G/4G/5G zariadenie aby využilo GSM protokol. V tomto protokole nie je nutná vzájomná autentizácia a využitá šifra sa dá jednoducho prelomiť, no to nie je nutné keďže šifrovanie výmeny dát v 2G/3G/4G je voliteľné a je možné ho vypnúť. Obdobne sa dá docieliť aj DoS útok, za rovnakých podmienok[3].

Avšak nejde len o odpočúvanie komunikácie, útočník pomocou tohto prístroja dokáže zistiť veľmi veľa súkromných informácií, je schopný napríklad:

- nahrávať a odpočúvať konverzácie,
- rovnako sledovať SMS správy a preposielať ich inam ako boli určené,
- určiť polohu daného mobilného zariadenia,
- získať súbory z daného telefónu, vrátane fotiek,
- zapnúť mikrofón, kameru a iné aplikácie.
- posielať operátorom správy o rekonfigurácii telefónu (inštalovanie permanentneého MITM útoku)
- prerušiť dvojfaktorovú autentizáciu

3. Po nastavení falošných staníc a pokusu zariadenia o pripojenie, počas ktorého neustále posiela svoje IMSI číslo, nasleduje odmietnutie žiadosti o pripojenie. Keďže stanice toto IMSI číslo nepoznajú a berú ho ako ilegálne zariadenie, čo vyústi v úvahu, že daná sieť je nedostupná, až dokým nenastane reštart zariadenia. Ak sa bude UE neustále vypínať a zapínať a podvodné stanice budú stále vysielať signál, zariadeniu sa nikdy nepodarí pripojiť na akúkoľvek bunku. Toto spôsobí kontrolovaný DoS útok na cielenú sieť v danej oblasti [42].

Pri úvodnom pripájaní používateľského zariadenia (UE) do siete prebieha procedúra na výber výberu buniek. To je systém, kde si UE vyberá, ktorá je pre ňu vhodná a ponúka najlepšie služby. Ak nájde neskôr vhodnejšiu, tak sa prepojí, nastava opätovný výber bunky. UE sa pripája podľa lokálne uloženého zoznamu a kritérií, z ktorých vyberá, pri znovu pripojení sa najčastejšie pripojí opäť na sieť v rovnakej lokácii, kde bolo pripojené predtým, nemusí to byť nutne domáca sieť, často ide o úplne odlišného operátora. Pre úspešný útok je nutné vytvoriť takú eNodeB stanicu, ktorá bude spĺnať najviac kritérií, častokrát iba umiestnenie falošnej stanice v blízkosti daného zariadenia nestačí.

## 5.1 Potrebný hardvér

Na uskutočnenie tohto útoku je potrebné základné hardvérové vybavenie, napríklad: dva počítače s portami USB3, tieto porty sú dôležité na pripojenie nosiča softvéru, ktorý sa využije, dva univerzálne softvérové rádiové pripojenia a aspoň jedno mobilné zariadenie. Cena tohto hardvérového vybavenia je takmer minimálna a mnoho z týchto zariadení sa používa denne a sú prístupné takmer komukoľvek a kdekoľvek.

V tomto útoku sa konkrétne využili dva počítače, oba bežiace na 64-bitovom Kubuntu s jadrom s nízkou latenciou a s pripojenými perifériami, oba kompatibilné s daným softvérom. Tri mobilné zariadenia, jedno na nájdenie LTE pásiem a získanie informácií na vytvorenie následných falošných staníc. Zvyšné dva mobilné zariadenia na testovanie daného IMSI zachytávača. Následne sa využili USIM karty od cielených operátorov. Približná cena tohto konkrétneho hardvéru bola 300€. Avšak očakáva sa, že cena zariadenia potrebného na tento útok bude neustále klesať.

**Univerzálne softvérové rádiové zariadenie** (**Universal Software Radio Peripheral, USRP**) umožňuje navrhovať a implementovať výkonné a flexibilné softvérové rádiové systémy, ktoré dokážu následne fungovať na vysokých frekvenciách vo všetkých LTE frekvenčných pásmach. V tomto útoku sa využilo B200mini od spoločnosti Ettus Research. B200mini má byť lacnejšie zariadenie, ktoré bolo vyvinuté pre účely univerzít, laboratórií a nadšencov. Taktiež podporuje široký

rozsah frekvencií (70MHz-6GHz), tým pokrýva všetky frekvenčné pásma či už v GSM, UMTS alebo LTE. B200mini je praktické, veľmi malé a ľahko prenositeľné (na napájanie stačí prenosná batéria) vo veľkosi platobnej karty. Na toto zariadenie sú pripojené dve antény, jedna slúži na vysielanie aj prijímanie signálu a druhá iba na prijímanie [25].

