UNIVERSITATEA NAȚIONALĂ DE ȘTIINȚĂ ȘI TEHNOLOGIE POLITEHNICA BUCUREŞTI

Școala Doctorală de Electronică, Telecomunicații și Tehnologia Informației

Decizie nr. 161 din 21-12-2023

TEZĂ DE DOCTORAT

Ing. Cristian Nicolae CAPOTA

CONTRIBUȚII CU PRIVIRE LA SECURITATEA COMUNICAȚIILOR TELEFONICE MOBILE DE NOUĂ GENERAȚIE

COMISIA DE DOCTORAT

Prof. dr. ing. Ion MARGHESCU Universitatea Națională de Știință și Tehnologie Politehnica București	Președinte
Prof. dr. ing. Simona HALUNGA Universitatea Națională de Știință și Tehnologie Politehnica București	Conducător de doctorat
Prof. dr. ing. Corina NAFORNIȚĂ Universitatea Politehnica din Timișoara	Referent
Prof. dr. ing. Ioan NICOLAESCU Academia Tehnică Militară București	Referent
Prof. dr. ing. Teodor PETRESCU Universitatea Națională de Știință și Tehnologie Politehnica București	Referent

BUCUREŞTI 2024

Cuprins

Introducere

Prezentarea domeniului de doctorat

Scopul tezei

Principalul obiectiv al acestei lucrări constă în sensibilizarea unei audiențe extinse cu privire la prezența unor vulnerabilități exploatabile de către persoane rău intenționate, în tehnologiile implementate deja, sau în curs de implementare, la nivelul operatorilor de telefonie mobilă din România. Totodată, am dorit prezentarea unor metode simple de contracarare a acestor vulnerabilități identificate, precum și de protejare a canalelor de comunicații la nivel interfață utilizator-rețea care pot reduce semnificativ riscurile de securitate prezentate în această lucrare. Măsurătorile experimentale au creat o imagine actuală și clară cu privire la acoperirea cu semnal radio a operatorilor de telefonie mobilă din municipiul București, în tehnologiile 2G-4G, determinarea vitezelor de transfer date, pentru toți operatorii, în fiecare bandă de frecvență și tehnologie disponibilă și de evidențiere a unor dispozitive Wi-Fi (Puncte de acces și utilizatori) și a unor dispozitive ce utilizează tehnologia Bluetooth Low Energy. Experimentele și măsurătorile efectuate în teren au condus către devoalarea ușurinței cu care o persoană rău intenționată poate derula acțiuni de tip Refuz de servicii, asupra utilizatorilor dintr-un spațiu interior. Am dezvoltat un sistem de bruiaj inteligent capabil să emită pe o frecvență, la sesizarea unui prag de amplitudine minimă pe o altă frecvență, în vederea blocării accesului la rețea dintr-o anumită facilitate (e.g. închisori).

Conținutul tezei

Teza își propune, în cele 8 capitole, să analizeze elemente fundamentale de funcționare și securitate a rețelelor de comunicații fără fir, în vederea utilizării în cadrul unor scenarii experimentale practice, aplicate pentru standardele de comunicații disponibile la nivelul operatorilor de telefonie mobilă din România, respectiv teste de laborator a standardelor ce urmează a fi implementate, cu referire directă la ecosistemul IOT-5G.

Ca element de noutate, se propune aplicarea tehnicii de amprentă radio a dispozitivelor mobile testate, cu detalierea principalilor parametri ai rețelelor, respectiv disponibilitatea radio a operatorilor de telefonie mobilă, prin furnizarea integrată a serviciilor de date prin intermediul stațiilor de bază și a APN open.

Capitolul 1 Introducere

1.1 Scurt istoric

În cadrul secțiunii, au fost prezentate aspecte referitoare la istoricul comunicațiilor telefonice mobile. În acest moment, suntem angrenați într-un proces amplu de implementare la nivel european a celei de-a cincea generații de comunicații mobile, 5G NSA și 5G SA. [4]

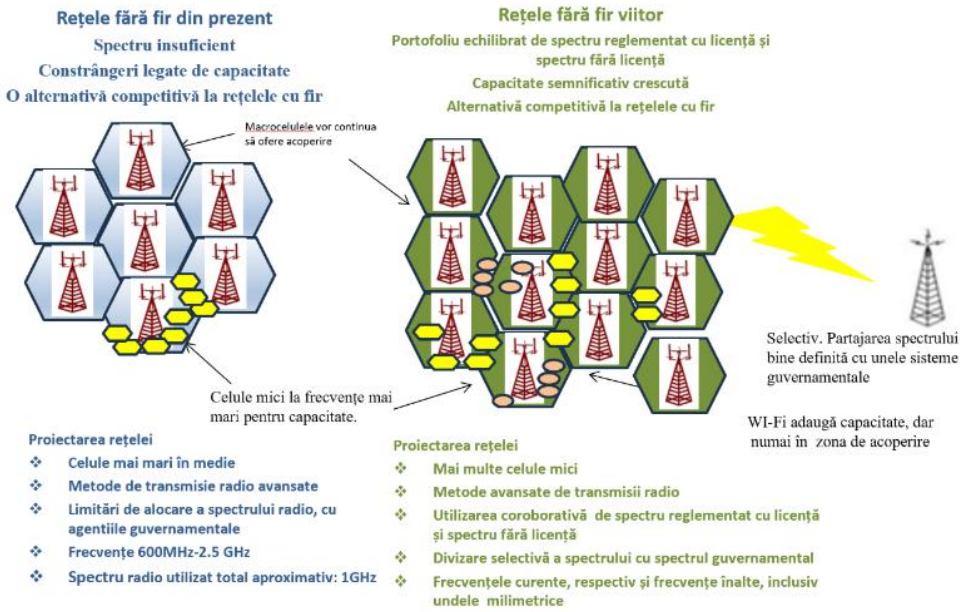


Figura 1.1. Prezentul și viitorul rețelelor de comunicații fără fir

1.2 Evoluția sistemelor de comunicație de la 1G la 6G

Au fost prezentate principalele caracteristici al standardelor de comunicații de la 1G la prezentul 5G, respectiv considerații cu privire la viitoarele rețele 6G, respectiv domenii de aplicabilitate practică, de interconectare a dispozitivelor mobile.

Capitolul 2 Considerații fundamentale ale rețelelor de comunicații fără fir

Considerații fundamentale ale tehnologiei 2G-GSM

Considerat învechit și depășit tehnologic, de către cei mai mulți specialiști în domeniu, cu multiple vulnerabilități în ceea ce privește autentificarea și securitatea datelor utilizatorilor, standardul GSM este încă prezent în rețelele operatorilor de telefonie mobilă din România.

2.1. Arhitectura rețelei 2G-GSM

Au fost prezentate aspecte teoretice cu privire la arhitectura GSM, cu evidențierea principalilor parametri, respectiv măsurători practice de evidențiere a vulnerabilităților cu privire la autentificare.

2.2 Algoritmi de criptare utilizați în tehnologia GSM

În tehnologia GSM, se realizează autentificarea unilaterală a stațiilor mobile față de stațiile de bază, prin folosirea unor algoritmi de criptare simetrică, protejând de asemenea și confidențialitatea abonaților, prin utilizarea unei chei secrete.

2.3 Aspectele practice ale cercetării doctorale aplicative, în rețeaua GSM

2.3.1. Autentificarea dispozitivelor mobile în tehnologia GSM

Partea practică a procesului de Autentificare în rețeaua GSM a fost realizată în condiții de laborator: prin excluderea altor terminale mobile din imediata apropiere, respectiv amplasarea dispozitivelor utilizate într-o cameră anecoică.

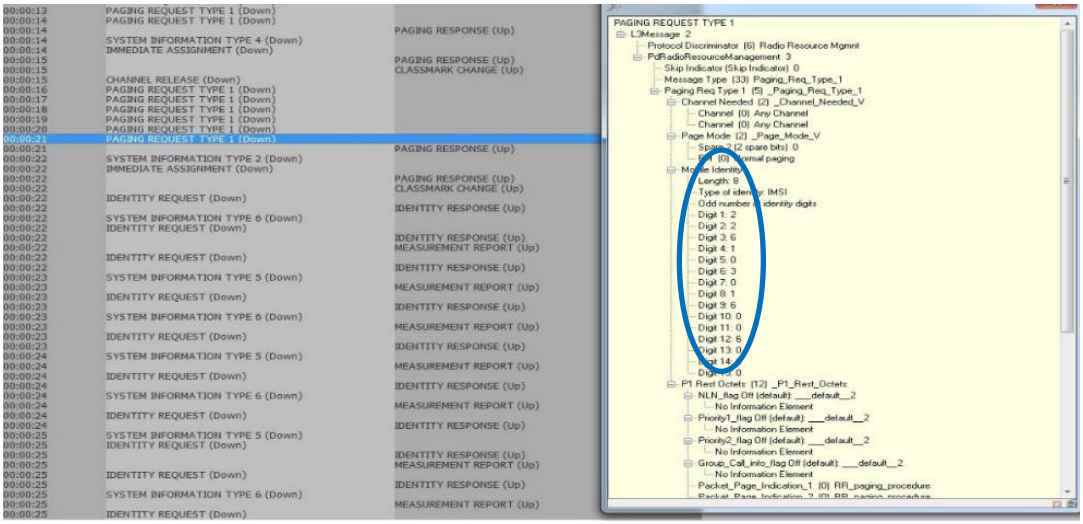


***Figura 2.6. (b)** IMSI este transmis.*

Au fost prezentate aspecte rezultate din măsurătorile practice privind vulnerabilitățile rețelelor GSM.

