Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 127-133

Electronic Attack Using SDR

Ivan Ivanov
C4I Systems Development Directorate
Defence Institute "Prof. Tsvetan Lazarov"
Sofia, Bulgaria
i.p.ivanov@di.mod.bg

Sevdalin Spassov
C4I Systems Development Directorate
Defence Institute "Prof. Tsvetan Lazarov"
Sofia, Bulgaria
s.spasov@di.mod.bg

Abstract: **The essence and main characteristics of electronic attack (EA) are examined, as well as its place in the electronic warfare (EW). The main elements of EA are examined, such as jamming, spoofing and electronic neutralization of enemy radio devices. A definition and the main terms for software-defined radio (SDR) are given. The architecture and main characteristics of SDR are examined. A prototype of SDR is made and demonstrated for the purpose of proving the concept.**

Keywords: electronic warfare, electronic attack, GNU radio framework, software-defined radio.

I. INTRODUCTION

Over the past three decades of persistent conflict, the opposing forces had used its most capable communications systems ever. During this time, the most powerful armies have continued to dominate the electromagnetic spectrum over the enemies and adversaries who lack the ability to challenge their technological superiority. However, in recent years, regional peers have demonstrated formidable capabilities in hybrid operational environments, including electromagnetic spectrum. These capabilities have been also demonstrated in the ongoing conflict in Ukraine mainly in the form of jamming of communications, global navigation satellite system (GNSS) and control systems of military drones.

All combat platforms are being built with a wide application of electronic devices and systems. A large part of these systems receives and transmit both data and control signals. These data and signals are transmitted and received using electromagnetic waves. The use of the electromagnetic spectrum makes them vulnerable to interference by the enemy. All this assumes the growing importance of electromagnetic warfare in recent military conflicts. US Air Force and US Department of the Army use the term Electromagnetic Warfare (EW) [1], [2]. NATO uses the term Electronic Warfare in some doctrinal documents [3], but has changed it to Electromagnetic Warfare in the recent documents [4]. The Electromagnetic Warfare has been adopted as a main term in this paper and it is used in the entire text. Electromagnetic Warfare is one of the main warfare domains. When conducting all electromagnetic warfare activities, it is necessary to receive, digitally process, analyse and store radio signals in a wide frequency range. In addition, in order to conduct an electromagnetic attack, it is necessary to synthesize jamming signals with different parameters, after which they can be emitted in several frequency ranges. All technical activities such as reception, digital processing, analysis and synthesis of signals can be performed using software-defined radio (SDR). The possibilities of applying SDR in electromagnetic attack systems, as well as an exemplary prototype of such a system, are discussed further in the article.

II. MATERIALS AND METHODS

A. Main characteristics of Electromagnetic Attack (EA) and its place in Electromagnetic Warfare (EW).

Electromagnetic warfare [1], [2] is the use of electromagnetic energy to provide situational awareness and achieve offensive and defensive results, and to ensure superiority in the electromagnetic spectrum. EW consists [1] - [4] of three main elements (Fig. 1).

The three main elements of the EW are Electromagnetic Attack (EA), Electromagnetic support (ES) and Electromagnetic Protection (EP). The adjective Electromagnetic replaces adjective Electronic in the recent EW conceptual documents. These three elements are inextricably linked, as they are mutually dependent and are applied in a certain sequence. For example, information about the parameters of radio signals and the location of enemy radio assets, acquired by electromagnetic support, is used to synthesize jamming signals emitted by the transmitters of the electromagnetic attack.

