NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY POLITEHNICA BUCHAREST

Doctoral School of Electronics, Telecommunications and Information Technology

Decision No. 163 from 21-12-2023

THESIS OF DOCTORATE

Ing. Cristian Nicolae CAPOTA

CONTRIBUTIONS ON THE SECURITY OF NEXT GENERATION MOBILE TELEPHONE COMMUNICATIONS

DOCTORAL COMMITTEE

Prof. dr. ing. Ion MARGHESCU National University of Science and Technology Politehnica Bucharest	President
Prof. dr. ing. Simona HALUNGA National University of Science and Technology Politehnica Bucharest	Scientific adviser
Prof. dr. ing. Corina NAFORNIȚĂ Politehnica University of Timișoara	Referent
Prof. dr. ing. Ioan NICOLAESCU Bucharest Military Technical Academy	Referent
Prof. dr. ing. Teodor PETRESCU National University of Science and Technology Politehnica Bucharest	Referent

BUCUREŞTI 2024

Cuprins

Introduction

Presentation of the doctoral domain

Purpose of the thesis

The main objective of this paper is to raise awareness among a wide audience about the presence of exploitable vulnerabilities by malicious persons, in technologies already implemented, or under implementation, at the level of mobile operators in Romania. At the same time, we wanted to present simple methods to counteract these identified vulnerabilities, as well as to protect communication channels at the user-network interface level that can significantly reduce the security risks presented in this paper. The experimental measurements created a current and clear picture regarding the radio signal coverage of mobile operators in Bucharest, in 2G-4G technologies, determining data transfer speeds for all operators in each frequency band and available technology and highlighting Wi-Fi devices (Access Points and Users) and devices using Bluetooth Low Energy technology. Experiments and measurements carried out in the field have led to revealing the ease with which a malicious person can carry out Denial of Service actions on users in an indoor space. We have developed an intelligent jamming system capable of broadcasting on one frequency, upon sensing a minimum amplitude threshold on another frequency, in order to block access to the network from a certain facility (e.g. prisons).

Content of the thesis

The thesis aims, in its 8 chapters, to analyze fundamental elements of operation and security of wireless communications networks, in order to be used in practical experimental scenarios, applied for communication standards available at the level of mobile operators in Romania, respectively laboratory tests of the standards to be implemented, with direct reference to the IOT-5G ecosystem.

As a novelty, it is proposed to apply the radio fingerprint technique of the tested mobile devices, detailing the main parameters of the networks, namely the radio availability of mobile operators, through the integrated provision of data services through base stations and open APN.

Chapter 1 Introduction

1.1 Short history

In the section, aspects related to the history of mobile telephone communications were presented. Currently, we are engaged in an extensive process of implementation at European level of the fifth generation of mobile communications, 5G NSA and 5G SA. [4]

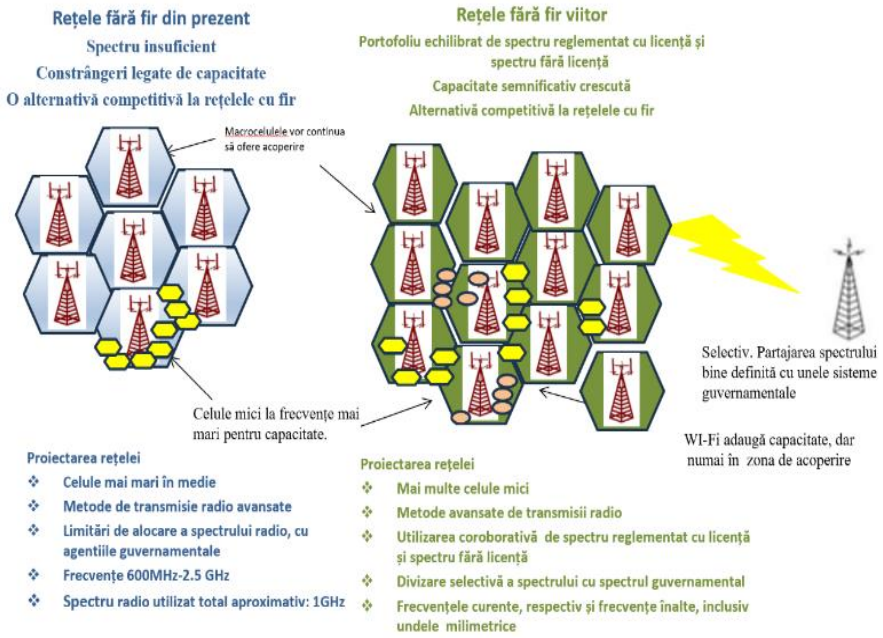


Figure 1.1. The present and future of wireless communications networks

1.2 The evolution of communication systems from 1G to 6G

The main features of the communication standards from 1G to the present 5G were presented, namely considerations regarding future 6G networks, respectively areas of practical applicability, interconnection of mobile devices.

Chapter 2: Basic considerations of wireless communications networks

Fundamental considerations of 2G-GSM technology

Considered obsolete and technologically outdated by most specialists in the field, with multiple vulnerabilities in terms of authentication and security of user data, the GSM standard is still present in the networks of mobile operators in Romania.

2.1. 2G-GSM network architecture

Theoretical aspects regarding the GSM architecture were presented, highlighting the main parameters, respectively practical measurements to highlight vulnerabilities regarding authentication.

2.2 Encryption algorithms used in GSM technology

In GSM technology, unilateral authentication of mobile stations to base stations is achieved by using symmetric encryption algorithms, also protecting the privacy of subscribers by using a secret key.

2.3 Practical aspects of applied doctoral research in GSM network

2.3.1. Authentication of mobile devices in GSM technology

The practical part of the GSM Network Authentication process was achieved under laboratory conditions: by excluding other mobile terminals in the immediate vicinity, respectively placing the devices used in an anechoic chamber.

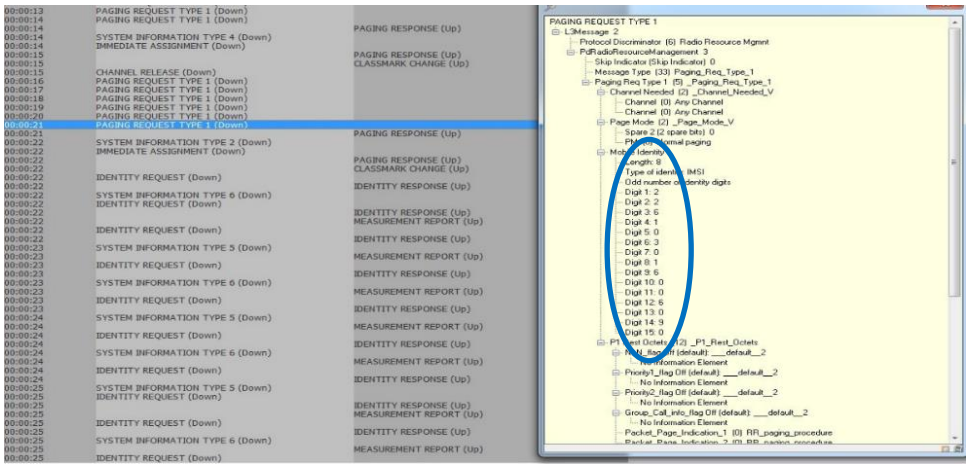


Figure 2.6. (b) *IMSI is transmitted.*

Aspects resulting from practical measurements of GSM network vulnerabilities were presented.