## 5.2 Potrebný softvér

Tento kokrétny útok má za cieľ použiť dostupné softvéry, ktoré nebudú vyžadovať žiadnu či takmer minimálnu zmenu na vykonanie daného útoku, ako demonštráciu aký veľký problém tieto útoky sú.

Poznáme viac softvérov, ktorými je možné simulovať LTE sieť za účelom testovania či vývoju nových technológií. Napríklad srsLTE, openLTE či OpenAirInterface. Tieto testovacie sofvéry väčšinou simulujú jedno či viacero používateľských zariadení, jednu základovú stanicu a vyvinuté paketové jadro. Najznámejší OAI podporu najviac funkcií pre LTE siete, ktoré sú využiteľné na Linuxových počítačových zariadeniach. Na využívanie tohto softvéru je potrebné bežne dostupné laboratórne zariadenie. OpenLTE oproti OAI funguje prevažne iba so zariadením (USRP) od spoločnosti Ettus, podporuje menej funkcií (nepodporuje obsluhujúce brány, SGw). Kód openLTE je dobre organizovaný a dokumentovaný, avšak stále nie je úplne dokončený, množstvo funkcionalít je nestálych, neposkytuje používateľské zariadenie. Kód OAI je komplexnejší a funguje bez chýb či komplikácií, no je ťažšie si tento kód upraviť či využiť iba časť z neho. Softvér srsLTE sa zameral na kód, ktorý bude ľahko znovupoužiteľný a modifikovateľný. Poporuje aj simuláciu uživateľského zariadenia, funguje najlepšie so zariadením od Ettus, no je možné ho využiť aj s iným zariadením, oproti OAI poskytuje aj funkciu LTE downlikového odpočúvača. Napriek tomu OAI stále poskytuje viac funkcií ako srsLTE [28].

V konkrétne tomto útoku sa využil OpenAirInterface, pretože funguje na bežných zariadeniach a poskytuje najviac možností, tento open-source softvér slúži na implementáciu 3GPP bunkových sietí. Simuluje hlavné jadro (EPC) a prístupovej siete (EUTRAN), je vhodné simulovať tieto siete zvlášť na jednotlivých počítačoch, avšak je možné

simuláciu uskutočniť aj na jednom počítači pre minimálizáciu nákladov.

Následne sa v tomto útoku využíjú servisné a testovacie režimy mobilných zariadení, na získanie potrebných informácií o konkrétnych LTE sieťach. V niektorých zariadeniach sú tieto režimy dostupné bežne zavolaním na číslo *#0011# (Samsung) alebo *#*#4636#*#* (Android telefóny).

Na prípadné testovanie sa taktiež využíva ďalší open-source softvér OpenBTS, nie je nutný. Je možné pomocou daného IMSI čísla, ktoré sa zhoduje s nejakým regulárnym výrazom, pristupovať k sieti. Využíva sa sotvér pre GSM siete, pretože nemajú obojstrannú autentizáciu.

## 5.3 Priebeh aktívneho útoku na IMSI v LTE

Na simulovanie eNodeB základovej stanice sa využije počítač a USPR bude fungovať ako rádiová platforma. Pomocou softvéru OAI budú vytvorené a konfigurované dve podvodné základové stanice eNodeB. Prvá bude figurovať ako rušička, ktorej funkciou je, aby sa dané zariadenie odpojilo od momentálnej siete a pripojila sa k ďalšej vytvorenej falošnej stanici. Rušička funguje na rovnakej a zároveň najvyššej frekvencii ako daná komerčná eNodeB, čo má za následok ich vzájomné rušenie. Druhá stanice vystupuje ako autorizovaná stanica s druhou najvyššou frekvenciou a vysiela MCC a MNC siete daného cieľového mobilného operátora. Keďže rušička blokuje najvyššiu frekvenciu, mobilné zariadenie sa bude snažiť pripojiť na stanicu s druhou najvyššou prioritou, bude sa pripájať na vopred pripravenú druhú falošnú stanicu. Všetky tieto podmienky zabezpečujú, aby sa zariadenie podľa daných priorít pripojilo práve na túto podvodnú stanicu. Postup ako prebieha opätovný výber stanice je popísaný vyššie. Je však dôležité, aby sa druhá stanica vytvorila skôr ako rušička, keďže by sa zariadenie mohlo pripojiť do inej bunky kvôli rušeniu na najvyššej frekvencii a žiadnej inej stanici na vysokej priorite.