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8483

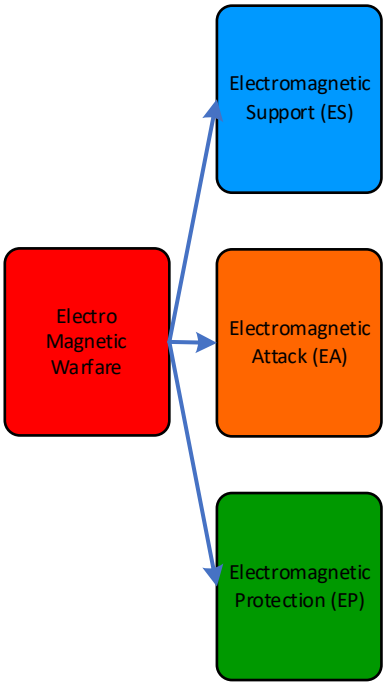

Fig. 1. Elements of the Electromagnetic warfare.

Electromagnetic attack is one of the three main elements of electromagnetic warfare. Electromagnetic attack consists of three main elements: electromagnetic jamming (EJ), electromagnetic deception (ED) and electromagnetic neutralization (EN).

Electromagnetic support (ES) is a component of electromagnetic warfare, which includes actions to search, intercept and identify electromagnetic emissions and locate their sources, in order to immediately recognize the threat and build situational awareness. It provides a source of information necessary for immediate decision-making for electronic countermeasures [5] and other tactical actions.

Electromagnetic Protection (EP) is a complex of technical and organizational measures using electromagnetic energy to provide protection and effective use of the electromagnetic spectrum by allied forces, carried out in order to ensure the stable operation of their own systems and means of controlling troops and weapons, in conditions of electronic effects from the enemy. Electromagnetic protection is divided into active and passive. Active electromagnetic protection is a complex of measures that can be revealed by the enemy, such as - a change in the parameters of the transmitter to such an extent as is necessary to ensure the effective use of the electromagnetic spectrum. Passive electromagnetic protection is a complex of measures that remain hidden from enemy intelligence, such as - operational procedures and reducing their own radiation (signature) in different frequency ranges of EM waves. For example, in the radio frequency range, technical and constructive measures are applied to reduce the effective reflecting surface (RCS - radar cross section) of their own combat platforms - these are the so-called STEALTH technologies. Similar measures are taken to reduce emissions from combat platforms in the infrared (IR), visible, ultraviolet (UV) and sound ranges. Conducting EW involves several processes, combined into the two main cycles shown in Fig. 2.

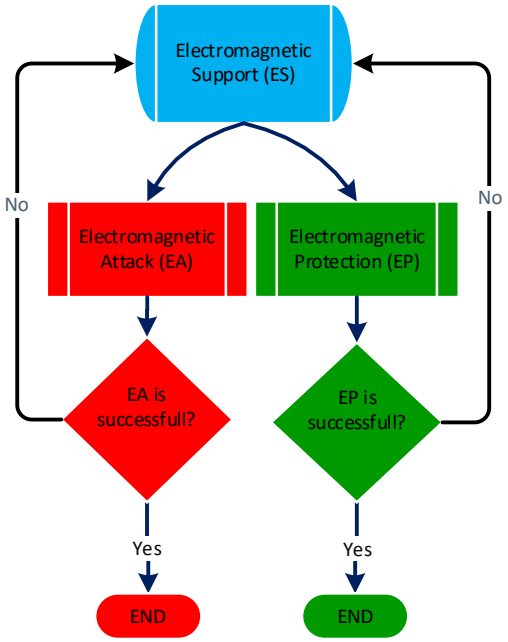

Fig. 2. Processes in the EW.

EW begins with Electromagnetic Support (ES) actions: searching, intercepting and identifying electromagnetic emissions and locating their sources. This information then is used to initiate actions, organized in two cycles: electromagnetic protection and electromagnetic attack. Electromagnetic Protection (EP) includes a set of technical and organizational measures for protection and sustainable operation of the own electronic systems and for the effective use of the electromagnetic spectrum by allied forces. These actions are carried out in order to ensure sustainable control of weapons in conditions of radio-electronic jamming by the enemy. At the end of this cycle of actions, it is checked whether the electromagnetic protection has achieved its goal. If the goal is achieved, then the electromagnetic protection actions stop, and if the goal is not met, the electromagnetic protection actions begin again and the cycle repeats. The electromagnetic attack is organized in the second cycle. It also uses the results of the electromagnetic support, which determines the parameters of the received enemy radio signals and their sources. Jamming signals are emitted to the enemy using electromagnetic attack devices. At the end of this cycle of actions, it is checked whether the electromagnetic attack has achieved its goal. If the goal is achieved, then the electromagnetic attack stops, and if the goal is not achieved, then the parameters of the received enemy radio signals are again determined using the electromagnetic support and the cycle repeats. This type of functioning of the system is called reactive jamming.