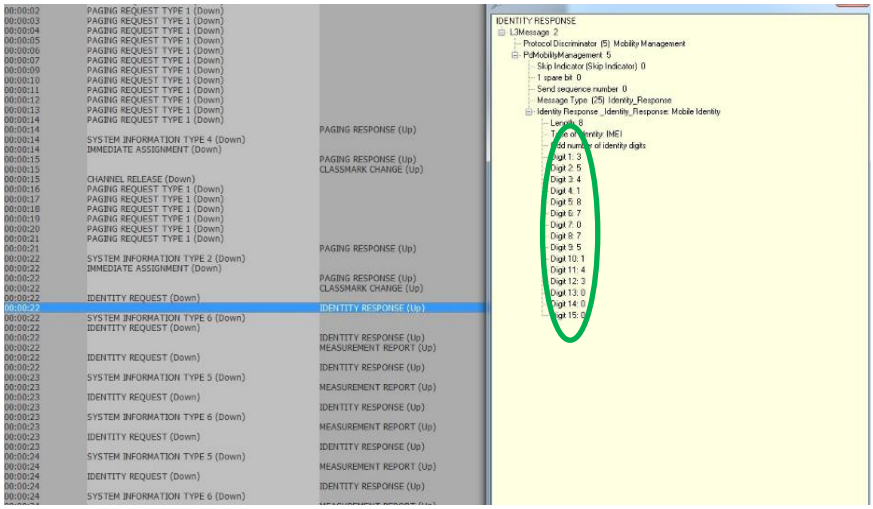


Figure 2.7. *The IMEI parameter is passed.*

2.3.2 Location of mobile devices using GSM technology

Under the section were presented the experimental tests performed in order to locate a mobile device operating in the GSM standard, in the network of operators Orange Romania and Vodafone Romania.

Currently, at the level of 112 emergency services, localization is done at BTS level – Cell Code, mobile operators in Romania do not offer services for accurate location of mobile devices in a geographical area, as in our country legal regulations do not impose such provisions.

Locating a mobile device in the Orange Romania network

Figure 2.9 shows all Broadcast Control Channels (BCCHs), available at the measurement point, for the operator Orange Romania.

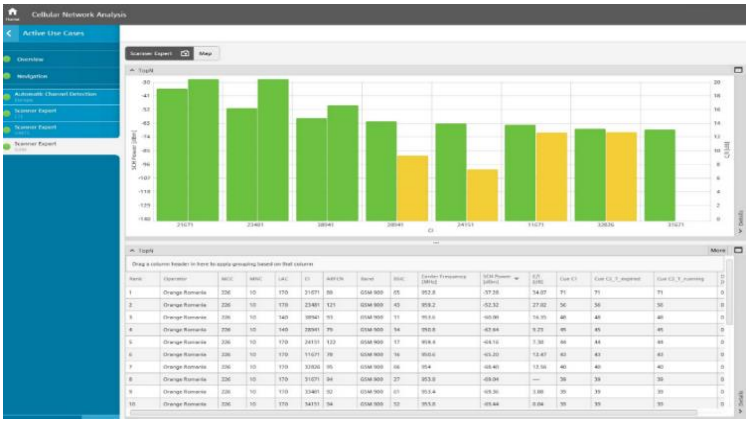


Figure 2.9. *Measurements of BTS, BCCH in GSM, Orange Romania*

In order to locate a device using the GSM standard, the channel, the cell code serving the area where the measurements were made, as well as the signal level received on the uplink of the network were identified. Given the nature of full-duplex communication in the GSM standard, the radio link between the mobile terminal and the network is performed on two different frequencies, the upward connection between the terminal and the network (UpLink) and the downward connection between the network and the mobile terminal (DownLink-DL).

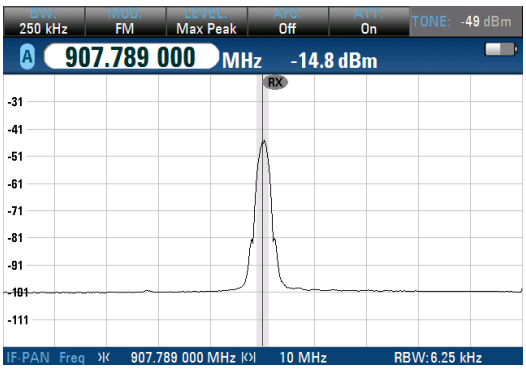


Figure 2.12. *Signal level measured on uplink*

Locating a mobile device in the network of the operator Vodafone Romania

The way of working is similar to locating a mobile device in the network of the operator Orange Romania.

Chapter 3 Basic considerations of 3G-UMTS technology

The 3G standard plays a crucial role in this network evolution, so mobile/wireless internet has become widely available to users, which has raised new and new concerns about security issues. [13]

3.1 3G-UMTS network architecture

The main components of the 3G-UMTS network were presented. [13]

3.2 Authentication of mobile devices in UMTS technology

In the section was presented the set of security mechanisms. [13] and [14] as well as the procedure for authentication by practical examples.

3.3 Practical experiments and radio measurements in UMTS technology

The measurements aimed to highlight the radio footprint of mobile terminals in the frequency spectrum, the emission level characteristic of a communication with the base cell in the authentication process, respectively the location of a mobile device.

3.3.1 Authentication of mobile devices in UMTS technology

Details of the authentication process, which can be divided into three stages, have been presented. Step 1 in which the mobile terminal transmits at the request of the network in order to initiate the authentication process, the IMSI parameter, step 2, the transmission of the IMEI parameter, respectively step 3, the assignment by the UMTS network of the P-TMSI parameter.

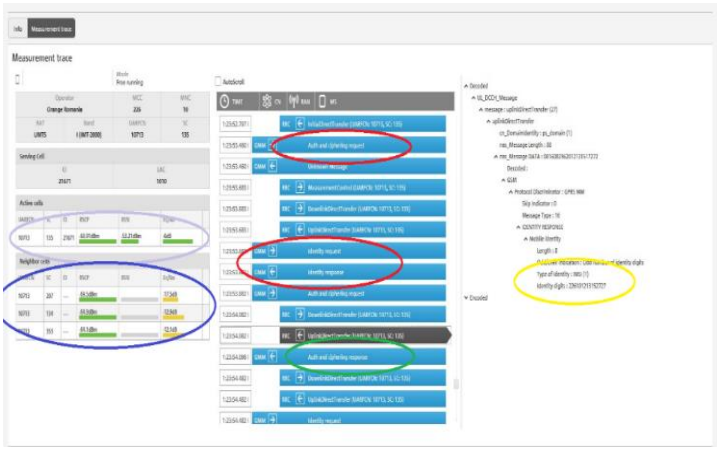


Figure 3.5. *Authentication process in 3G-UMTS, IMSI transmission*

Figure 3.6 shows step 2 of the process of authentication of a mobile terminal on the network, through a request, the network requests the identity of the equipment used, in order to validate access to the network.