**Prvá fáza**

- Mobilné zariadenie sa využije na pripojenie k pôvodnej sieti a zistí jej sledovací smerový kód (Tracking Area Code, TAC)

a EARFCN (EUTRA Absolute Radio-Frequency Channel Number) využitím daných servisných režimov a konkrétnym volaním týchto čísiel. TAC označuje konkrétnu oblasť, niekoľko buniek v rovnakej oblasti spolu tvoria daný kód. EARFCN slúži na dizajnovanie frekvencie (uplink a downlink) a identifikáciu daných kanálov v pásme. Na útok potrebujeme nepoužitú frekvenciu a tú nám práve zabezpečí zistenie EARFCN.

- Nasleduje nastavenie prvej stanice (rušičky), pomocou MCC a MNC a získanej EARFCN.

- Pokračuje znovu-výber stanice a získanie a uloženie pôvodného EARFCN.

**Druhá fáza**

- Nastavenie a spustenie druhej stanice pomocou MCC, MNC, získanej EARFCN a iného TAC kódu ako v prvej fáze.

- Opätovné nastavenie EARFCN na pôvodnú hodnotu získanú mobilným zariadením a pomocou MCC, MNC spustenie prvej stanice (rušičky).

Zariadenie sa prepojí na našu druhú základovú stanicu a pri Žiadosti o identitu zašle svoje IMSI číslo behom niekoľkých sekúnd. Sledovaním a porovnávaním informačných správ v danej oblasti vieme určovať najvyššie priority v daných frekvenčných pásmach, a podľa toho vybrať tie najvhodnejšie pre dve určené falošné stanice a tým zabezpečiť, že sa cielené zariadenie pripojí na konkrétnu základovú stanicu a ku konkrétnej generácii siete. Rušenie rádiového signálu je najjednoduchšia metóda, ako blokovať 3G/4G/5G siete pomocou ich frekvencií a donútiť tým dané cielené zariadenie aby využilo 2G sieť. Toto môžme v podstate donekonečne opakovať a získavať tak množstvo IMSI čísel, čo má veľký dopad na dôveru a spoľahlivosť komerčných sietí [42, 59, 21].

Okrem aktívneho útoku na zachytávanie IMSI čísel existuje aj pasívny. Pasívny útok iba čaká a odpočúva na danej sieti a zachytáva všetky IMSI čísla, nešpecifikuje sa na žiadne konkrétne, iba získava čo

môže. Oblasť pokrytia takéhoto zachytávača IMSI, ak je dobre usmiestnený (napríklad na vrchole vysokej budovy) a útočník má dosť dobré technické vybavenie, môže byť až taká veľká ako oblasť normálnej bunkovej siete. Na takéto odpočúvanie sa využíva sieť antén alebo štruktúra s využitím mobilných zariadení. Avšak typ tohto pasívneho útoku je veľmi pomalý, keďže útočník musí čakať na moment, keď sa bude IMSI číslo posielať spontánne, a to sa deje vo veľmi špecifických a málo pravdepodobných situáciach vo väčšine oblastí (výnimkou sú letiská) [46].

V 5G sieťach je stále možnosť získavať tieto IMSI čísla, avšak už nie je možný pasívny zber IMSI čísel. Potom čo sa UE autentizuje, obsluhujúca sieť mu priradí dočasnú identitu, GUTI (táto dočasná identita nemá nič spoločné s TMSI).. Autentizácia sa navyše deje cez bezpečný kanál, aby bola zaistená integrita a dôvera danej výmeny. Následne zariadenie toto GUTI používa na svoju identifikáciu. Keďže UE následne všade využíva GUTI namiesto IMSI čísla, nie je možné ich iba pasívne odpočúvať. Avšak aktívny downgrade útok (útok, ktorý využíva mechanizmy zo starších generácii aby sa vyhli novým, bezpečným postupom) je stále možný, pretože siete neustále podporujú aj štandardy nižších generácií, ktoré sa spolu snažia koexistovať, a aj mobilné zariadenia musia podporovať viac vecí naraz. GUTI poskytuje dobrú a bezpečnú ochranu v 5G, avšak pokiaľ existuje podpora starších generácií, tak je možnosť z dôvodu spätnej kompatibility vynútiť za určitých okolností zaslanie IMSI čísla. Tento stav však s časom a zánikom 3G/4G vymizne a k takýmto útokom už nebude dochádzať [36].

## 5.4 Zachytávač zachytávača IMSI

Vykonanie takéhoto IMSI útoku je jednoduché a nepotrebujeme obsiahle znalosti. Práve preto sa začali objavovať opatrenia proti týmto útokom, zachytávače zachytávača IMSI (IMSI Catcher Catcher, ICC). Tieto zariadenia detektujú tieto útoky a chránia bezpečnosť používateľov.