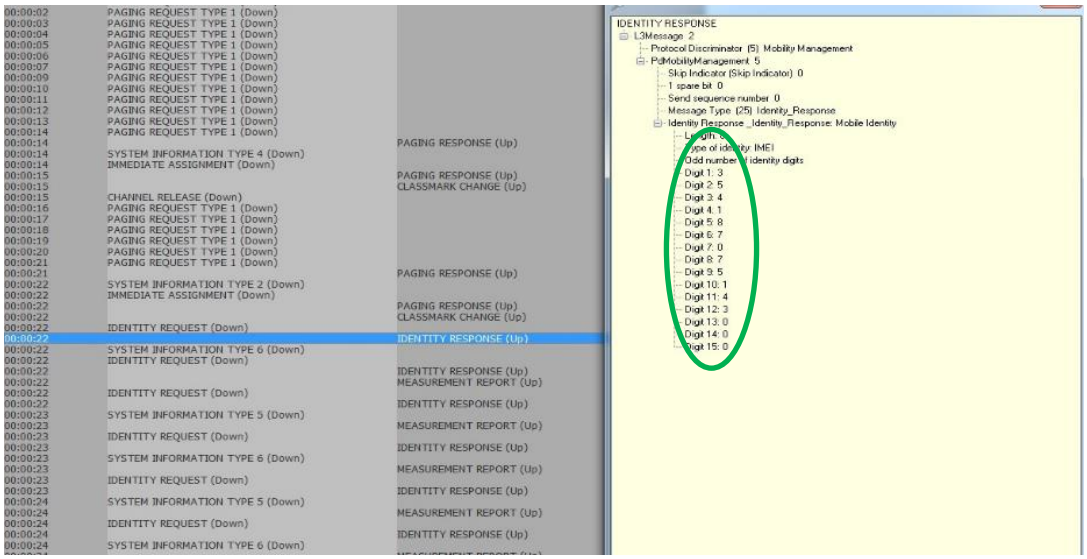


***Figura 2.7**. Parametrul IMEI este transmis.*

2.3.2 Localizarea dispozitivelor mobile ce utilizează tehnologia GSM

În cadrul sub secțiunii au fost prezentate testele experimentale efectuate în vederea localizării unui dispozitiv mobil ce funcționează în standardul GSM, în rețeaua operatorilor Orange România și Vodafone România.

În prezent, la nivelul serviciilor de urgență 112, localizarea se face la nivel de BTS – Cod de celulă, operatorii de telefonie mobilă din România nu oferă servicii de localizare cu precizie a dispozitivelor mobile într-un areal geografic, întrucât în țara noastră reglementările legale nu impun astfel de prevederi.

Localizarea unui dispozitiv mobil în rețeaua Orange România

În figura 2.9 sunt prezentate toate canalele de control a emisiei (Broadcast Control Channel-BCCH–urile), disponibile în punctul de măsură, pentru operatorul Orange România.

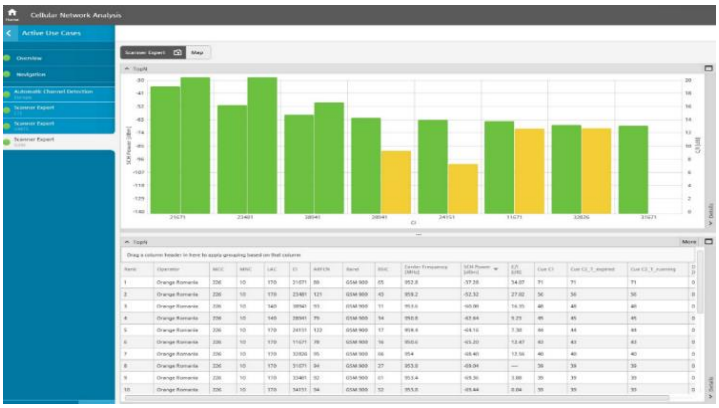


Figura 2.9. *Măsurători ale BTS, BCCH în GSM, Orange România*

Pentru localizarea unui dispozitiv ce utilizează standardul GSM, a fost identificate canalul, codul celulei care deservește zona în care au fost efectuate măsurătorile, precum și nivelul de semnal recepționat pe conexiunea ascendentă a rețelei. Având în vedere caracterul comunicației full-duplex în standardul GSM, legătura radio între terminalul mobil și rețea se realizează pe două frecvențe diferite, conexiunea ascendentă dintre terminal și rețea (UpLink-UL) și conexiunea descendentă dintre rețea și terminalul mobil (DownLink-DL).

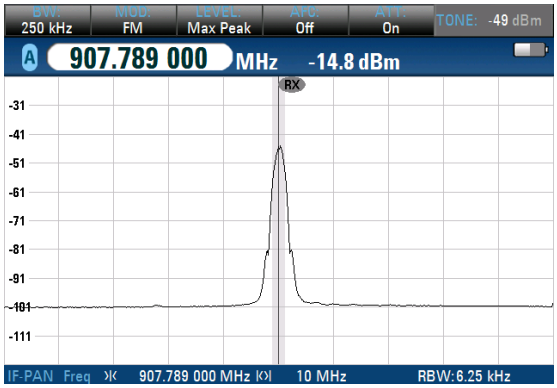


Figura 2.12. *Nivelul de semnal măsurat pe conexiunea ascendentă*

Localizarea unui dispozitiv mobil în rețeaua operatorului Vodafone România

Modul de lucru este similar cu localizarea unui dispozitiv mobil în rețeaua operatorului Orange România.

Capitolul 3 Considerații fundamentale ale tehnologiei 3G-UMTS

Standardul 3G joacă un rol crucial în această evoluție a rețelei, astfel, internetul mobil/fără fir a devenit disponibil pe scară largă, pentru utilizatori, fapt care a ridicat noi și noi preocupări legate de problemele de securitate. [13]

3.1 Arhitectura rețelei 3G-UMTS

Au fost prezentate principalele componente ale rețelei 3G-UMTS. [13]

3.2 Autentificarea dispozitivelor mobile în tehnologia UMTS

În cadrul secțiunii a fost prezentat setul de mecanisme de securitate.[13] și [14] precum și procedura de autentificare prin exemple practice.

3.3 Experimente practice și măsurători radio în tehnologia UMTS

Măsurătorile au vizat evidențierea amprentei radio a terminalelor mobile în spectrul de frecvențe, a nivelului de emisie caracteristic unei comunicații cu celula de bază în procesul de autentificare, respectiv localizarea unui dispozitiv mobil. [16] și [17]

3.3.1 Autentificarea dispozitivelor mobile în tehnologia UMTS

Au fost prezentate detalii referitoare la procesul de autentificare care poate fi împărțit în trei etape. Etapa 1 în care terminalul mobil transmite la solicitarea rețelei în vederea inițierii procesului de autentificare, parametrul IMSI, etapa 2, transmiterea parametrului IMEI, respectiv etapa 3, atribuirea de către rețeaua UMTS a parametrului P-TMSI.

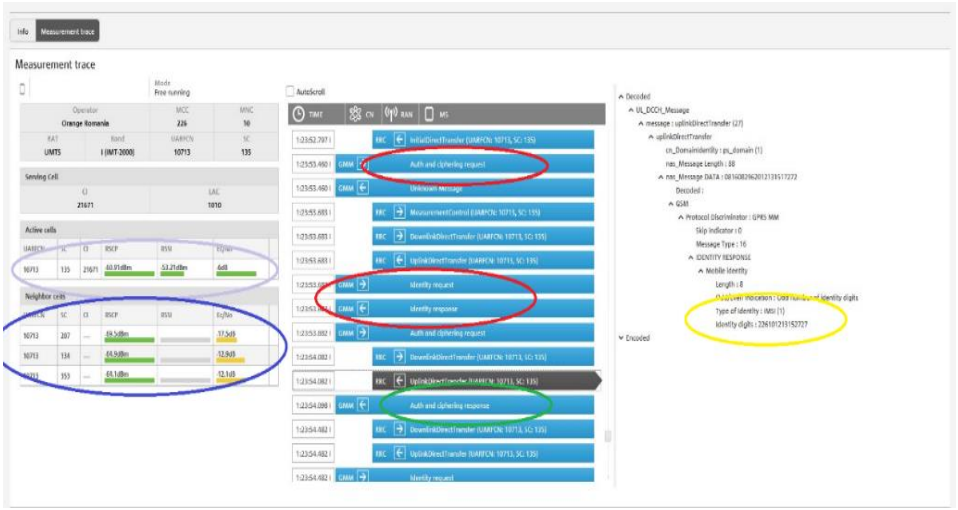


Figura 3.5. *Procesul de autentificare în 3G-UMTS, transmiterea IMSI*

În figura 3.6, este prezentată etapa 2 din procesul de autentificare a unui terminal mobil în rețea, printr-o cerere, rețeaua solicită identitatea echipamentului folosit, în vederea validării accesului în rețea.