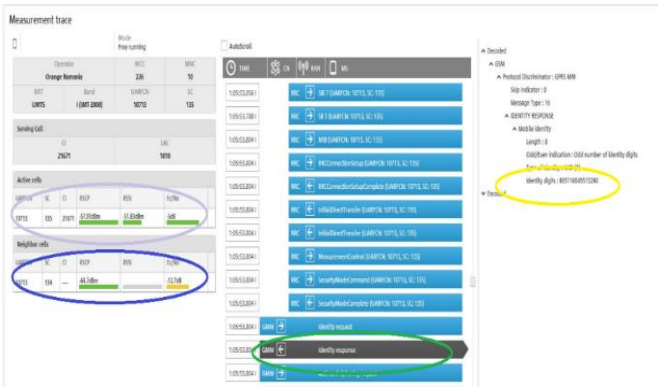


Figure 3.6. *Authentication process in 3G-UMTS, IMEI transmission*

3.3.2 Location of mobile devices using 3G-UMTS technology

Measurements of the 3G-UMTS standard were made in the network of the corresponding operator Orange Romania, UARFCN, respectively the technical parameters characteristic of the connection from the network to the mobile terminal. In figure 3.12, it can be seen that when the physical distance between the antenna of the handheld receiver and the mobile device decreases, the signal level increases to -24.7 dBm.

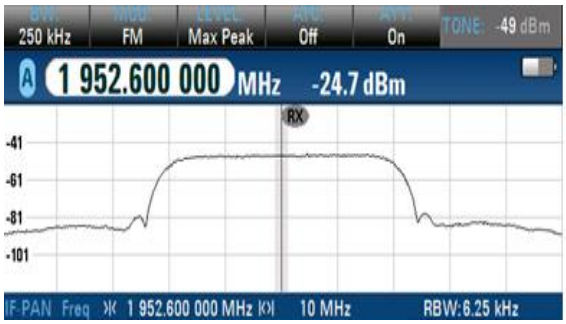


Figure 3.12. *Signal level measured in proximity to mobile device.*

Chapter 4: Fundamental considerations of 4G-LTE

The 4G network developed by the 3GPP group, (3rd Generation Partnership Project), the first generation of the Long-Term Evolution standard, is a significant evolution of the 3G standard, which paves the way for a radical development of the network architecture, along with the benefits offered to subscribers.

4.1 4G - LTE network architecture

Theoretical aspects regarding the architecture of the 4G-LTE network and the main components, as well as their role in the network were presented. [13]

4.2. Mobile Device Authentication in LTE Technology

In this section, theoretical aspects regarding the vulnerabilities of 4G-LTE technology have been formulated.

4.3 Experimental radio evaluations in LTE technology

Within the section were presented radio measurements of signal levels, as well as the authentication procedure of a mobile terminal in the 800 MHz band where LTE services are provided, but also aspects related to location determination.

4.3.1 Radio link measurements in the 800 MHz frequency band LTE technology

The measurements aimed to highlight the authentication process of mobile terminals in the network, the emission level characteristic of a communication with the base cell, respectively the location of a mobile device.

4.3.2 Autentificarea dispozitivelor mobile în tehnologia LTE

The main change that was introduced by 3GPP when authenticating a mobile terminal in the LTE network is given by the fact that the IMEI parameter is no longer used in the authentication process, implicitly required by the network, thus eliminating the vulnerability of previous standards.

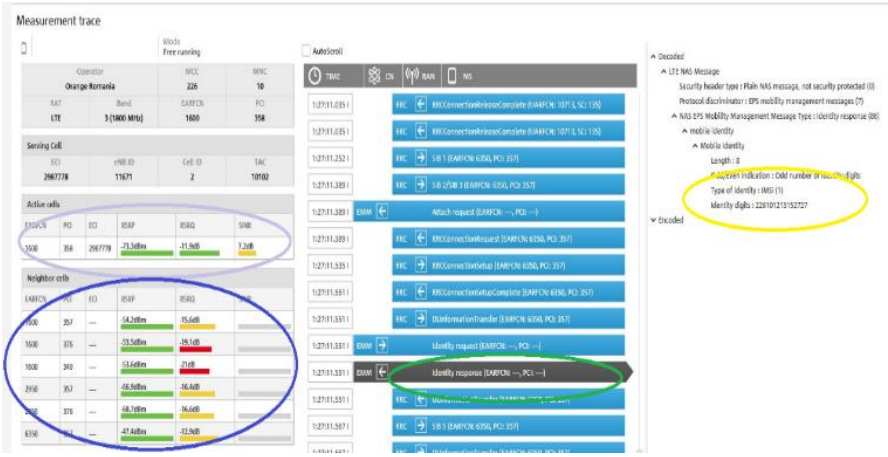


Figure 4.4. *Successful completion of authentication and IMSI transmission.*

Upon successful completion of the authentication session, the corresponding IMSI is assigned a temporary parameter used in 4G GUTI networks, which is equivalent to the temporary TMSI parameter used in the GSM standard.

4.3.3 Locating mobile devices using LTE technology

Practically locating devices using the 4G standard, in a laboratory environment, is a challenge, as in the bandwidth (RB) there can be several devices communicating at the same time with the network. To determine the position of the device, the RSSI signal level is measured in figure 4.6, in the LTE 20 band, the bandwidth is 10 MHz. [35]

The definite correspondence of frequencies between the uplink channel and the downlink channel reveals that for the EARFCN 6350 channel, in the 800MHz band 20, measured in an indoor environment, the uplink frequency is 852 MHz.

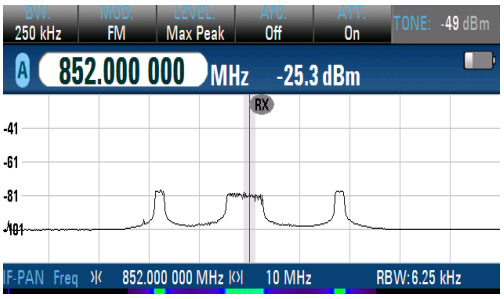


Figure 4.8. *Uplink measured in 20 band (800MHz) LTE standard.*

Chapter 5 Basic considerations of 5G communication networks

5G communication networks are designed to connect industries (such as manufacturing and processing, smart transport, smart grids and e-health), but also to serve people and society, basically in a new radio ecosystem. [34] și [41]

5.1 5G communication network architecture

Theoretical considerations of 5G network architecture were presented in the section.

5.2 Security requirements and procedures for 5G communication networks

Main security requirements and corresponding procedures for the RAN of 5G communication networks were presented [43] și [47]

5.2.1 Key workstream

Key workstream refers to the process by which two entities, a mobile device and a 5G network, establish a common encryption key to ensure the privacy and security of their communications. [39]

5.2.2 Home network authentication and control

Details were presented on mobile device authentication [39] and methods to increase home network control through network segmentation.

5.3 Radio measurements in 5G communication networks

In the context of the implementation of 5G-NSA technology, by the mobile operator Orange Romania, radio measurements were performed in laboratory conditions, in

order to visualize a downward connection between the network and mobile terminals.

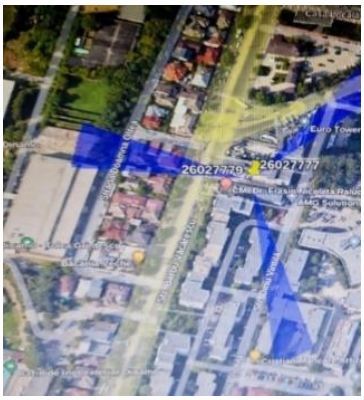


Figure 5.4. *Propagation prediction representation of a cell site providing 5G NSA services in Google Earth.*

During an internship included in the OPTIM Research project developed by UPB, I managed to undertake applied research activities on this 5G SA technology, measurements presented in figure 5.5.