Jednou z možných techník je napríklad využitie statických jednotiek v špecifickej geografickej oblasti, ktoré neustále merajú a skenujú frekvenčné pásma. Zameriavajú sa na zvláštné a odlišné oznámenie či odtlačky sieťových parametrov daných podvodných staníc. Každá

základová stanica má aj akýsi zoznam podporovaných funkcií, ak útočník neskopíruje správne všetky dané funckie, falošná stanica nebude ponúkať rovnaké služby ako pôvodná. Napríklad GPRS a EDGE sú komplikovanejšie služby, ktoré typicky zachytávače IMSI neimplementujú. Častým problémom je napríklad neznalosť šifrovacích kľúčov (3G, 4G) alebo nepublikovaný šifrovací GPRS algoritmus.

Ďalšou technikou je bežná aplikácia, dostupná pre všetkých používateľov. Pri tejto možnosti sa využíva najmä všestranný vstavaný prijímač GPS v dnešných komerčných telefónoch a možnosť snímania odtlačkov v bunkových sieťach. Tento prijímač pracuje pre okolie telefónu tak, že sa naučí danú štruktúru siete a následne ju dokáže kedykoľvek porovnať oproti naučeným dátam a zistiť či nedošlo k nejakej zmene.

Podrobnejší výskum a implementácia týchto zachytávačov zachytávačov IMSI [21].

# 6 Zhrnutie

Cieľom mojej práce bolo analyzovať a preskúmať bezpečnostné aspekty nových sietí piatej generácie a tak vytvoriť súhrnný prehľad problémov a útokov v rôznych menších oblastiach tejto generácie.

Zameriavala som sa primárne na postupný vývoj a útoky, ktoré sa objavovali už v predošlých generáciách a naďalej sa objavujú aj v nasledujúcich. Následne na autentizačné protokoly a upozorňovala som na ich neodstatky, možné útoky a taktiež na zbytočnú zložitosť, ktorá všetko len zbytočne zhoršuje. Zaujímala som sa aj o dôvernosť a integritu v sieťach, jedny z dôležitých aspektov pri komunikácii v sieti. Existuje množstvo útokov, ktoré tieto základné bezpečnostné vlastnosti porušujú aj v novej generácii sietí. Hlavné zameranie mojej práce tvorili konkrétne IMSI útoky, vytvorením falošnej základovej stanice, ktoré sú známe už veľmi dlho a zatiaľ sa im nedá zabrániť ani v 5G. Avšak po zániku 3G/4G sietí už tieto útoky na zbieranie IMSI čísel nebudú možné, GUTI bude predstavovať bezpečnú ochranu pred týmito útokmi.

Na základe všetkých týchto informácií a útokov sa mi podarilo vytvoriť výslednú rešerš nedostatkov v novonasadzovanej generácii so zameraním na jednotlivé vybrané oblasti a tým poukázať na nedostatočnú bezpečnostnú ochranu v sieťach.

Generácia týchto sietí je pomerne nová, začala sa nasadzovať približne pred dvomi rokmi. Ďalším prínosom tejto práce by mohlo byť testovanie a skúmanie týchto útokov na sieťach piatej generácie v Českej republike. Čoskoro sa táto generácie sietí rozšíri do rôznych oblastí aj v tejto krajine, a bolo by vhodné otestovať reálne problémy konkrétne na sieťach, ktoré sú nasadzované českými operátormi a poskytovateľmi tejto 5G siete.

Piata generácia je veľmi mladá a využíva nové technológie a protokoly, je možné, že sa postupne objavia nové doposiaľ nepoznané útoky, ktoré by bolo potrebné preskúmať a tým rozsíriť túto rešerš o nové útoky, poznatky a reálne fungovanie v krajinách či prípadné nedostatky v nasadzovaní operátormi vo svete.

# A Zachytávače IMSI v praxi

Zachytávače IMSI sa využívajú veľmi často aj v praxi v rôznych odvetviach. Častokrát tieto bezpečnostné chyby v sieťach využívajú firmy na produkciou týchto zachytávačov, alebo dokonca aj štátne zložky. Prvé komerčné IMSI zachytávače sa začali vyrábať už v roku 1996 nemeckou spoločnosťou Rohde & Schwarz. Zopár zachytávač IMSI bolo vytvorených už zopár rokov skôr, no boli príliš veľké, ťažké a drahé [21].

Najznámejšou spoločnosťou, ktorá vyrába a komerčne predáva sledovače telefónov, je L3Harris Technologies. Patrí medzi prvé firmy, ktoré vytvorili tieto zachytávače pre vojenské služby či štátne a právne agentúry [64, 26]. Ďalšie firmy, ktoré vytvárajú a inkasujú na využívaní chýb v sieťach, sú napr. Digital Receiver Technology (zariadenie DRTBOX, „dirtbox“), Meganet Corporation (VME Dominator, toto zariadenie dokonca umožňuje manipuláciu hlasových hovorov, blokovanie frekvenčných kanálov, modifikáciu textu a konkrétne hľadanie používateľov monitorovaním jeho telefonátov), Septier či PKI (tieto zariadenia už využívali rušenie signálu a nútenie 3G zariadení, aby sa pripájali na špecifické GSM frekvencie) [1, 41, 58, 22].