The essence, elements and main characteristics of the electromagnetic attack (EA)

Electromagnetic attack includes actions to prevent or reduce the effective use of the electromagnetic spectrum by the enemy through the use of electromagnetic energy. EA is expressed in:

– actions aimed at preventing or reducing the effective use of the electromagnetic spectrum by the enemy, such as suppression of radio transmission or electromagnetic deception;

– use of weapons that use electromagnetic or directed energy such as lasers, radio frequency weapons, particle radiation, etc.;

– offensive and defensive actions including countermeasures.

Electromagnetic attack includes two types of actions: offensive and defensive. Defensive actions use the electromagnetic spectrum to protect personnel, facilities, capabilities and equipment. Examples of defensive actions include protective measures such as: active jammers, countermeasure systems using infrared directed energy, countermeasures against unmanned aerial systems (C-UAS). Offensive EA prevents or reduces the effective use of the electromagnetic spectrum (EMS) by the enemy by using electronic jammers and directed energy weapons systems against enemy systems receiving EM waves in the radio frequency and electromagnetic spectrum. Electromagnetic attack [1] includes three main elements as shown on Fig. 3:

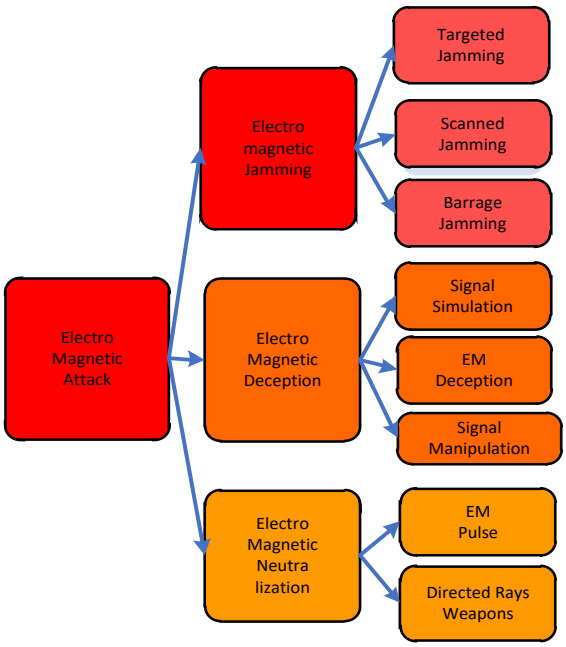

Fig. 3. Components of the electromagnetic attack

– Electromagnetic jamming (EJ),
– Electromagnetic deception (ED) and
– Electromagnetic neutralization (EN).

The general form of EA involves detecting and identifying enemy targets, and conducting activities to gain superiority in the electromagnetic spectrum. In addition, electromagnetic attack actions include a variety of electromagnetic deception techniques, such as false targets or the creation of duplicate targets. Directed energy can be defined as a concentration of electromagnetic energy or atomic and subatomic particles. Directed energy weapons use it as a means of damaging or destroying enemy assets, systems, equipment, and personnel. In addition to their destructive effects, directed energy weapon systems maintain the isolation of areas and control of large groups of people.

Electromagnetic jamming (EJ) is the deliberate emission, secondary emission, or reflection of electromagnetic energy to reduce the effectiveness of enemy electronic devices, equipment, or systems. Examples of offensive actions include jamming enemy radars or electronic command and control systems and the use of anti-radar missiles to suppress enemy air defence assets.