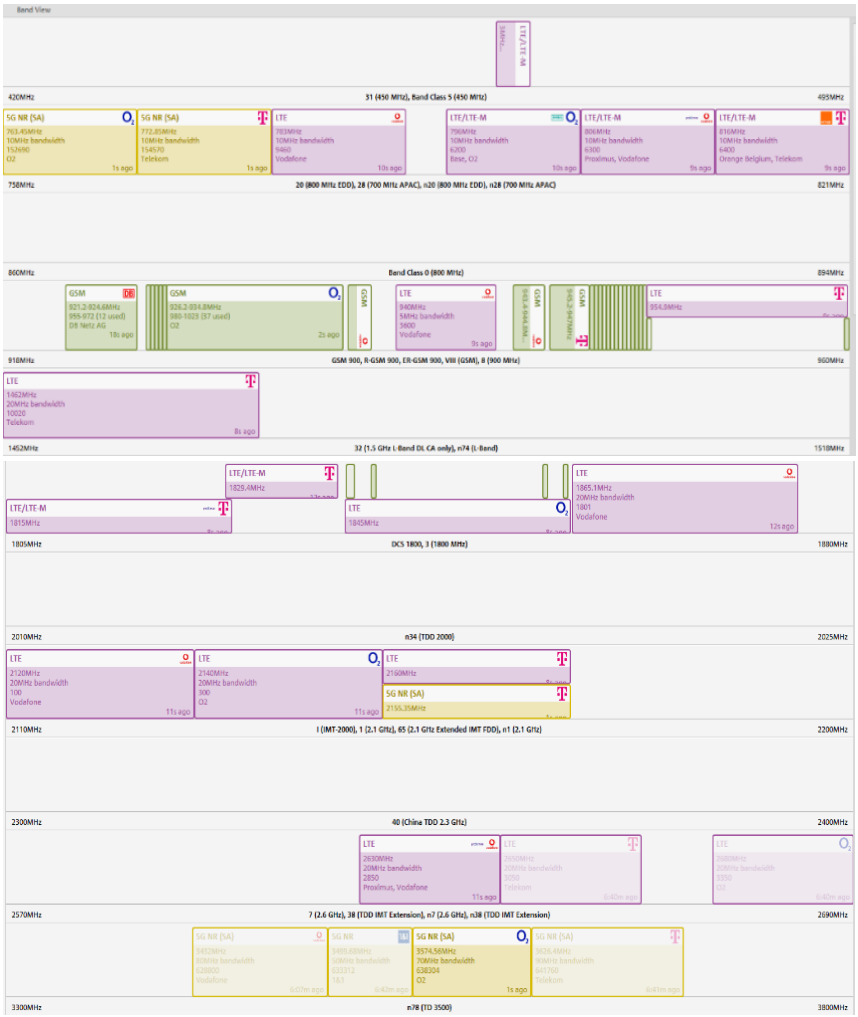


Figure 5.5. *Spectral diagram of mobile operators at the measurement point.*

Analysis of figure 5.5 reveals the following:

- GSM technology, marked in green, is implemented by all mobile operators, active at the measuring point.
- UMTS technology is totally excluded;
- The presence of LTE – 4G technology (marked in purple) in frequency bands:
    - ✓ 800 MHz LTE and LTE-M2M operators Vodafone, O2 and Telekom;
    - ✓ 900 MHz Vodafone and Telekom;
    - ✓ 1500 MHz Telekom;
    - ✓ 1800MHz, operators Vodafone, O2 and Telekom;
    - ✓ 2100 MHz, operators Vodafone, O2 and Telekom;
    - ✓ 2600 MHz, operators Vodafone, O2 and Telekom.
- Predominant presence of 5G SA technology (marked in yellow) in frequency bands:
    - ✓ 700 MHz, band n20, operators O_2 and Telekom;
    - ✓ 2100 MHz, band n1, operator Telekom;
    - ✓ 3500 MHz, band n78, operators O_2 and Telekom.

Chapter 6 Basic considerations of WiFi and BLE networks

The Internet of Things (IoT) is a paradigm in technology that refers to the connection, interconnection and communication of physical devices or smart objects through the Internet. [49].

The main features of IoT devices were presented.

6.1 Networks working in WiFi technology

6.1.1 Network architecture in WiFi technology

Within the section, the architecture of WiFi networks was described, the main components, as well as the connection steps between a mobile device and a WiFi network.

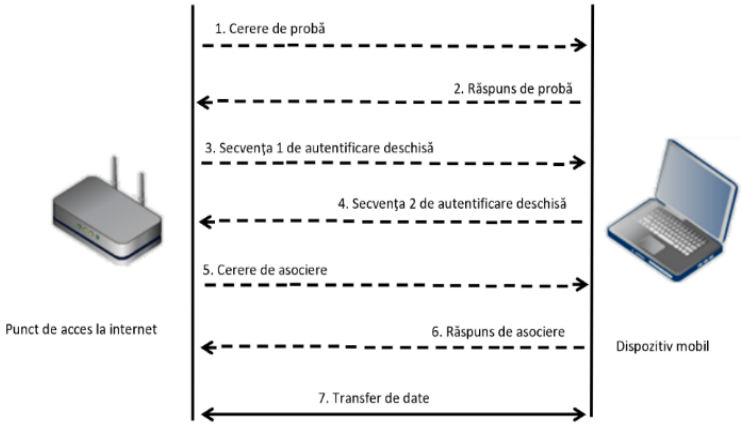


Figure 6.2. 802.11 authentication and association process.

6.1.2. Practical tests to highlight WiFi vulnerabilities

The subsection includes RF signal level measurements, i.e. methods for positioning devices and WiFi service provider in a laboratory environment in the WiFi standard.

6.1.3.1 Radio measurements of the mobile terminal for WiFi calling function

The measurements carried out aimed at identifying in the radio spectrum allocated to WiFi the radio transmission of the AP, respectively on the screen of the mobile terminal of the AP, which is available to provide services to users in the vicinity.

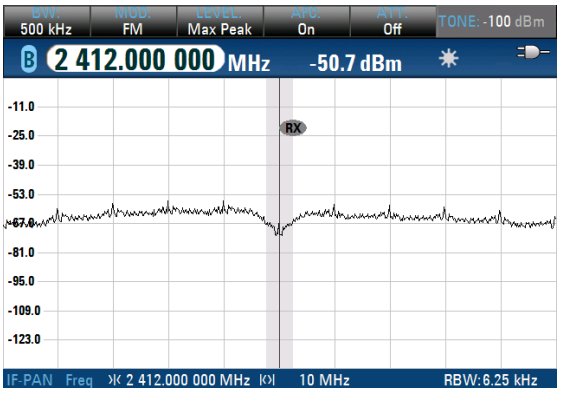


Figure 6.9. *The signal level of the clone AP.*

6.1.3.2 Security testing of WiFi calling feature

The predisposition of mobile devices to select the WiFi network based on the aforementioned parameters, according to WiFi calling standards makes them susceptible to fetch attacks (Man in the Middle - MitM). [50]

6.1.3.3 Takeover attacks

A Man in the Middle (MitM) attack involving configuring a clone AP with the same radio parameters as the valid router, the same Extended Service Set Identifier (ESSID), encryption, cipher and key was presented. The clone AP will be placed between the real network and the mobile device so that it becomes more attractive to the target. [50]

6.1.3.4 Target identification

Under the section, details on the authentication procedure, respectively the practical cloning of an AP, were presented.