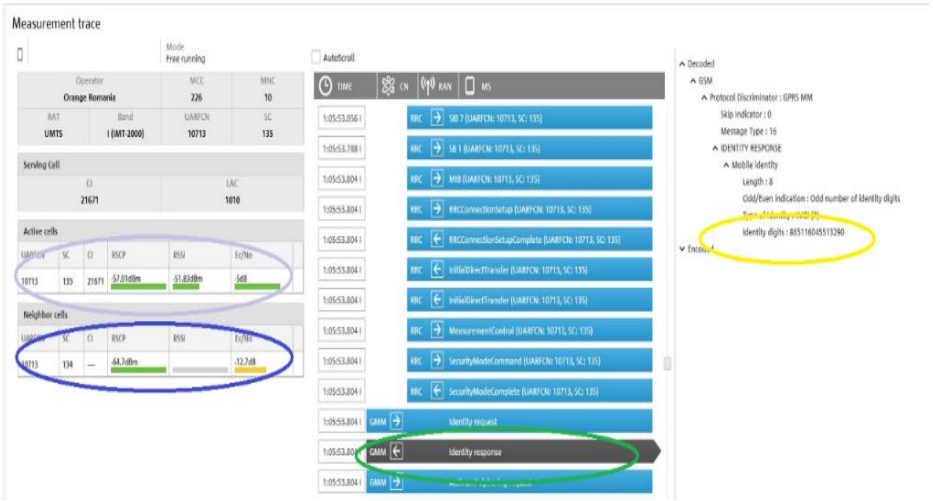


Figura 3.6. *Procesul de autentificare în 3G-UMTS, transmiterea IMEI*

3.3.2 Localizarea dispozitivelor mobile ce utilizează tehnologia 3G-UMTS

Au fost efectuate măsurători ale standardului 3G-UMTS, în rețeaua operatorului Orange România, UARFCN corespondente, respectiv parametrii tehnici caracteristici conexiunii de la rețea către terminalul mobil. În figura 3.12, se poate observa că atunci când distanța fizică dintre antena receptorului portabil și dispozitivul mobil scade, nivelul semnalului crește până la -24.7 dBm.

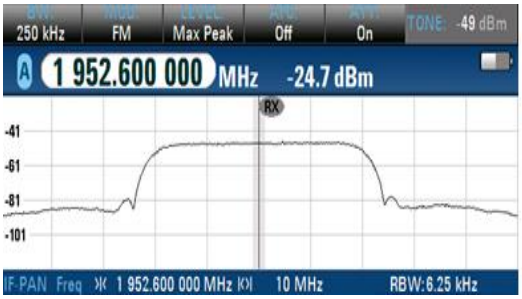


Figura 3.12. *Nivelul de semnal măsurat în proximitatea dispozitivului mobil.*

Capitolul 4 Considerații fundamentale ale tehnologiei 4G-LTE

Rețeaua 4G dezvoltată de către grupul 3GPP, (3rd Generation Partnership Project), prima generație a standardului Evoluție pe termen lung, este o evoluție semnificativă a standardului 3G, care deschide calea către o dezvoltare radicală a arhitecturii rețelei, concomitent cu beneficiile oferite abonaților.

4.1 Arhitectura rețelei 4G - LTE

Au fost prezentate aspecte teoretice cu privire la arhitectura rețelei 4G-LTE și principalele componente, precum și rolul acestora în rețea. [13]

4.2. Autentificarea dispozitivelor mobile în tehnologia LTE

În această secțiune au fost formulate aspecte de ordin teoretic cu privire la vulnerabilitățile tehnologiei 4G-LTE.

4.3 Evaluări experimentale radio în tehnologia LTE

În cadrul secțiunii au fost prezentate măsurători radio ale nivelurilor de semnal, precum și procedura de autentificare a unui terminal mobil în banda de 800 MHz unde sunt furnizate servicii LTE dar și aspecte referitoare la determinarea locației.

4.3.1 Măsurători ale legăturii radio în banda de frecvență 800 MHz tehnologie LTE

Măsurătorile au vizat evidențierea procesului de autentificare a terminalelor mobile în rețea, a nivelului de emisie caracteristic unei comunicări cu celula de bază, respectiv de localizare a unui dispozitiv mobil.

4.3.2 Autentificarea dispozitivelor mobile în tehnologia LTE

Principala modificare care a fost introdusă de către 3GPP, la autentificarea unui terminal mobil în rețeaua LTE este dată de faptul că parametrul IMEI nu mai este utilizat în procesul de autentificare, implicit cerut de rețea, astfel a fost eliminată vulnerabilitatea standardelor anterioare.

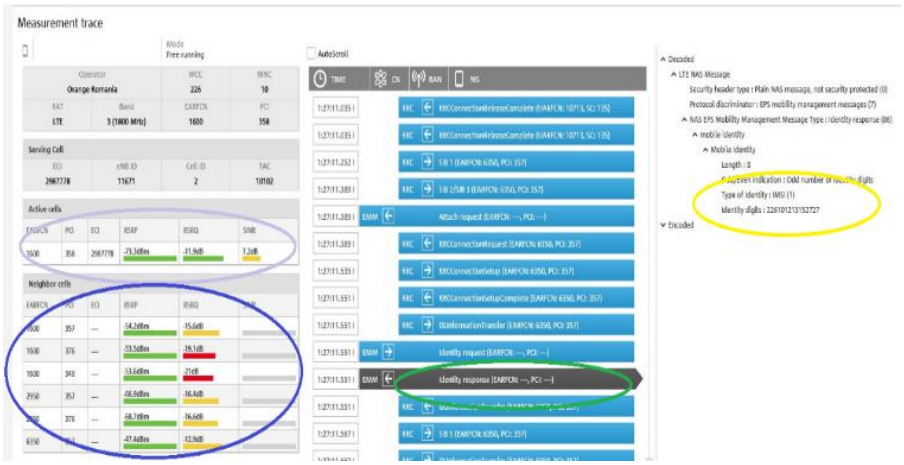


Figura 4.4. *Finalizarea cu succes a autentificării și transmiterea IMSI.*

După încheierea cu succes a sesiunii de autentificare, corespondent IMSI este alocat un parametru temporar utilizat în rețelele 4G GUTI, care este echivalentul parametrului temporar TMSI utilizat din standardul GSM.

4.3.3 Localizarea dispozitivelor mobile ce utilizează tehnologia LTE

Localizarea practică a dispozitivelor ce utilizează standardul 4G, într-un mediu de laborator, este o provocare, întrucât în lărgimea de bandă (RB) pot fi mai multe dispozitive care comunică la același moment de timp cu rețeaua. Pentru determinarea poziției dispozitivului, în figura 4.6 este măsurat nivelul de semnal RSSI, în banda LTE 20, lărgimea de bandă este de 10 MHz. [35]

Corespondența certă a frecvențelor, între canalul conexiunii ascendente și cel de conexiune descendentă, relevă faptul că, pentru canalul EARFCN 6350, în banda 20 de

800Mhz, măsurat într-un mediu interior, frecvența conexiunii ascendente este 852 MHz.

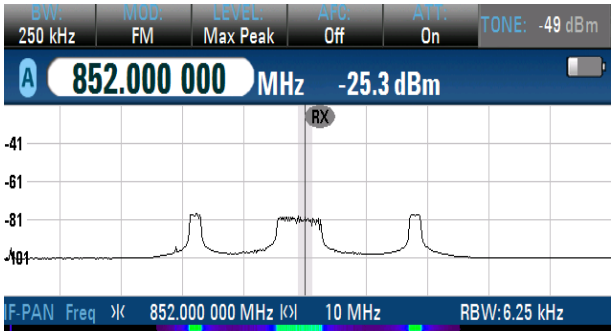


Figura 4.8. *Conexiunea ascendentă măsurată în banda 20 (800MHz) standardul LTE.*

Capitolul 5 Considerații fundamentale ale rețelelor de comunicații 5G

Rețelele de comunicații 5G sunt concepute pentru a conecta industriile (cum ar fi producția și prelucrarea, transportul inteligent, rețelele inteligente și e-sănătatea), dar și pentru a servi oamenii și societatea, practic într-un nou ecosistem radio. [34] și [41]

5.1 Arhitectura rețelei de comunicații 5G

În cadrul secțiunii au fost prezentate considerente teoretice ale arhitecturii rețelei 5G.