Electromagnetic deception (ED) by electronic means is the deliberate emission, secondary emission, modification, absorption, or reflection of electromagnetic energy in a manner intended to confuse, destroy, or divert an adversary or its electronic systems from proper operation.

Electromagnetic neutralization (EN) is the deliberate use of electromagnetic energy to temporarily or permanently damage adversary devices that rely exclusively on electromagnetic radiation for their operation [3]. Electromagnetic neutralization typically results from the use of directed energy or a beam from a device possessing sufficient electromagnetic energy at a target to temporarily or permanently disable the target, its electronics, or both. The use of lasers to blind people or to destroy sensitive optical devices are two such examples. The considered classification of the elements of the electromagnetic attack is according to the type of emitted jamming signals. If the electromagnetic attack is considered from the point of view of the object of the attack, then several types of jamming signals are determined. These are jamming signals for enemy radars, for communication networks, for reconnaissance radio systems, for other combat platforms. A good study of electromagnetic attacks on wireless communication networks have been done in [7].

B. General information about software-defined radio (SDR)

Software-defined radio is a modern paradigm for the practical implementation of radio communication systems. The foundations of the “software-defined radio” (software-defined radio - SDR) paradigm are associated with the research of DARPA and the US Air Force under the SpeakEasy project in the early 1980s on the creation of a prototype radio station covering the range from 2 MHz to 2 GHz and implementing about 10 communication standards [8]. Part of the results obtained in the field of system architecture were published by Mitola in the early 1990s, where the author [9] introduced the concepts [10] “software radio” and “software-defined radio” [11]. Each professional organization attempts to

define a common framework of terms and definitions to allow for easy communication among professionals working in a common field. In the field of software-defined radio communications, the Institute of Electrical and Electronics Engineers (IEEE), through its working group P1900.1, has created definitions (Table I) to ensure that everyone in the field has a common terminology [12]. A key definition in this brief ontic is that of "software-defined radio": a radio in which some or all of the physical layer functions are software-defined.

The definitions introduced allow not only to standardize the concept of SDR, but also to create a context in which this concept "lives". This allows the formation of other contexts in which SDR can be attributed to different entities.

A structural-functional block diagram of such a radio is shown in Fig. 4.

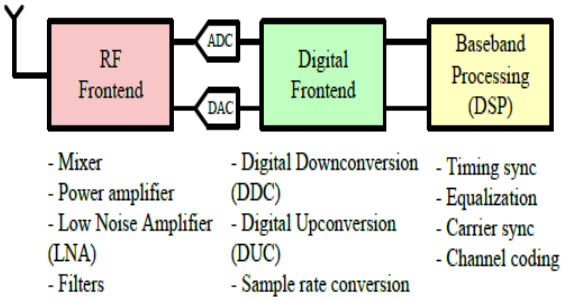

Fig. 4. Software-defined radio architecture

One of the main differences between the architecture of a software-defined radio and an ideal one is the presence/need of a radio frequency front-end operating in the analogue space and implementing such functions as mixing, low-noise amplification, analogue filtering, etc. Another architectural feature of modern SDRs is the implementation of digital processing by two digital blocks – a digital front-end and a baseband digital signal processing block. The first block performs all conversions from transmitted to baseband (and vice versa) and those related to the clock frequency (frequency compression, expansion, etc.). The second block performs all conversions to baseband and is typically implemented by a general-purpose computer or a single-board microcomputer.