6.1.3.5 AP clone

The analysis of data packets obtained from WiFi capture, respectively the identified vulnerabilities, were presented. [73].

6.2 Networks working in Bluetooth Low Energy technology

6.2.1 Bluetooth introduction

A brief history of BLE networks was presented in the section.

6.2.2 BLE architecture and measurements of radio channels

There were presented aspects related to the architecture of BLE networks, radio measurements in the radio system and the main components.

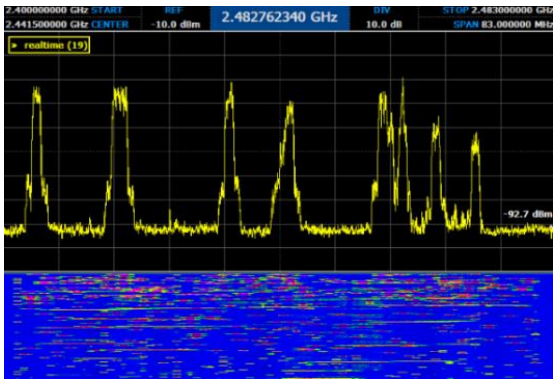


Figure 6.15. *RF measurements of the BLE spectrum.*

6.2.3 Authentication process in BLE networks

Details were presented regarding the authentication procedure of BLE devices, respectively a takeover attack on the BLE connection.

The entire communication process has four phases – advertising, initiating, connecting and exchanging. The peripheral device sends timed advertising packets. The central device scans and uses advertising packages to find the peripheral device.

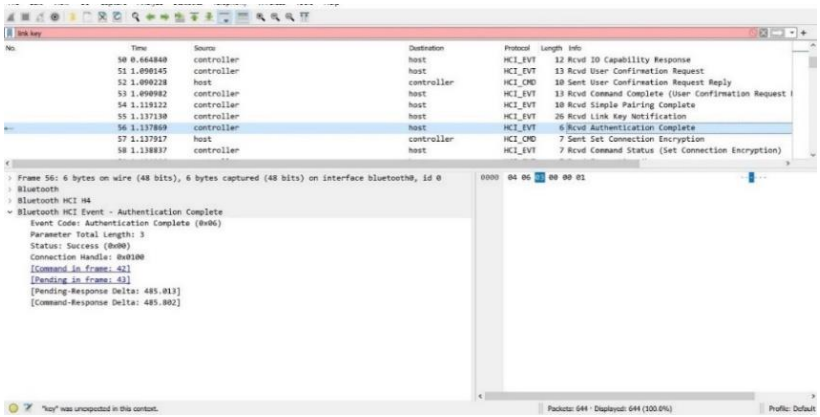


Figure 6.17. *Authentication is valid and complete.*

In order to identify and highlight the authentication process of some devices working in the BLE standard, the connection between the 2 devices was monitored and thus the .pcap file was obtained, which was analyzed with the help of the WireShark software application.

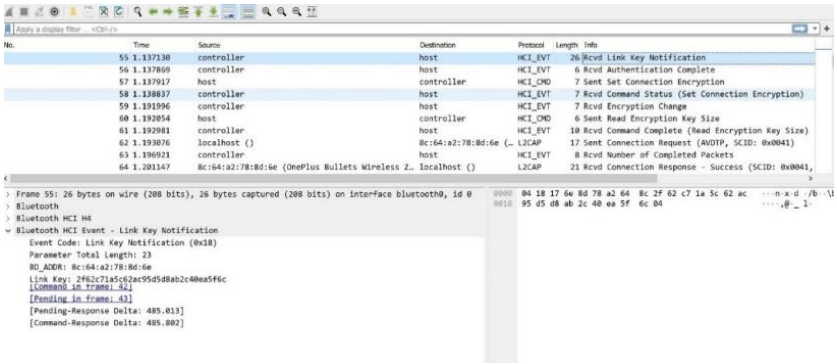
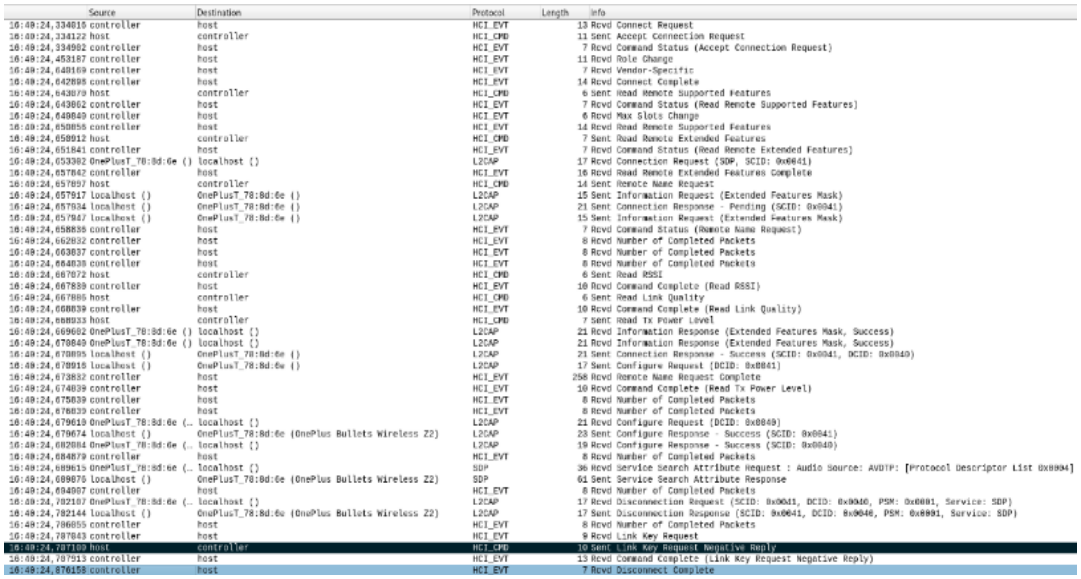


Figure 6.18. *The connection key is extracted*

The last step is performed when the actual data transmission takes place and the data transmission can be bidirectional. The entire security link is based on the connection key generated by the two devices, which is stored in the RAM of the devices.

The relatively easy cloning of parameters: BLE MAC address, device name, even entering into the authentication process the link key previously obtained from valid login, makes the connection process not validated. So, the security of BLE connections cannot be forged using common tools such as cloning BLE MAC address and/or changing device name.