5.2 Cerințe și proceduri de securitate pentru rețelele de comunicații 5G

Au fost prezentate principalele cerințe de securitate și procedurile corespunzătoare pentru RAN al rețelelor de comunicații 5G [43] și [47]

5.2.1 Secvența de lucru a cheii

Secvența de lucru a cheii se referă la procesul prin care două entități, un dispozitiv mobil și o rețea 5G, stabilesc o cheie de criptare comună pentru a asigura confidențialitatea și securitatea comunicațiilor lor. [39]

5.2.2 Autentificarea și controlul rețelei de domiciliu

Au fost prezentate detalii referitoare la autentificare dispozitivelor mobile [39] și la metode de creștere a controlului rețelei de domiciliu, prin segmentarea rețelei.

5.3 Măsurători radio în rețelele de comunicații 5G

În contextul implementării tehnologiei 5G-NSA, de către operatorul de telefonie mobilă Orange România, au fost efectuate măsurători radio în condiții de laborator, în vederea vizualizării unei conexiuni descendente, dintre rețea și terminalele mobile.

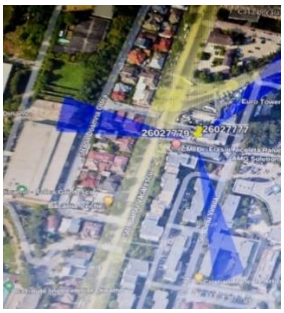


Figura 5.4. *Reprezentarea predicției propagării a unui site de celule ce furnizează servicii 5G NSA, în Google Earth.*

Pe perioada desfășurării unui stagiu de practică inclus în cadrul proiectului OPTIM Research derulat de UPB, am reușit să întreprind activități de cercetare aplicativă și asupra acestei tehnologii 5G SA, măsurători prezentate în figura 5.5.

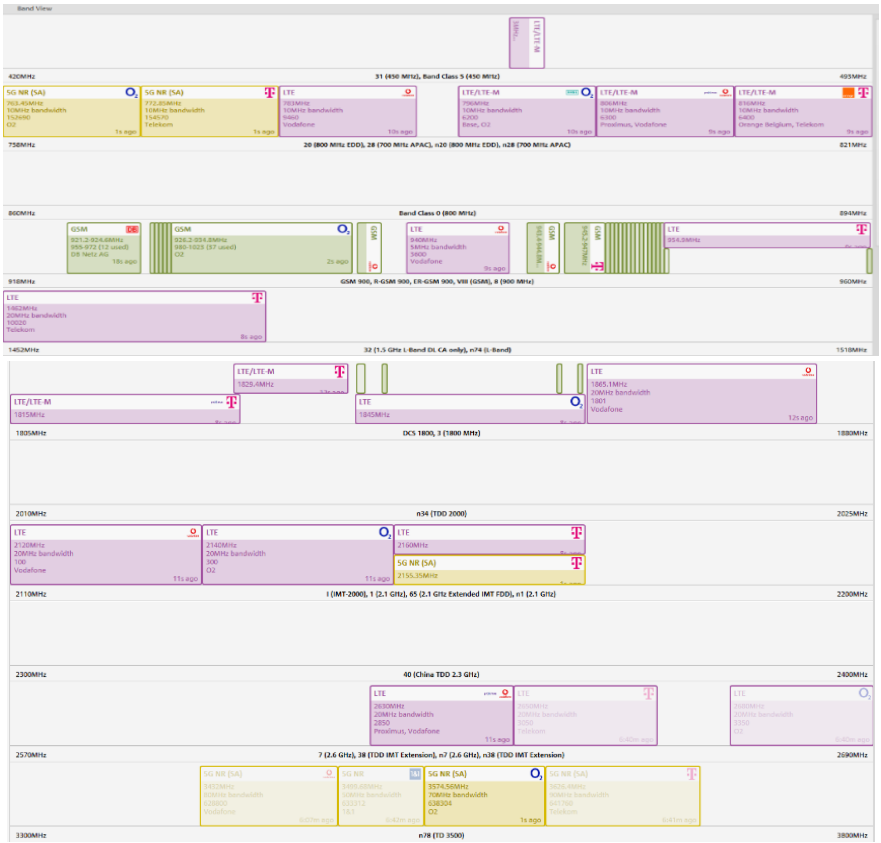


Figura 5.5. *Diagrama spectrală a operatorilor de telefonie mobilă în punctul de măsură.*

Analiza figurii 5.5 relevă următoarele:

- Tehnologia GSM, marcată în culoarea verde, este implementată de către toți operatorii de telefonie mobilă, activi în punctul de măsură.
- Tehnologia UMTS este exclusă total;
- Prezența tehnologiei LTE – 4G (marcată în culoarea mov) în benzile de frecvență:
    - ✓ 800 MHz LTE și LTE-M2M operatorii Vodafone, O_2 și Telekom;
    - ✓ 900 MHz Vodafone și Telekom;
    - ✓ 1500 MHz Telekom;
    - ✓ 1800MHz, operatorii Vodafone, O_2 și Telekom;
    - ✓ 2100 MHz, operatorii Vodafone, O_2 și Telekom;
    - ✓ 2600 MHz, operatorii Vodafone, O_2 și Telekom.
- Prezența preponderentă a tehnologiei 5G SA (marcată în culoarea galbenă) în benzile de frecvență:
    - ✓ 700 MHz, banda n20, operatorii O_2 și Telekom;
    - ✓ 2100 MHz, banda n1, operatorul Telekom;
    - ✓ 3500 MHz, banda n78, operatorii O_2 și Telekom.

Capitolul 6 Considerații fundamentale ale rețelelor ce utilizează tehnologiile WiFi și BLE

Internetul Obiectelor (Internet of Things - IoT) reprezintă o paradigmă în tehnologie care se referă la conexiunea, interconectarea și comunicarea dispozitivelor fizice sau obiectelor inteligente prin intermediul internetului. [49].

Au fost prezentate principalele caracteristici ale dispozitivelor IoT.

6.1 Rețele ce lucrează în tehnologia WiFi

6.1.1 Arhitectura rețelelor în tehnologia WiFi

În cadrul secțiunii a fost descrisă arhitectura rețelelor WiFi principalele componente, precum și pașii de conectare dintre un dispozitiv mobil și o rețea WiFi..

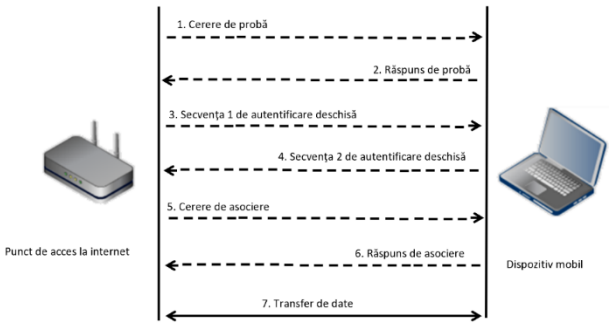


Figura 6.2. *Procesul de autentificare și asociere 802.11.*

6.1.2. Teste practice în vederea evidențierii vulnerabilităților WiFi

Subsecțiunea cuprinde măsurători ale nivelului de semnal RF, respectiv metode de poziționare în standardul WiFi a dispozitivelor și a furnizorului de servicii WiFi, într-un mediu de laborator.

6.1.3.1 Măsurători radio ale terminalului mobil pentru funcția de apelare WiFi

Măsurătorile efectuate au vizat identificarea în spectrul radio alocat WiFi a emisiei radio a AP, respectiv pe ecranul terminalului mobil a AP, care este disponibil a furniza servicii utilizatorilor din proximitate.

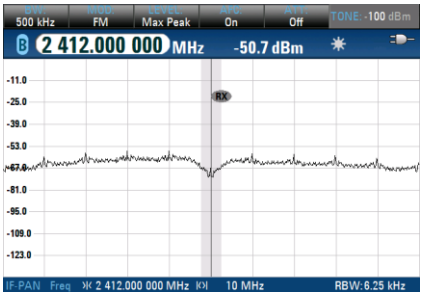


Figura 6.9. *Nivelul de semnal al AP clonă.*

6.1.3.2 Testarea securității funcției de apelare WiFi

Predispoziția dispozitivelor mobile pentru a selecta rețeaua WiFi în baza parametrilor menționați anterior, în conformitate cu standardele apelare WiFi le face ca acestea să fie susceptibile la atacurile de tip preluare (Man in the Middle - MitM). [50]

6.1.3.3 Atacuri de tip preluare

A fost prezentat un atac de tip preluare (Man in the Middle - MitM) care implică configurarea unui AP clonă, cu aceiași parametri radio ca router-ul valid, același set de identificatori de service (Extended Service Set Identifier-ESSID), criptare, cifru și cheie. AP-ul clonă va fi plasat între rețeaua reală și dispozitivul mobil, astfel încât să devină mai atractiv pentru țintă. [50]

6.1.3.4 Identificarea țintei

În cadrul sub secțiunii au fost redate detalii cu privire la procedura de de autentificare, respectiv clonarea practică a unui AP.