The Gamma Group dokonca v roku 2003 vytvorili zachytávače IMSI, ktoré sa mali nosiť na tele, avšak mali slúžiť iba na zachytávanie IMSI. Na pokročilejšie odpočúvanie už boli potrebné ďalšie zariadenia od tejto spoločnosti[2].

Od roku 2010 už bolo možné vytvoriť si vlastné IMSI zachytávače v domácom prostedí. Prvýkrát túto možnosť demonštroval Chris Paget, cena tohto zariadenia vyšla na približne 1500$ a bolo zložené z softvérového definovaného rádia, dvoch antén, laptopu a následne softvéru ako OpenBTS a Asterisk [21].

Najčastejšie tieto zariadenia využívajú štátne agentúry (vrátane Federal Bureau of Investigation) na riešenie prípadov (tieto zachytávače sa dokázali zamerať na telefóny podozrivých a filtrovať mobilné zariadenia podľa daných dôkazov), sledovanie podozrivých či sledovanie kradnutých telefónov. Stávalo sa však, že IMSI zachytávače identifikovali zlú budovu a polícia vrazila do bytu nevinných ľudí [10].

Dokonca tieto zariadenia polícia využila aj na sledovanie a uloženie IMSI čísiel na protestoch. V roku 2014 pri proteste v Kyjeve

mobilné telefóny daných protestujúcich obdržali správu o tom, že sú zaregistrovaní ako účastníci v tomto hromadnom proteste [44].

# Bibliografia


[1] *3G UMTS IMSI Catcher*. URL: http://www.pki-electronic.com/products/interception-and-monitoring-systems/3g-umts-imsi-catcher/ (cit. 07. 05. 2021).

[2] *3G-GSM Interctiopn & Target Location. Sales brochure.* URL: https://info.publicintelligence.net/Gamma-GSM.pdf (cit. 07. 05. 2021).

[3] I. Ahmad et al. „5G security: Analysis of threats and solutions“. In: *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*. 2017, s. 193–199. DOI: 10.1109/CSCN.2017.8088621.

[4] H. Alrashede a R. A. Shaikh. „IMSI Catcher Detection Method for Cellular Networks“. In: *2019 2nd International Conference on Computer Applications Information Security (ICCAIS)*. 2019, s. 1–6. DOI: 10.1109/CAIS.2019.8769507.

[5] R. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd Edition. Chapter 22: Phones*. 3. vyd. Chichester: John Wiley & Sons Ltd, 2020. ISBN: 978-1-119-64278-7.

[6] R. Anderson a M. Roe. *Crack A5*. 1998. URL: http://cryptome.org/jya/crack-a5.htm (cit. 13. 04. 2021).

[7] S. Aragon, F. Kuhlmann a T. Villa. „SDR-Based Network Impersonation Attack in GSM-Compatible Networks“. In: *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*. 2015, s. 1–5. DOI: 10.1109/VTCSpring.2015.7146071.

[8] J. Arkko a H. Haverinen. *Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)*. 2006. URL: https://tools.ietf.org/html/rfc4187 (cit. 26. 02. 2021).

[9] J. Baek et al. „Wi Not Calling: Practical Privacy and Availability Attacks in Wi-Fi Calling“. In: 2018, s. 278–288. DOI: 10.1145/3274694.3274753.

[10] D. Barrett. *Americans' Cellphones Targeted in Secret U.S. Spy Program*. 2014. URL: https://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533 (cit. 07. 05. 2021).

[11] N. Bhandari, S. Devra a K. Singh. „Evolution of Cellular Network: From 1G to 5G“. In: *International Journal of Engineering Trends and Technology* 3 (2017), s. 98–105. URL: http://oaji.net/articles/2017/1992-1515158039.pdf.

[12] E. Biham a O. Dunkelman. „Cryptanalysis of the A5/1 GSM Stream Cipher“. In: *Progress in Cryptology —INDOCRYPT 2000*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, s. 43–51. ISBN: 978-3-540-44495-4. URL: https://link.springer.com/chapter/10.1007/3-540-44495-5_5.

[13] E. Biham, O. Dunkelman a N. Keller. „A Related-Key Rectangle Attack on the Full KASUMI“. In: *Advances in Cryptology - ASIACRYPT 2005*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, s. 443–461. ISBN: 978-3-540-32267-2. URL: https://link.springer.com/chapter/10.1007/11593447_24.