Source	Destination	Protocol	Length	Info
16:49:24,334015 controller	host	HCI_EVT	13	Rcvd Connect Request
16:49:24,334122 host	controller	HCI_CMD	11	Sent Accept Connection Request
16:49:24,334982 controller	host	HCI_EVT	7	Rcvd Command Status (Accept Connection Request)
16:49:24,453187 controller	host	HCI_EVT	11	Rcvd Role Change
16:49:24,640169 controller	host	HCI_EVT	7	Rcvd Vendor-Specific
16:49:24,642895 controller	host	HCI_EVT	14	Rcvd Connect Complete
16:49:24,643070 host	controller	HCI_CMD	6	Sent Read Remote Supported Features
16:49:24,643862 controller	host	HCI_EVT	7	Rcvd Command Status (Read Remote Supported Features)
16:49:24,649849 controller	host	HCI_EVT	6	Rcvd Max Slots Change
16:49:24,650856 controller	host	HCI_EVT	14	Rcvd Read Remote Supported Features
16:49:24,650912 host	controller	HCI_CMD	7	Sent Read Remote Extended Features
16:49:24,651841 controller	host	HCI_EVT	7	Rcvd Command Status (Read Remote Extended Features)
16:49:24,653302 OnePlusT_78:8d:6e ()	localhost ()	L2CAP	17	Rcvd Connection Request (SDP, SCID: 0x0041)
16:49:24,657042 controller	host	HCI_EVT	16	Rcvd Read Remote Extended Features Complete
16:49:24,657897 host	controller	HCI_CMD	14	Sent Remote Name Request
16:49:24,657917 localhost ()	OnePlusT_78:8d:6e ()	L2CAP	15	Sent Information Request (Extended Features Mask)
16:49:24,657934 localhost ()	OnePlusT_78:8d:6e ()	L2CAP	21	Sent Connection Response - Pending (SCID: 0x0041)
16:49:24,657947 localhost ()	OnePlusT_78:8d:6e ()	L2CAP	15	Sent Information Request (Extended Features Mask)
16:49:24,658835 controller	host	HCI_EVT	7	Rcvd Command Status (Remote Name Request)
16:49:24,662832 controller	host	HCI_EVT	8	Rcvd Number of Completed Packets
16:49:24,663837 controller	host	HCI_EVT	8	Rcvd Number of Completed Packets
16:49:24,664838 controller	host	HCI_EVT	8	Rcvd Number of Completed Packets
16:49:24,667072 host	controller	HCI_CMD	6	Sent Read RSSI
16:49:24,667839 controller	host	HCI_EVT	10	Rcvd Command Complete (Read RSSI)
16:49:24,667886 host	controller	HCI_CMD	6	Sent Read Link Quality
16:49:24,668839 controller	host	HCI_EVT	10	Rcvd Command Complete (Read Link Quality)
16:49:24,668933 host	controller	HCI_CMD	7	Sent Read Tx Power Level
16:49:24,669602 OnePlusT_78:8d:6e ()	localhost ()	L2CAP	21	Rcvd Information Response (Extended Features Mask, Success)
16:49:24,670049 OnePlusT_78:8d:6e ()	localhost ()	L2CAP	21	Rcvd Information Response (Extended Features Mask, Success)
16:49:24,670895 localhost ()	OnePlusT_78:8d:6e ()	L2CAP	21	Sent Connection Response - Success (SCID: 0x0041, DCID: 0x0040)
16:49:24,670916 localhost ()	OnePlusT_78:8d:6e ()	L2CAP	17	Sent Configure Request (DCID: 0x0041)
16:49:24,673832 controller	host	HCI_EVT	258	Rcvd Remote Name Request Complete
16:49:24,674839 controller	host	HCI_EVT	10	Rcvd Command Complete (Read Tx Power Level)
16:49:24,675839 controller	host	HCI_EVT	8	Rcvd Number of Completed Packets
16:49:24,676839 controller	host	HCI_EVT	8	Rcvd Number of Completed Packets
16:49:24,679619 OnePlusT_78:8d:6e (..	localhost ()	L2CAP	21	Rcvd Configure Request (DCID: 0x0040)
16:49:24,679674 localhost ()	OnePlusT_78:8d:6e (OnePlus Bullets Wireless Z2)	L2CAP	23	Sent Configure Response - Success (SCID: 0x0041)
16:49:24,682084 OnePlusT_78:8d:6e (..	localhost ()	L2CAP	19	Rcvd Configure Response - Success (SCID: 0x0040)
16:49:24,684879 controller	host	HCI_EVT	8	Rcvd Number of Completed Packets
16:49:24,689615 OnePlusT_78:8d:6e (..	localhost ()	SDP	36	Rcvd Service Search Attribute Request : Audio Source: AVDTP: [Protocol Descriptor List 0x0004]
16:49:24,689875 localhost ()	OnePlusT_78:8d:6e (OnePlus Bullets Wireless Z2)	SDP	61	Sent Service Search Attribute Response
16:49:24,694907 controller	host	HCI_EVT	8	Rcvd Number of Completed Packets
16:49:24,702107 OnePlusT_78:8d:6e (..	localhost ()	L2CAP	17	Rcvd Disconnection Request (SCID: 0x0041, DCID: 0x0040, PSM: 0x0001, Service: SDP)
16:49:24,702144 localhost ()	OnePlusT_78:8d:6e (OnePlus Bullets Wireless Z2)	L2CAP	17	Sent Disconnection Response (SCID: 0x0041, DCID: 0x0040, PSM: 0x0001, Service: SDP)
16:49:24,706855 controller	host	HCI_EVT	8	Rcvd Number of Completed Packets
16:49:24,787043 controller	host	HCI_EVT	9	Rcvd Link Key Request
16:49:24,787109 host	controller	HCI_CMD	10	Sent Link Key Request Negative Reply
16:49:24,787913 controller	host	HCI_EVT	13	Rcvd Command Complete (Link Key Request Negative Reply)
16:49:24,876158 controller	host	HCI_EVT	7	Rcvd Disconnect Complete

Figure 6.19. *Negative response authentication process.*

Chapter 7 Experimental measurements

Within the chapter were extensively presented the experiments carried out in 5 crowded points in Bucharest, in order to determine the quality and quantity of data services made available to users, for each frequency band, respectively the technology available in the band, respectively the second part of the chapter aimed at creating an intelligent jamming device, capable of DoS attacks.

7.1. Radio operator measurements Orange Romania

The results of traffic speeds obtained as a result of measurements made for the operator Orange Romania were presented.

Table 7.12. *Speed test results, operator Orange, at measurement points 1-5.*

Measuring point	Traffic speed (MB/s)	Band 800 MHz LTE	Band 900MHz			Banda 1800 MHz LTE	Band 2100 MHz		Band 2600 MHz LTE
			GSM	UMTS	LTE		UMTS	LTE	
Obor Area	Download	11,1	-	7,81	-	100	error	-	217
	Upload	26,1	-	2,45	-	49,8	error	-	43
Alba Iulia Square Area	Download	13,1	-	14,9	-	15,7	9,04	-	52
	Upload	7,44	-	4,3	-	42,4	3,43	-	48,8
South Square Area	Download	2,07	-	3,06	-	21,7	5,58	-	45,3
	Upload	1,5	-	1,35	-	12,7	2,51	-	6,13
Vulcan Area	Download	3,64	-	1,82	-	42,5	7,82	-	79,2
	Upload	0,71	-	0,3	-	40,3	3,6	-	47,3
Area Mall Plaza	Download	9,24	-	3,26	-	5,33	9,82	-	33,7
	Upload	24,1	-	1,57	-	25,3	2,15	-	33

7.2. Radio operator measurements Vodafone Romania

The results of traffic speeds obtained as a result of measurements made for the operator Vodafone Romania were presented.

7.3. Radio operator Telekom Romania measurements

The results of the traffic speeds obtained, in measuring points 1-5, as a result of the measurements made for the operator Telekom Romania were presented.

7.4. DigiMobil Romania radio operator measurements

The results of the traffic speeds obtained, in measuring points 1-5, as a result of the measurements made for the DigiMobil Romania operator were presented.

7.5 Radio measurement conclusions

The conclusions of the measurements related to the radio connection of the availability of mobile operators at the measuring points, for all measured mobile operators, were presented.