6.1.3.5 AP clonă

Au fost prezentate analiza pachetelor de date obținute din captura WiFi, respectiv vulnerabilitățile identificate. [73].

6.2 Rețele ce lucrează în tehnologia Bluetooth Low Energy

6.2.1 Bluetooth introducere

În cadrul secțiunii a fost prezentat un scurt istoric al rețelelor BLE.

6.2.2 BLE arhitectura și măsurători ale canalelor radio

Au fost prezentate aspecte referitoare la arhitectura rețelelor BLE, măsurători radio în spetrul radio și principalele componente.

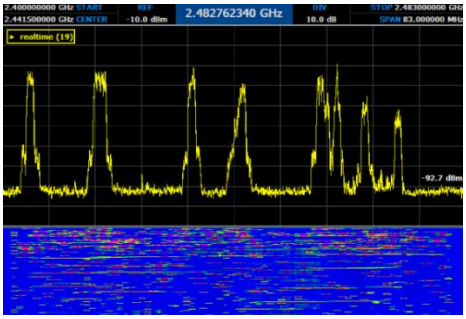


Figura 6.15. *Măsurători RF ale spectrului BLE.*

6.2.3 Procesul de autentificare în rețelele BLE

Au fost prezentate detalii referitoare la procedura de autentificare a dispozitivelor BLE, respectiv un atac de tip preluare asupra conexiunii BLE.
Întregul proces de comunicare are patru faze – publicitate, inițiere, conectare și schimb. Dispozitivul periferic trimite pachete publicitare temporizate. Dispozitivul central scanează și utilizează pachetele publicitare pentru a găsi dispozitivul periferic.

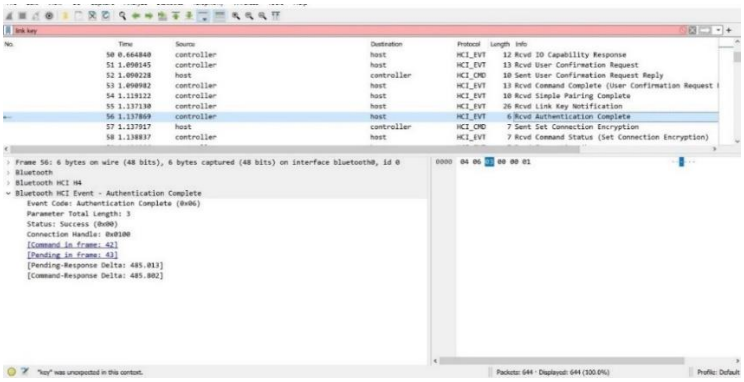


Figura 6.17*. Autentificarea este validă şi completă.*

Pentru a identifica și evidenția procesul de autentificare a unor dispozitive ce lucrează în standardul BLE, a fost monitorizată conexiunea dintre cele 2 dispozitive și astfel a fost obținut fișierul .pcap care a fost analizat cu ajutorul aplicației software WireShark.

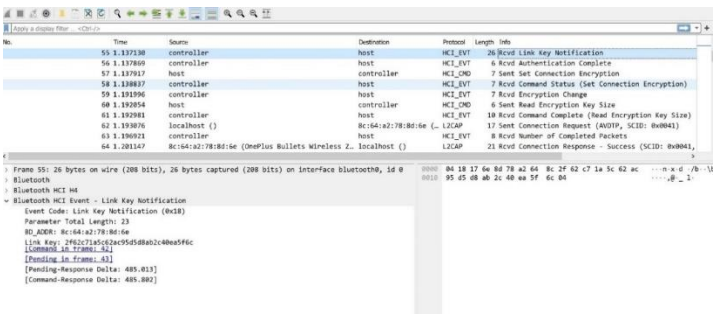


Figura 6.18. *Cheia de conexiune este extrasă*

Ultimul pas se efectuează atunci când are loc transmiterea efectivă a datelor, iar transmisia de date poate fi bidirecțională. Întreaga legătură de securitate se bazează pe cheia de conexiune generată de cele două dispozitive, care este stocată în memoria RAM a dispozitivelor.

Clonarea relativ facilă a parametrilor: adresă MAC BLE, nume dispozitiv, chiar și introducerea în procesul de autentificare a cheii de legătură obținute anterior din conectarea validă, face ca procesul de conectare să nu fie validat. Deci, securitatea conexiunilor BLE nu poate fi falsificată folosind instrumente obișnuite, cum ar fi clonarea adresei MAC BLE și/ sau schimbarea numelui dispozitivului.

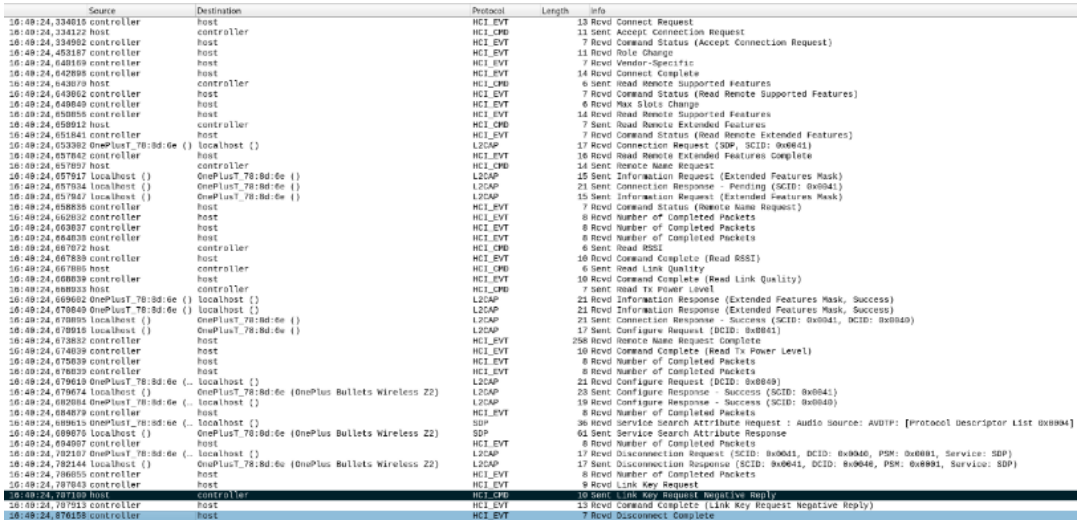


***Figura 6.19**. Procesul de autentificare cu răspuns negativ.*

Capitolul 7 Măsurători experimentale

În cadrul capitolului au fost prezentate pe larg experimentele efectuate în 5 puncte aglomerate din municipiul București, în vederea determinării calității și cantității serviciilor de date puse la dispoziția utilizatorilor, pentru fiecare tehnologie disponibilă în bandă, iar partea a doua a capitolului a vizat realizarea unui dispozitiv inteligent de bruiaj, capabil de atacuri de tip DoS.

7.1. Măsurători radio operatorul Orange România

Rezultatele vitezelor de trafic obținute ca urmare a măsurătorilor efectuate pentru operatorul Orange România.

Tabelul 7.12. *Rezultatele testelor de viteză, operatorul Orange, în punctele de măsură 1-5.*

Punctul de măsură	Viteza de trafic (MB/s)	Banda 800 MHz LTE	Banda 900MHz			Banda 1800 MHz LTE	Banda 2100 MHz		Banda 2600 MHz LTE
			GSM	UMTS	LTE		UMTS	LTE	
Zona Obor	Descărcare	11,1	-	7,81	-	100	error	-	217
	Încărcare	26,1	-	2,45	-	49,8	error	-	43
Zona Piața Alba Iulia	Descărcare	13,1	-	14,9	-	15,7	9,04	-	52
	Încărcare	7,44	-	4,3	-	42,4	3,43	-	48,8
Zona Piața Sudului	Descărcare	2,07	-	3,06	-	21,7	5,58	-	45,3
	Încărcare	1,5	-	1,35	-	12,7	2,51	-	6,13
Zona Vulcan	Descărcare	3,64	-	1,82	-	42,5	7,82	-	79,2
	Încărcare	0,71	-	0,3	-	40,3	3,6	-	47,3
Zona Mall Plaza	Descărcare	9,24	-	3,26	-	5,33	9,82	-	33,7
	Încărcare	24,1	-	1,57	-	25,3	2,15	-	33

7.2. Măsurători radio operatorul Vodafone România

Au fost prezentate rezultatele vitezelor de trafic obținute ca urmare a măsurătorilor efectuate pentru operatorul Vodafone România.

7.3. Măsurători radio operatorul Telekom România

Au fost prezentate rezultatele vitezelor de trafic obținute, în punctele de măsură 1-5, ca urmare a măsurătorilor efectuate pentru operatorul Telekom România.

7.4. Măsurători radio operatorul DigiMobil România

Au fost prezentate rezultatele vitezelor de trafic obținute, în punctele de măsură 1-5, ca urmare a măsurătorilor efectuate pentru operatorul DigiMobil România.