[14] R. Borgaonkar et al. „New Privacy Threat on |3G, 4G, and Upcoming 5G AKA Protocols“. In: *Proceedings on Privacy Enhancing Technologies* (2019), s. 108–127. DOI: https://doi.org/10.2478/popets-2019-0039.

[15] A. Canteaut. „A5/1“. In: *Encyclopedia of Cryptography and Security*. Boston, MA: Springer US, 2011, s. 1–2. ISBN: 978-1-4419-5906-5. DOI: 10.1007/978-1-4419-5906-5_332.

[16] A. Canteaut. „Linear Feedback Shift Register“. In: *Encyclopedia of Cryptography and Security*. Boston, MA: Springer US, 2011, s. 726–729. ISBN: 978-1-4419-5906-5. DOI: 10.1007/978-1-4419-5906-5_357.

[17] M. Conti, N. Dragoni a V. Lesyk. „A Survey of Man In The Middle Attacks“. In: *IEEE Communications Surveys Tutorials* 18.3 (2016), s. 2027–2051. DOI: 10.1109/COMST.2016.2548426.

[18] *COPACOBANA*. URL: https://www.copacobana.org (cit. 13. 04. 2021).

[19] N. T. Courtois a W. Meier. „Algebraic Attacks on Stream Ciphers with Linear Feedback“. In: *Advances in Cryptology — EUROCRYPT 2003*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, s. 345–359. ISBN: 978-3-540-39200-2. DOI: 10.1007/3-540-39200-9_21.

[20] F. J. D'souza a D. Panchal. „Advanced encryption standard (AES) security enhancement using hybrid approach“. In: *2017 International Conference on Computing, Communication and Au-*

*tomation (ICCCA)*. 2017, s. 647–652. DOI: 10.1109/CCAA.2017.8229881.

[21] A. Dabrowski et al. *IMSI-catch me if you can: IMSI-catcher-catchers*. 2014. DOI: 10.1145/2664243.2664272.

[22] *DRT Company History*. URL: https://www.drti.com/our-technology/ (cit. 07. 05. 2021).

[23] O. Dunkelman, N. Keller a A. Shamir. *A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony*. Cryptology ePrint Archive, Report 2010/013. https://eprint.iacr.org/2010/013. 2010.

[24] I. Erguler a E. Anarim. „A modified stream generator for the GSM encryption algorithms A5/1 and A5/2“. In: *13th European Signal Processing Conference(EUSIPCO)* (2005). URL: https://www.researchgate.net/publication/228963335_A_modified_stream_generator_for_the_GSM_encryption_algorithms_A51_and_A52.

[25] *Ettus Research USRP B210*. URL: https://www.ettus.com/all-products/UB210-KIT/ (cit. 08. 04. 2021).

[26] R. Gallagher. *Meet the machines that steal your phone's data*. 2013. URL: https://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/ (cit. 07. 05. 2021).

[27] T. Gendrullis, M. Novotný a A. Rupp. „A Real-World Attack Breaking A5/1 within Hours“. In: *Cryptographic Hardware and Embedded Systems – CHES 2008*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, s. 266–282. DOI: 10.1007/978-3-540-85053-3_17.

[28] I. Gomez-Miguelez et al. „srsLTE: an open-source platform for LTE evolution and experimentation“. In: 2016, s. 25–32. ISBN: 978-1-4503-4252-0. DOI: 10.1145/2980159.2980163.

[29] M. Green. *A Few Thoughts on Cryptographic Engineering*. 2013. URL: https://blog.cryptographyengineering.com/2013/05/14/a-few-thoughts-on-cellular-encryption/ (cit. 16. 03. 2021).

[30] T. Güneysu et al. „Cryptanalysis with COPACOBANA“. In: *IEEE Transactions on Computers* 57.11 (2008), s. 1498–1513. DOI: 10.1109/TC.2008.80.

[31] F. Hadiji, F. Zarai a L. Kamoun. „Authentication protocol in fourth generation wireless networks“. In: *2009 IFIP International Conference on Wireless and Optical Communications Networks*. 2009, s. 1–4. DOI: 10.1109/WOCN.2009.5010508.

[32] H. Haverinen a J. Salowey. *Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)*. 2006. URL: https://tools.ietf.org/html/rfc4186 (cit. 26. 02. 2021).

[33] A. Jain a N. Chaudhari. „Two Trivial Attacks on A5/1:A GSM Stream Cipher“. In: (2013). URL: https://arxiv.org/vc/arxiv/papers/1305/1305.6817v1.pdf.

[34] H. Khan a K. Martin. „A survey of subscription privacy on the 5G radio interface - The past, present and future“. In: *Journal of Information Security and Applications* 53 (2020), s. 102537. DOI: 10.1016/j.jisa.2020.102537.