Table 7.38. *Summary of technologies implemented in frequency bands, for the operator Orange Romania:*

Frequency band / Point measure	800 MHz	900 MHz			1800 MHz	2100 MHz		2600 MHz
	LTE	GSM	UMTS	LTE	LTE	UMTS	LTE	LTE
Obor Area	✗	✗	✗	-	✗	-	-	✗
Alba Iulia Square Area	✗	✗	✗	-	✗	✗	-	✗
South Square Area	✗	✗	✗	-	✗	✗	-	✗
Vulcan Area	✗	✗	✗	-	✗	✗	-	✗
Area Mall Plaza	✗	✗	✗	-	✗	✗	✗	✗

7.6. Identification of WIFI access points, respectively clients

Also, measurements were made in the radio spectrum allocated to WiFi communications at all measuring points 1-5, the results obtained were summarized as follows:

Table 7.44. *Statistics of mobile devices and APs using WiFi technology, in measuring points.*

Measuring point	Access points	Number of clients
Obor Area	52	92
Alba Iulia Square Area	59	66
South Square Area	10	31
Vulcan Area	7	46
Area Mall Plaza	14	45

7.7 Identification of BLE devices

Table 7.46. *Statistics of the number of BLE devices with single MAC, at measurement points 1-5.*

Measuring point	BLE devices
Obor Area	132
Alba Iulia Square Area	565
South Square Area	39
Vulcan Area	15
Area Mall Plaza	16

Taking into account the BLE device number statistics shown in Table 7.46. we note that the Alba Iulia Square area was the busiest in terms of the presence of BLE devices (565), respectively the Vulcan commercial area, the least crowded (15).

7.8 Experimental intelligent jamming device in LTE technology

The analysis based on experimental measurements, presented in previous chapters, highlighted the ease with which some attacks can be carried out through the radio interface of wireless communication channels.
Basically, Denial of Service (DoS) attacks can be executed by a malicious person, by jamming the radio connection, regardless of technology, of course under certain conditions of radio propagation, respectively proximity to the targeted mobile devices. [91]
Within the section were presented the characteristics of SDR technology, as well as theoretical considerations regarding jamming techniques.

The main objectives of developing a jamming system are:

1. Determination of jamming limits, in two different scenarios, positioning the receiver in the vicinity of the cell and at the coverage edge of the cell, for two values of the received signal level;
2. Determination of operating conditions in order to react on the downlink to the measurement of a minimum amplitude on the uplink.

7.8.1 Radio spectrum allocated to mobile operators, downlink connection

Within the section were analyzed the availability of mobile operators at the measuring point performed with spectrum analyzer, respectively intelligent mobile terminal that has a special software for analyzing network parameters.

Figure 7.29. *NB-RSRP, NB-RSRQ and other Digi Mobil downstream connection data at the radio monitoring point, obtained with the Nestor monitoring platform.*

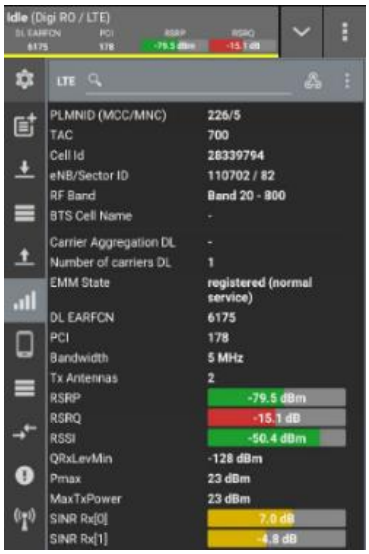


Figure 7.30. *Smart mobile terminal registered in the LTE 800 MHz band.*

7.8.2 Smart jamming

Within the section were exemplified theoretical considerations used in the realization of the intelligent jamming device.

7.8.3 Estimation of jamming effect

Within the section, calculations were presented regarding the estimation of the jamming effect under the technical conditions available.
In Digi Mobil, under laboratory conditions, downward connection jamming was successfully demonstrated, due to the fact that the power of network parameters did not exceed the possibilities of Hack-RF in terms of power.

7.8.4 Implementation of jamming

The practical and functional aspects of intelligent jamming developed for DoS attacks were extensively presented.

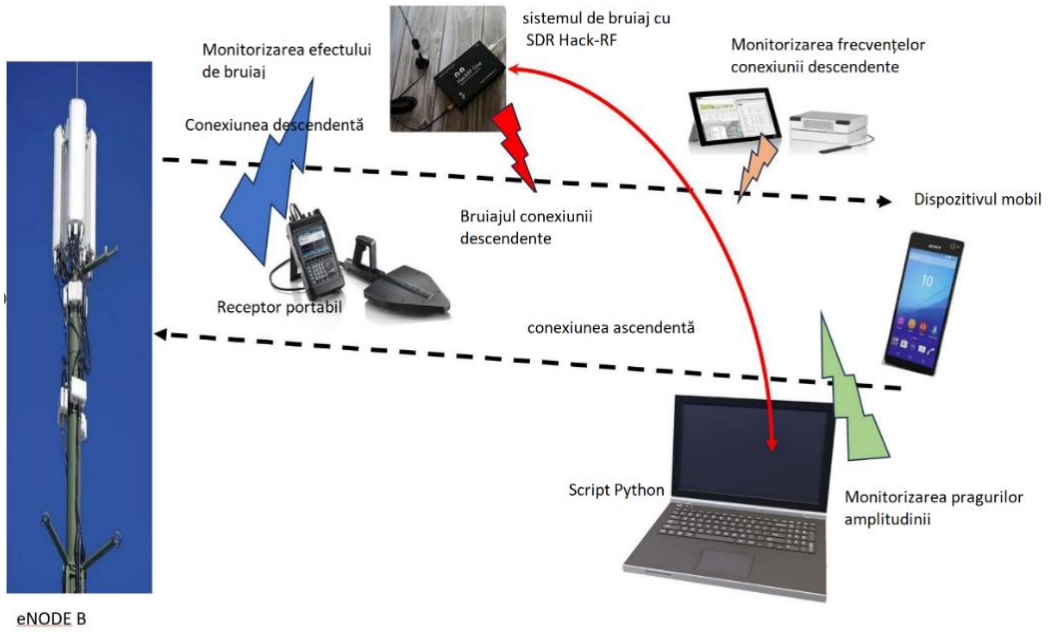
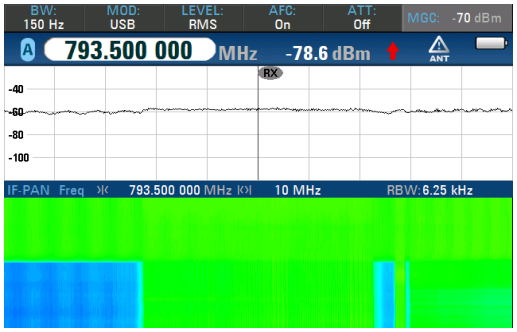
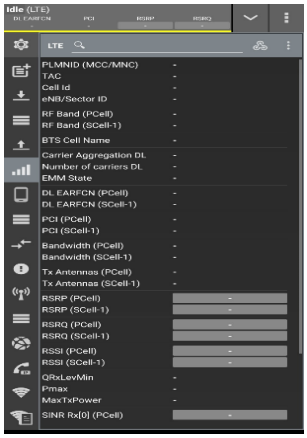


Figure 7.35. *Experimental setup to block downlink connection.*

Basically, for any amplitude above -70 dBm that is detected on the uplink frequencies, provided by Nestor, an emission is started on the frequency of the radio frequency channel of the corresponding downlink connection, with the maximum power of Hack-RF. After 15 seconds, the lock is stopped and the process resumes in a loop.
After several practical tests, it was experimentally established that the effect of jamming, with the power provided by Hack-RF, manifests itself up to 7 meters, an experiment also confirmed by previous calculations of the SIR.
Figure 7.37 (a) illustrates the radio spectrum obtained with PR100, showing graphically the jamming manifestation on the downlink frequency 793,5 MHz. Figure 7.37 (b) shows the effect of the jamming device on the signal received by the smart mobile terminal.