7.5 Concluzii măsurători radio

Au fost prezentate măsurătorile aferente conexiunii radio a disponibilității operatorilor de telefonie mobilă în punctele de măsură, pentru toți operatorii de telefonie mobilă măsurați.

Tabelul 7.38. *Rezumat tehnologii implementate în benzile de frecvență, pentru operatorul Orange România:*

Banda de frecvență / Punct de măsură	800 MHz	900 MHz			1800 MHz	2100 MHz		2600 MHz
	LTE	GSM	UMTS	LTE	LTE	UMTS	LTE	LTE
Zona Obor	✗	✗	✗	-	✗	-	-	✗
Zona Piata Alba Iulia	✗	✗	✗	-	✗	✗	-	✗
Zona Piața Sudului	✗	✗	✗	-	✗	✗	-	✗
Zona Vulcan	✗	✗	✗	-	✗	✗	-	✗
Zona Mall Plaza	✗	✗	✗	-	✗	✗	✗	✗

7.6. Identificarea punctelor de acces WIFI, respectiv clienți

De asemenea, au fost efectuate măsurători în spectrul radio alocat comunicațiilor WiFi în toate punctele de măsură 1-5, rezultatele obținute au fost sintetizate astfel:

Tabelul 7.44. *Statistică dispozitive mobile și AP ce utilizează tehnologia WiFi, în punctele de măsură.*

Punct de măsură	Puncte de acces	Număr clienți
Zona Obor	52	92
Zona Piata Alba Iulia	59	66
Zona Piața Sudului	10	31
Zona Vulcan	7	46
Zona Mall Plaza	14	45

7.7 Identificarea dispozitivelor BLE

Tabelul 7.46. *Statistica numărului de dispozitive BLE cu MAC unic, în punctele de măsură 1-5.*

Punctul de măsură	Dispozitive BLE
Zona Obor	132
Zona Piata Alba Iulia	565
Zona Piața Sudului	39
Zona Vulcan	15
Zona Mall Plaza	16

Având în vedere statistica numărului de dispozitive BLE, prezentată în Tabelul 7.46. constatăm faptul că zona Piața Alba Iulia a fost cea mai aglomerată din punct de vedere al prezenței dispozitivelor BLE (565), respectiv zona comercială Vulcan, cea mai puțin aglomerată (15).

7.8 Dispozitiv experimental de bruiaj inteligent în tehnologia LTE

Analiza realizată în baza măsurătorilor experimentale, prezentate în capitolele anterioare a evidențiat ușurința cu care se pot întreprinde unele atacuri prin interfața radio a canalelor de comunicații fără fir.
Practic, se pot executa atacuri de tip Refuz de servicii (DoS) din partea unei persoane rău intenționate, prin bruiajul conexiunii radio, indiferent de tehnologie, bineînțeles în anumite condiții de propagare radio, respectiv de proximitate față de dispozitivele mobile vizate.[91]
În cadrul secțiunii au fost prezentate caracteristicile tehnologiei SDR, precum și considerații teoretice cu privire la tehnicile de bruiaj.

Obiectivele principale ale dezvoltării unui sistem de bruiaj sunt:

1. Determinarea limitelor de bruiaj, în două scenarii diferite, poziționând receptorul în vecinătatea celulei și la marginea de acoperire a celulei, pentru două valori a nivelului de semnal recepționat;
2. Determinarea condițiilor de exploatare, pentru a reacționa pe conexiunea descendentă la măsurarea unei amplitudini minime pe conexiunea ascendentă.

7.8.1 Spectrul radio alocat operatorilor de telefonie mobilă, conexiunea descendentă

În cadrul secțiunii au fost analizate disponibilitatea operatorilor de telefonie mobilă în punctul de măsură efectuate cu analizor de spectru respectiv terminal mobil inteligent ce dispune de un soft special de analiză a parametrilor de rețea.

Figura 7.29. *NB-RSRP, NB-RSRQ și alte date privind conexiunea descendentă Digi Mobil în punctul de monitorizare radio, obținute cu platforma de monitorizare Nestor.*

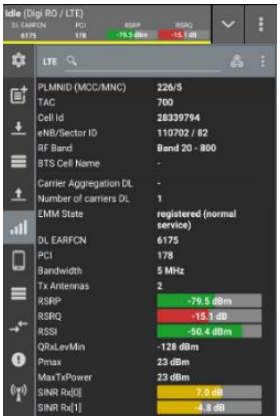


Figura 7.30. *Terminal mobil inteligent înregistrat în banda LTE 800 MHz.*

7.8.2 Bruiaj inteligent

În cadrul secțiunii au fost exemplificate considerații teoretice utilizate în cadrul realizării dispozitivului de bruiaj inteligent.

7.8.3 Estimarea efectului de bruiaj

În cadrul secțiunii au fost prezentate calcule cu privire la estimarea efectului de bruiaj în condițiile tehnice avute la dispoziție.
În Digi Mobil, în condiții de laborator, bruierea conexiunii descendente a fost demonstrată cu succes, datorită faptului că puterea parametrilor rețelei nu a depășit posibilitățile Hack-RF în materie de putere.

7.8.4 Implementarea bruiajului

Au fost prezentate pe larg aspectele practice și de funcționare ale bruiajului inteligent dezvoltat pentru atacuri de tip DoS.

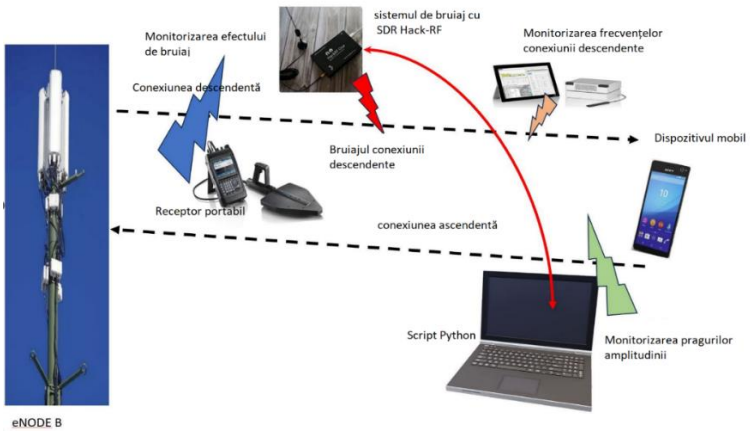
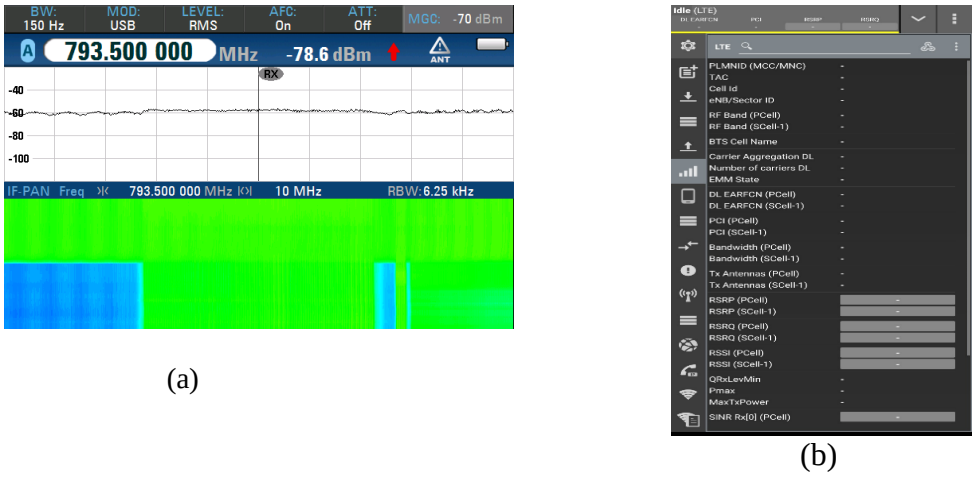


Figura 7.35. *Configurare experimentală pentru blocarea conexiunii descendente cu Nestor.*

Practic, pentru orice amplitudine peste -70 dBm care este detectată pe frecvențele de legătură ascendentă, furnizate de Nestor, este pornită o emisie pe frecvența canalului de radiofrecvență al conexiunii descendente corespondente, cu puterea maximă a Hack-RF. După 15 secunde, blocarea este oprită și procesul este reluat în buclă.
După mai multe încercări practice, s-a stabilit experimental faptul că efectul bruiajului, cu puterea furnizată de Hack-RF, se manifestă până la 7 metri, experiment confirmat și de calculele efectuate anterior, ale SIR.
În figura 7.37 (a), este ilustrat spectrul radio obținut cu PR100, care prezintă grafic manifestarea bruiajului pe frecvența de legătură descendentă 793,5 MHz. În figura 7.37 (b), este prezentat efectul dispozitivului de bruiaj asupra semnalului primit de terminalul mobil inteligent.