[35] M. Khan a Ch. Mitchell. „Retrofitting Mutual Authentication to GSM Using RAND Hijacking“. In: zv. 9871. 2016, s. 17–31. ISBN: 978-3-319-46597-5. DOI: 10.1007/978-3-319-46598-2_2.

[36] M. Khan et al. „Defeating the Downgrade Attack on Identity Privacy in 5G“. In: *Security Standardisation Research*. Cham: Springer International Publishing, 2018, s. 95–119. ISBN: 978-3-030-04762-7. DOI: 10.1007/978-3-030-04762-7_6.

[37] A. Koutsos. „The 5G-AKA Authentication Protocol Privacy“. In: *2019 IEEE European Symposium on Security and Privacy (EuroSP)*. 2019, s. 464–479. DOI: 10.1109/EuroSP.2019.00041.

[38] J. Krhovják et al. „TMTO attacks on stream ciphers – theory and practice“. In: 2011. URL: http://spi.unob.cz/papers/2011/2011-10.pdf.

[39] M. Kušnier. „Bezpečnostní aspekty technologií VoLTE a VoWiFi [online]“. Diplomová práce. Masarykova univerzita, Fakulta informatiky, Brno, 2019 [cit. 2021-03-18]. URL: https://is.muni.cz/th/c8l5g/.

[40] J. Lu, Z. Li a M. Henricksen. „Time–Memory Trade-Off Attack on the GSM A5/1 Stream Cipher Using Commodity GPGPU“. In: 2015, s. 350–369. ISBN: 978-3-319-28165-0. DOI: 10.1007/978-3-319-28166-7_17.

[41] *Meganet Products - Cell Phone Interceptors*. URL: http://www.meganet.com/meganet-products-cellphoneinterceptors.html (cit. 07. 05. 2021).

[42] S. Mjølsnes a R. Olimid. „Easy 4G/LTE IMSI Catchers for Non-Programmers“. In: 2017, s. 235–246. ISBN: 978-3-319-65126-2. DOI: 10.1007/978-3-319-65127-9_19.

[43] H. Mun, K. Han a K. Kim. „3G-WLAN interworking: security analysis and new authentication and key agreement based on EAP-AKA“. In: *2009 Wireless Telecommunications Symposium*. 2009, s. 1–8. DOI: 10.1109/WTS.2009.5068983.

[44] H. Murphy. *Ominous Text Message Sent to Protesters in Kiev Sends Chills Around the Internet*. 2014. URL: https://thelede.blogs.nytimes.com/2014/01/22/ominous-text-message-sent-to-protesters-in-kiev-sends-chills-around-the-internet/?action=click&contentCollection=Europe&module=RelatedCoverage&region=&mtrref=undefined&gwh=D4A40B9E478CDF385991F4F4BA09CE64&gwt=pay&assetType=PAYWALL (cit. 07. 05. 2021).

[45] R. Muthalagu a R. Jain. „Modifying the structure KASUMI to improve its resistance towards attacks by inserting FSM and S-Box“. In: *Journal of Cyber Security Technology* 2 (2018), s. 1–14. DOI: 10.1080/23742917.2018.1485415.

[46] K. Norrman, M. Naslund a E. Dubrova. „Protecting IMSI and User Privacy in 5G Networks“. In: MobiMedia '16. Xi'an, China: ICST (Institute for Computer Sciences, Social-Informatics a Telecommunications Engineering), 2016, s. 159–166. ISBN: 9781631901041. URL: https://www.researchgate.net/publication/311943117_Protecting_IMSI_and_User_Privacy_in_5G_Networks.

[47] Ch. Ntantogian a Ch. Xenakis. „One-pass EAP-AKA authentication in 3G-WLAN integrated networks“. In: *Wireless Personal Communications* 48 (2009), s. 569–584. DOI: 10.1007/s11277-008-9548-4.

[48] P. O'Hanlon, R. Borgaonkar a L. Hirschi. „Mobile Subscriber WiFi Privacy“. In: *2017 IEEE Security and Privacy Workshops (SPW)*. 2017, s. 169–178. DOI: 10.1109/SPW.2017.14.

[49] H. Ohta a M. Matsui. *A Description of the MISTY1 Encryption Algorithm*. 2000. URL: https://tools.ietf.org/html/rfc2994 (cit. 16. 04. 2021).

[50] M. Parviz, S. H. Mousavi a S. Mirahmadi. „Key Classification Attack on Block Ciphers“. In: *IACR Cryptol. ePrint Arch.* 2013 (2013), s. 288. URL: https://arxiv.org/ftp/arxiv/papers/1305/1305.4229.pdf.