(a)



(b)

Figure 7.36. *(a) Downlink jamming (b) QualiPock frequency monitoring*

7.9 Recommendations on increasing the security of wireless communication networks

A whole series of recommendations have been made for wireless network users to be aware of the risks they expose themselves to when they decide to use such networks, as well as practical advice to protect their data exposed on radio infrastructure.

Chapter 8 Conclusions

8.1 Results achieved

In Chapter 2, fundamental considerations on GSM technology are presented. For a better example of the reported vulnerabilities, in GMS technology, experimental measurements were carried out in mobile operators, Orange and Vodafone, and techniques and means of locating mobile devices were also presented.

Chapter 3 presents the fundamental considerations of 3G-UMTS technology, a predecessor of GSM, which comes to solve some of the shortcomings registered in the previous technology. It has been demonstrated, under laboratory conditions, that a mobile device can be successfully located, knowing details about the infrastructure of mobile operators active at a measuring point, respectively the definite correspondence between the downward frequency on which the network communicates with the mobile device and that of the ascending frequency on which the mobile device communicates with the network.

In chapter 4, theoretical aspects of 4G-LTE technology were presented, which targeted the process of authenticating a mobile device in the network, respectively testing the possibilities of locating a mobile device working in 4G. The results obtained were

appreciated, offering a new perspective of indoor location of mobile devices, by knowing some characteristics of upward connections in which communication is made to the network.

Chapter 5 covered theoretical aspects of 5G SA technology, but also radio measurements to provide an image of a network using 5G SA technology. In Romania, mobile operators have not advanced a deadline for implementing 5G SA technology, currently, they provide data services to users through 5G NSA. The second part of Chapter 5 presents, for the first time, field radio measurements of downstream radio connections of mobile operators offering services to subscribers. The measurements also looked at a picture of what the radio spectrum will look like when 5G technology is implemented. From the aspects presented in the chapter, the presence of GSM technology in all mobile operators in Germany stands out, namely the implementation of 4G in the traditional bands, 800/1800/2600 MHz, and 5G technology in the 700/2100/3500 MHz bands.

In Chapter 6, theoretical aspects of WiFi and BLE technologies were presented, focusing on the vulnerabilities highlighted after experimental tests, respectively after analyzing the results obtained by issuing recommendations to users, increasing network security.

Chapter 7 represents experimental measurements of the technologies studied during doctoral courses. This time, they were deployed in Bucharest in 5 measuring points, chosen to reflect a radio reality of mobile operators active on the national territory.

The results of the measurements showed that a mobile network that has a diversification of technologies in frequency bands can offer, under current conditions, even speeds of 217 MB / s (obtained at the measurement point of the Obor area, operator Orange Romania, LTE technology, implemented in the 2600 MHz frequency band). Practical experiments also aimed to highlight devices using WiFi and BLE technology in the radio spectrum. It was found that the emergence and development of IoT has made the use of devices working in such networks very widespread, which is confirmed by field measurements.

Since attacks through radio infrastructure are the most common that can manifest themselves on mobile devices, working in GSM, LTE and 5G technologies, the last part of chapter 7 presents an intelligent jamming system developed with affordable SDR (Software Defined Radio) equipment, with directive antenna systems, suitable for use inside a prison-type facility.

8.2 Original contributions

The results of research and studies conducted throughout the doctoral cycle led to the original contributions contained in this paper that can be synthesized as follows:

1. Highlighting the vulnerabilities of communication networks in Romania using GSM technology;
2. Practical tests for locating a mobile device using GSM technology;
3. Determining the location of a BTS in GSM technology, through practical measurements;
4. Study on exposure on the radio interface of parameters specific to mobile terminals;
5. Highlighting the vulnerabilities of communication networks in Romania using UMTS technology;
6. Locating a mobile device using UMTS technology, based on emission parameters on the upward connection;
7. Study on the vulnerability of communication networks using LTE technology;
8. Challenges of the procedure for locating a mobile device using LTE technology, with radio receiver, based on emission parameters;
9. Study on the vulnerability of communication networks using 5G technology;
10. Highlighting by measurements the parameters of 5G SA communication networks, given that 5G SA services are not provided in Romania.
11. Practical demonstrations of vulnerabilities of communication networks using Wi-Fi technology;
12. Demonstration of Wi-Fi Calling vulnerabilities;
13. Challenges of attack typologies through Wi-Fi infrastructure;
14. Highlighting vulnerabilities of communication networks using BLE technology;
15. Study on attacks through BLE infrastructure;
16. Practical measurements of the availability of mobile operators' services from 5 measuring points, of the traffic speed for each allocated frequency band, respectively in each available technology.
17. Comparative study of the availability of mobile operators' services from 5 measuring points.
18. Study on the availability of wireless communication networks, identification of access points and users, using WiFi technology, in 5 measuring points.
19. Study on the development of an intelligent jamming system in GSM and LTE technologies, by identifying a minimum signal level threshold for uplink frequencies.
20. Implementation of intelligent jamming solution for LTE technology in the 800MHz band.

8.3. List of original works published or in the process of publication

During my doctoral studies, I published 11 articles, of which 10 conference articles and one article in the journal Applied Science, rated Q2.

The results of Article [C1] shall be partially inserted in Chapter 2, the results of Articles [C2] and [C3] shall be partially incorporated into Chapter 3, [C4] partially incorporated into Chapter 4 and the results of Article [J1] and [C5] used in Chapters 6 and 7.

The results obtained in chapter 7 "Experimental measurements" were constituted in a draft article, which was sent for validation to the Journal Applied Sciences, Section Computing and Artificial Intelligence, Special Issue Trends and Prospects for Wireless Sensor Networks and IoT Article submitted with the title: "**A study case, in Bucharest, regarding real mobile internet speed on mobile network operators"**, authors: Cristian Capota, Mădălin Popescu, Simona Halunga & Mircea Popescu.

At the same time, in Chapter 7 were partially introduced results obtained and published in article [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.

Conference articles:

[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. Opportunities for further development

An immediate challenge is to receive the acceptance to publish the article entitled: **"A study case, in Bucharest: regarding real mobile internet speed on mobile network operators",** authors: Cristian Capota, Mădălin Popescu, Simona Halunga & Mircea Popescu. The article was submitted to the journal Applied Science.

Also, in the medium term (6-12 months) I intend that, as soon as 5GSA networks are implemented in Romania, I will adapt the experimental technical solution for intelligent jamming to this technology and publish the results of the research carried out.

At the same time, I will expand the study of mobile telephone communications networks to identify and signal vulnerabilities in technologies used to provide services to subscribers. These studies will also be extended to 5G SA technology, when it will be implemented in the networks of mobile operators in Romania. I will test the data traffic speeds obtained in 5G SA technology, with presentation in conferences or specialized journals.

All these results will be the focus of my future publications, such as detailing the configuration of wireless communication networks, presenting details on frequency bands and implemented technologies, which must be considered when conducting network speed and availability tests.

REFERENCES:

[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].