(a) (b)

Figura 7.36. *(a) Bruiajul conexiunii descendente (b) QualiPock monitorizarea frecvenței*

7.9 Recomandări cu privire la creșterea securității rețelelor de comunicații fără fir

Au fost făcute o serie întreagă de recomandări, pentru utilizatorii de rețele fără fir, pentru a fi conștienți de riscurile la care se expun în momentul în care decid să utilizeze astfel de rețele, precum și sfaturi parctice pentru a-și proteja datele expuse pe infrastructura radio.

Capitolul 8 Concluzii

8.1 Rezultate obținute

În capitolul 2, sunt prezentate considerații fundamentale cu privire la tehnologia GSM. Pentru o mai bună exemplificare a vulnerabilităților sesizate, în tehnologia GMS, au fost efectuate măsurători experimentale în operatorii de telefonie mobilă, Orange și Vodafone și au fost prezentate și tehnici și mijloace de localizare a unor dispozitive mobile.

Capitolul 3, prezintă considerațiile fundamentale ale tehnologiei 3G-UMTS, un predecesor al GSM, care vine să rezolve o parte dintre neajunsurile înregistrate în tehnologia precedentă. A fost demonstrat, în condiții de laborator, că un dispozitiv mobil poate fi localizat cu succes, cunoscând detalii cu privire la infrastructura operatorilor de telefonie mobilă activi într-un punct de măsură, respectiv a corespondenței certe între frecvența descendentă pe care comunică rețeaua cu dispozitivul mobil și cea a frecvenței ascendente pe care comunică dispozitivul mobil cu rețeaua.

În capitolul 4, au fost prezentate aspecte de ordin teoretic ale tehnologiei 4G-LTE, care au vizat procesul de autentificare a unui dispozitiv mobil în rețea, respectiv de testare a posibilităților de localizare a unui dispozitiv mobil ce lucrează în 4G. Rezultatele obținute au fost apreciate, oferind o perspectivă nouă de localizare, la interior, a unor dispozitive mobile, prin cunoașterea unor caracteristici ale conexiunilor ascendente în care se comunică spre rețea.

Capitolul 5 a vizat aspectele teoretice ale tehnologiei 5G SA, dar și măsurători radio pentru a oferi o imagine asupra unei rețele care utilizează tehnologia 5G SA. În România, operatorii de telefonie mobilă nu au avansat un termen pentru implementarea tehnologiei 5G SA, în prezent, ei furnizează servicii de date utilizatorilor prin intermediul 5G NSA. Partea a doua a capitolului 5 prezintă, în premieră, măsurători radio în teren ale conexiunilor radio descendente ale operatorilor de telefonie mobilă ce oferă servicii abonaților. Măsurătorile au vizat, totodată, o imagine asupra felului în care va arăta spectrul radio în momentul la care se va implementa tehnologia 5G. Din aspectele prezentate în cadrul capitolului, se remarcă prezența tehnologiei GSM la toți operatorii de telefonie mobilă din Germania, respectiv implementarea 4G în benzile tradiționale, 800/1800/2600 MHz, iar tehnologia 5G în benzile de 700/2100/3500 MHz.

În capitolul 6, au fost prezentate aspecte teoretice ale tehnologiilor WiFi și BLE, cu accent pe vulnerabilitățile evidențiate în urma testelor experimentale, respectiv după analiza rezultatelor obținute de emitere a unor recomandări pentru utilizatori, de creștere a securității rețelelor.

Capitolul 7 reprezintă măsurători experimentale ale tehnologiilor studiate pe parcursul cursurilor doctorale. De data aceasta, ele au fost derulate în municipiul București în 5 puncte de măsură, alese astfel încât să reflecte o realitate radio a operatorilor de telefonie mobilă activi pe teritoriul național.

Rezultatele măsurătorilor au evidențiat că o rețea de telefonie mobilă care dispune de o diversificare de tehnologii în benzile de frecvență, poate oferi, în condițiile actuale, chiar și viteze de 217 MB/s (obținuți în punctul de măsură al zonei Obor, operator Orange România, tehnologie LTE, implementată în banda de frecvență 2600 MHz). Experimentele practice au vizat de asemenea evidențierea în spectrul radio și a dispozitivelor care utilizează tehnologia WiFi și BLE. S-a constatat faptul că apariția și dezvoltarea IoT a făcut ca utilizarea dispozitivelor care lucrează în astfel de rețele, să fie foarte răspândite, fapt confirmat de măsurătorile efectuate în teren.

Întrucât atacurile prin intermediul infrastructurii radio sunt cele mai frecvente care se pot manifesta asupra dispozitivelor mobile, ce lucrează în tehnologiile GSM, LTE și 5G, ultima parte a capitolului 7 prezintă un sistem de bruiaj inteligent dezvoltat cu echipamente accesibile de tip SDR (Software Defined Radio), cu sisteme de antene directive, pretabil a fi utilizat în incinta unei facilități de tip închisoare.

8.2 Contribuții originale

Rezultatele cercetărilor și studiilor efectuate pe toată perioada ciclului doctoral au condus spre contribuțiile originale cuprinse în prezenta lucrare care pot fi sintetizate astfel:

1. Evidențierea vulnerabilităților rețelelor de comunicații, din România, ce utilizează tehnologia GSM;
2. Teste practice de localizare a unui dispozitiv mobil ce utilizează tehnologia GSM;
3. Determinarea locației de amplasare a unui BTS în tehnologia GSM, prin măsurători practice;
4. Studiu privind expunerea pe interfața radio a parametrilor specifici terminalelor mobile;
5. Evidențierea vulnerabilităților rețelelor de comunicații, din România, ce utilizează tehnologia UMTS;
6. Localizarea unui dispozitiv mobil ce utilizează tehnologia UMTS, în baza parametrilor de emisie pe conexiunea ascendentă;
7. Studiu privind vulnerabilitatea rețelelor de comunicații ce utilizează tehnologia LTE;
8. Provocări ale procedurii de localizare unui dispozitiv mobil ce utilizează tehnologia LTE, cu receptor radio, în baza parametrilor de emisie;
9. Studiu privind vulnerabilitatea rețelelor de comunicații ce utilizează tehnologia 5G;

10. Evidențierea prin măsurători a parametrilor rețelelor de comunicații 5G SA, în condițiile în care în România nu sunt furnizate servicii 5G SA.
11. Demonstrații practice ale vulnerabilităților rețelelor de comunicații ce utilizează tehnologia Wi-Fi;
12. Demonstrarea vulnerabilităților funcției Apelare Wi-Fi;
13. Provocări ale tipologiilor de atacuri prin infrastructura Wi-Fi;
14. Evidențierea vulnerabilităților rețelelor de comunicații ce utilizează tehnologia BLE;
15. Studiu privind atacurile prin infrastructura BLE;
16. Măsurători practice ale disponibilității serviciilor operatorilor de telefonie mobilă din 5 puncte de măsură, a vitezei de trafic pentru fiecare bandă de frecvență alocată, respectiv în fiecare tehnologie disponibilă.
17. Studiu comparativ al disponibilității serviciilor operatorilor de telefonie mobilă din 5 puncte de măsură.
18. Studiu privind disponibilitatea rețelelor de comunicații fără fir, identificarea punctelor de acces și a utilizatorilor, care folosesc tehnologia WiFi, în 5 puncte de măsură.
19. Studiu privind dezvoltarea unui sistem de bruiaj inteligent în tehnologiile GSM și LTE, prin identificarea unui prag minim al nivelului de semnal pentru frecvențele conexiunii ascendente.
20. Implementarea soluției de bruiaj inteligent, pentru tehnologia LTE în banda de 800MHz.

8.3. Lista lucrărilor originale publicate sau în curs de publicare

În perioada studiilor doctorale am publicat 11 articole, din care 10 articole de conferință și un articol în jurnalul Applied Science, cotat Q2.

Rezultatele articolului [C1] sunt inserate parțial în cadrul capitolului 2, rezultatele articolelor [C2] și [C3] vor fi regăsite parțial în capitolul 3, [C4] vor fi regăsite parțial în capitolul 4 iar rezultatele articolului [J1] și [C5]au fost utilizate în cadrul capitolelor 6 și 7.

Rezultatele obținute în capitolul 7 “Măsurători experimentale” au fost constituite într-un draft de articol, care a fost trimis spre validare către Journal Applied Sciences, Section Computing and Artificial Intelligence, Special Issue Trends and Prospects for Wireless Sensor Networks and IoT Articolul transmis cu titlul: **“A study case, in Bucharest, regarding real mobile internet speed on mobile network operators”**, authors: Cristian Capota, Mădălin Popescu, Simona Halunga & Mircea Popescu.

Totodată, în cadrul capitolului 7 au fost introduse parțial rezultate obținute și publicate în articolul [J1] :

[J1] Cristian Capota, Mădălin Popescu, Eduard-Marian Bădulă, Simona Halunga, Octavian Fratu and Mircea Popescu. **Intelligent jammer on mobile networks LTE technology. A study case in Bucharest**, journal Applied Sciences, Section

Computing and Artificial Intelligence, Special Issue Trends and Prospects for Wireless Sensor Networks and IoT ISSN 2076-3417, Appl. Sci. 2023, 13, 12286. https://doi.org/10.3390/ app13221228. Publicat la data de 13.11.2023.