[51] P. Paudel a A. Bhattarai. *5G Telecommunication Technology: History, Overview, Requirements and Use Case Scenario in Context of Nepal*. 2008. URL: https://www.researchgate.net/publication/325250893_5G_Telecommunication_Technology_History_Overview_Requirements_and_Use_Case_Scenario_in_Context_of_Nepal (cit. 10. 02. 2021).

[52] S. Petrovic a A. Sabater. „CRYPTANALYSIS OF THE A5/2 ALGORITHM.“ In: *IACR Cryptology ePrint Archive* 2000 (2000), s. 52. URL: https://www.researchgate.net/publication/220337199_CRYPTANALYSIS_OF_THE_A52_ALGORITHM.

[53] Ch. Ru a R. Gupta. „A Comparative Study of Various Generations in Mobile Technology“. In: *International Journal of Engineering Trends and Technology* 28 (2015), s. 328–332. DOI: 10.14445/22315381/IJETT-V28P263.

[54] D. Rupprecht et al. „Breaking LTE on Layer Two“. In: *2019 IEEE Symposium on Security and Privacy (SP)*. 2019, s. 1121–1136. DOI: 10.1109/SP.2019.00006.

[55] D. Rupprecht et al. „Call Me Maybe: Eavesdropping Encrypted LTE Calls With ReVoLTE“. In: *USENIX Security Symposium (SSYM)*. USENIX Association, 2020. URL: https://revolte-attack.net/media/revolte_camera_ready.pdf.

[56] F. Ryšánek. *PÁSMA LTE/UMTS/EDGE/GSM POUŽÍVANÁ V ČESKÉ REPUBLICE*. URL: https://www.fccps.cz/pasma-lteumtsedgegsm-pouzivana-v-ceske-republice-1379 (cit. 20. 11. 2020).

[57] N. Seddigh et al. „Security advances and challenges in 4G wireless networks“. In: *2010 Eighth International Conference on Privacy, Security and Trust*. 2010, s. 62–71. DOI: 10.1109/PST.2010.5593244.

[58] *Septier IMSI Catcher*. URL: http://www.dreamcatcher.solutions/product-item/septier-imsi-catcher/ (cit. 07. 05. 2021).

[59] A. Shaik et al. „Practical attacks against privacy and availability in 4G/LTE mobile communication systems“. English. In: *23rd Annual Network and Distributed System Security Symposium (NDSS 2016)*. NDSS 2016 Volume: Proceeding volume: ; Network and Distributed System Security Symposium ; Conference date: 21-02-2016 Through 24-02-2016. United States: Internet Society, 2016. DOI: 10.14722/ndss.2016.23236.

[60] W. Stallings. *Wireless Communications & Networks (2nd Edition)*. USA: Prentice-Hall, Inc., 2004. ISBN: 0131918354. URL: http://59.51.24.50:8000/wxwl/Wireless_Communications_&_Networking_Stallings_2nd.pdf.

[61] *The Evolution of Security in 5G*. 2018. URL: https://www.5gamericas.org/wp-content/uploads/2019/07/5G_Americas_5G_Security_White_Paper_Final.pdf (cit. 23. 01. 2021).

[62] P. Tomek. *Mobilní historie: milníky ve vývoji mobilní komunikace. Rok 2001*. URL: https://mobilmania.zive.cz/clanky/mobilni-historie-milniky-ve-vyvoji-mobilni-komunikace/sc-3-a-1111658/default.aspx (cit. 17. 11. 2020).

[63] A. Tudzarov a T. Janevski. „Functional Architecture for 5G Mobile Networks“. In: *International Journal of Advanced Science and Technology* 3 (2011). URL: https://www.researchgate.net/publication/233862183_Functional_Architecture_for_5G_Mobile_Networks.

[64] J. Valentino-Devries. *Stingray' Phone Tracker Fuels Constitutional Clash*. 2011. URL: https://www.wsj.com/articles/SB10001424053111904194604576583112723197574 (cit. 07. 05. 2021).

[65] J. Vieira et al. „A flexible 100-antenna testbed for Massive MIMO“. In: *2014 IEEE Globecom Workshops (GC Wkshps)*. 2014, s. 287–293. DOI: 10.1109/GLOCOMW.2014.7063446.

[66] *What is the difference between SIM and USIM cards?* URL: https://justaskthales.com/en/what-difference-between-sim-and-usim-cards/ (cit. 28. 04. 2021).

[67] Ch. Xenakis a L. Merakos. „Security in third Generation Mobile Networks“. In: *Computer Communications* 27.7 (2004), s. 638–650. ISSN: 0140-3664. DOI: https://doi.org/10.1016/j.comcom.2003.12.004.

[68] Y. Zikria et al. „5G Mobile Services and Scenarios: Challenges and Solutions“. In: *Sustainability* 10 (2018), s. 3626. DOI: 10.3390/su10103626.