Articole de conferință:

[C1] Capotă, C., Fratu, O., Stancu, E., Găină, M., & Vizireanu, D. (2020, December). **Vulnerabilities in authentication process GSM standard: RF measurements, theoretical and practical aspects**. In Advanced Topics in Optoelectronics, Microelectronics and Nanotechnologies X (Vol. 11718, pp. 505-511). SPIE. ISBN 978-1-5106-4272-0 ISSN 0277-786X eISSN 1996-756X IDS Number BR2VD, DOI 10.1117/12.2571255.

[C2] Capotă, C., Halunga, S., Eugen, S., & Mădălin, P. (2021, May). **Vulnerabilities of UMTS-LTE Authentication Process–Theoretical and Practical Aspects during RF Measurements.** In 2021 IEEE International Black Sea Conference on Communications and Networking (pp. 1-5). IEEE. (WOS:000892556200053) ISBN 978-1-6654-0308-5 ISSN 2375-8236 IDS Number BU3OZ, DOI 10.1109/BlackSeaCom52164.2021.9527855.

[C3] Capota, C., Halunga, S., Fratu, O., Eugen, S., & Mădălin, P. (2021, May). Security **Aspects and Vulnerabilities in Authentication Process WiFi Calling–RF measurements.** In 2021 IEEE International Black Sea Conference on Communications and Networking (pp. 1-5). IEEE. (WOS:000892556200052) ISBN978-1-6654-0308-5 ISSN2375-8236 IDS Number BU3OZ. DOI 10.1109/BlackSeaCom52164.2021.9527884.

[C4] Capota, C. N., Popescu, M. V., Halunga, S., & Fratu, O. (2023, March). **Challenges in identifying and direction finder of electronic equipment in indoor environment, on mobile standards.** In Advanced Topics in Optoelectronics, Microelectronics, and Nanotechnologies XI (Vol. 12493, pp. 665-672). SPIE https://doi.org/10.1117/12.2642865.

[C5] Capotă, C. N., Popescu, M., Halunga, S., & Fratu, O. (2023, June). **Challenges In Spoofing Bluetooth Low Energy Devices In An IOT Environment.** In 2023 15th International Conference on Electronics, Computers and Artificial Intelligence (ECAI) (pp. 1-5). IEEE. DOI 10.1109/ECAI58194.2023.10193980.

[C6] Badea, A., Halunga, S., Berceanu, M., Găină, M., Capotă, C., & Stancu, E. (2019, October). **Influence of Manchester encoding over spreading codes used in multiple access techniques for IoT purposes.** In 2019 IEEE 25th International Symposium for Design and Technology in Electronic Packaging (SIITME) (pp. 216-219). IEEE. (WOS:000564733700043) ISBN 978-1-7281-3330-0 ISSN 2641-287X IDS NumberBP8ER. DOI 10.1109/SIITME47687.2019.8990780.

[C7] Stancu, E., Capotă, C., Badea, A., Halunga, S., & Vizireanu, N. (2020, December). **Measurements of the emission parameters of a WiMax BTS under interference conditions.** In Advanced Topics in Optoelectronics, Microelectronics and Nanotechnologies X (Vol. 11718, pp. 538-543). SPIE.

(WOS:000641147900076) ISBN 978-1-5106-4272-0 ISSN 0277-786X eISSN 1996-756X IDS NumberBR2VD.

[C8] Stancu, E., Halunga, S., Fratu, O., Florea, C., Berceanu, M. G., & Cristian, Capotă. (2020, June). **Spectral analysis in the 2.4 GHz WiFi band in Bucharest.** In 2020 13th International Conference on Communications (COMM) (pp. 435-438). IEEE. (WOS:000612723900077) ISBN 978-1-7281-5611-8 IDS Number BQ6NO, https://doi.org/10.1117/12.2571698.

[C9] Stancu, E., Capotă, C., Halunga, S., & Fratu, O. (2019, September). **Mutual Electromagnetic Perturbations-RF Measurements in the VHF and UHF Frequencies in Bucharest: Theoretical and Practical Aspects.** In Proceedings of the 6th Conference on the Engineering of Computer Based Systems (pp. 1-4). ISBN 978-1-4503-7636-5 IDS Number BO7PE, DOI https://doi.org/10.1145/3352700.3352721.

[C10] Popescu, M., Capotă, C., Țene, I., Găină, M., & Halunga, S. (2023, March). **Vulnerabilities of Windows systems through Wi-Fi infrastructure.** In Advanced Topics in Optoelectronics, Microelectronics, and Nanotechnologies XI (Vol. 12493, pp. 704-711). SPIE; https://doi.org/10.1117/12.264312.

8.4. Oportunități de dezvoltare ulterioară

O provocare imediată o reprezintă primirea acceptului de publicare a articolului cu titlul: **"A study case, in Bucharest: regarding real mobile internet speed on mobile network operators"**, authors: Cristian Capota, Mădălin Popescu, Simona Halunga & Mircea Popescu. Articolul a fost transmis către jurnalul Applied Science.

De asemenea, pe termen mediu (6-12 luni) intenționez ca, de îndată ce rețelele 5GSA sunt implementate în România, să adaptez soluția tehnică experimentală de bruiaj inteligent la această tehnologie și să publicăm rezultatele cercetărilor realizate.

Totodată, voi extinde studiul rețelelor de comunicații telefonice mobile, pentru a identifica și semnala vulnerabilitățile tehnologiilor utilizate în a oferi servicii abonaților. Aceste studii vor fi extinse și asupra tehnologiei 5G SA, la momentul la care aceasta va fi implementată în rețelele operatorilor de telefonie mobilă din România. Voi testa vitezele de trafic de date obținute în tehnologia 5G SA, cu prezentarea în conferințe sau reviste de specialitate.

Toate aceste rezultate vor fi subiectul central al publicațiilor mele viitoare, precum detalierea configurației rețelelor de comunicații fără fir, prezentarea detaliilor cu privire la benzile de frecvență și tehnologiile implementate, care trebuie avute în vedere atunci când sunt realizate teste de viteză și de disponibilitate a rețelei.

Referințe bibliografice:

[4] Ericsson mobility report,“https://www.ericsson.com/assets/local/mobilityreport/documents/2018/ericsson-mobility-report-november-2018.pdf. [On-line]”.

[13] 3GPP. 2015. 3GPP System Architecture Evolution (SAE); Security architecture. TS33.401 (2015). Latest release: 15.3.0 (2018-03-27). „http://www.3gpp.org/DynaReport/33401.htm” . [On-line]

[14] 3GPP. 2015. Characteristics of the Universal Subscriber Identity Module (USIM) application. TS31.102 (2015). Latest release: 15.0.0 (2018-04-03). „http://www.3gpp.org/DynaReport/31102.htm”. [On-line]

[34] Arcep (Autorite de Regulation des Communications Electroniqyuea et des postes, Republique Francaise), 5G: Issues and Challenges, March 2017. [On-line].

[35] Blanco, Bego et. Al., Technology pillars in the architecture of the future 5G mobil networks: NFV, MEC and SDN, Computer Standards&Interfaces 54 (2017) 216-228. [On-line].

[39] Dubrova, Elena si Hell, Martin - Espresso: A Stream Cipher for 5G Wireless Communication Systems, https://eprint.iacr.org/2015/241.pdf [On-line].

[41] Frias, Zoraida, 5G networks; Will technology and policy collide, Telecommunications Policy (2017), http://dx.doi.org/10.1016/j.telpol.2017.06.003. [On-line].

[43] Morgado, Antonio et. al., A survey of 5G technologies: Regulatory, standardization and industrial perspectives, Digital Communications and Networks (2017), https://doi.org/10.1016/j.dcan.2017.09.010. [On-line].

[47] Standardul ITU-R M.2083. [On-line].

[49] 3GPP. 2002. 3G Security; Wireless Local Area Network (WLAN) Interworking Security. TS33.234 (2002). Latest release: 14.0.0 (2017-03-27). „http://www.3gpp.org/DynaReport/33234.htm”. [On-line].

[50] J. Baek, S. Kyung, H. Cho, Z. Zhao, Y. Shoshitaishvili, A. Doupé, GJ. Ahn."Wi Not Calling: Practical Privacy and Availability Attacks in Wi-Fi Calling", Proceedings of the 34th Annual Computer Security Applications Conference, Computer Science, 2018. [On-line].

[73] E. M. Bădulă, S. Halunga, O. Fratu and M. Popescu, "Intelligent Blocking System for Mobile Communications Initiated by Unauthorized Users," 2023 15th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Bucharest, Romania, 2023, pp. 01-06, doi: 10.1109/ECAI58194.2023.10194110.

[91] R. P. Jover. "LTE security, protocol exploits and location tracking experimentation with low-cost software radio" July 2016. arXiv preprint arXiv:1607.05171 (2021)[online https://arxiv.org/abs/1607.05171v1]. [On-line].