TABLE I ONTIC OF CONCEPTS IN THE FIELD OF SOFTWARE-DEFINED RADIO COMMUNICATIONS

Concept	Definition
Radio	1. A technology for the wireless transmission or reception of electromagnetic signals enabling the transfer of information. 2. A system or device incorporating technology as defined in (1). 3. A general term applied to the use of radio waves.
Radio Node	A radio point of presence, including a transmitter and/or receiver.
Software	Modifiable instructions executed by a programmable processing device
Physical	The layer within a wireless protocol that processes radio frequency (RF), intermediate frequency (IF), or baseband signals, including performing channel coding. It is the lowest layer of the 7-layer ISO model adapted for wireless transmission and reception.
Data Link Layer	The protocol responsible for the reliable transmission of frames over a wireless link by using appropriate error detection and control procedures and media access control.
Software Controlled	Software control refers to the use of software processing in the radio system or device to select operating parameters.
Software Defined	Software-defined refers to the use of software processing in the radio system or device to perform operational (but not control) functions.
Software Controlled Radio	A radio in which some or all of the physical layer functions are software controlled.
Software-Defined Radio	**A radio in which some or all of the physical layer functions are software defined.**
Transmitter	Equipment producing radio frequency energy for radio communication purposes.
Receiver	A device that receives a radio signal and provides information extracted from it.
Air Interface	A subset of waveform functions designed to establish communication between two radio terminals. This is the equivalent of the wireless physical layer and wireless data layer waveforms.
Waveform	1. The set of transformations applied to the information to be transmitted and the corresponding set of transformations to convert the received signals back to their information content. 2. Representation of the signal in space. 3. Representation of the transmitted radio frequency signal plus additional radio functions, including all network layers.

The analogue RF front-end, ADC, DAC and digital front-end are combined into a common building block – RF digital front-end in current products on the market that allow prototyping in the field of SDR. This leads to the generalized, mass, modern SDR architecture shown in Fig. 5.

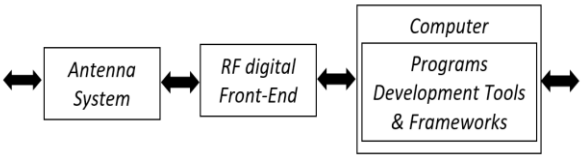

Fig. 5. Generalized mass architecture of SDR.

Table II summarizes the main characteristics of popular radiofrequency front-ends used to build SDRs.

The analysis of the data in Table 2 shows the availability of capabilities for supporting a wide frequency range – a part of HF, VHF and UHF, a wide bandwidth of the processed radio channel – up to 120 MHz. There is availability of transmitting/receiving a high data exchange speed with personal computer platforms – up to 10 GBit/s and to support of multiple coherent radio channels, etc.

These characteristics allow the implementation of variety technologies such as GSM, LTE, DVB, FMCW Radar, MIMO, etc.

TABLE II MAIN CHARACTERISTICS OF POPULAR RADIOFREQUENCY FRONT-ENDS FOR SDRs

Plat-form	Frequ-ency range	Channel band-width	Digital conver-ters bit resolution	Digital interface	Radio channel number
Hack RF One	10 MHz - 6GHz	20 MHz	8 bit	USB 2.0	1 Rx/1 Tx
Adalm PLUTO	325 MHz - 3.8 GHz	20 MHz	12 bit	USB 2.0	1 Rx/1 Tx
Ettus B210	70 MHz - 6 GHz	56 MHz	12 bit	USB 3.0	2 Rx/2Tx
Ettus N210	10 MHz - 6 GHz	40 MHz	14-bit ADC 16-bit DAC	1G Ethernet	2 Rx/2Tx
Ettus X210	50 MHz - 2,2 GHz 400 MHz - 4.4 GHz 1.2 GHz - 6 GHz	120 MHz	14-bit ADC 16-bit DAC	10G Ethernet, PCIe	2 Rx/2 Tx, 4 R x
Ettus X310	10 MHz до 6 GHz	160 MHz	14-bit ADC 16-bit DAC	10G Ethernet, PCIe	2 Rx/2 Tx, 4 Rx
Lime SDR	100 kHz - 3.8 GHz	61.44 MHz	12 bit	USB 3.0	6 Rx/4 Tx
Pico SDR	70 MHz - 6 GHz	56 MHz	12 bit	PCIe	4 Rx/4 Tx 8 Rx/8 Tx
RTL-SDR	24 – 1766 MHz	3.2 MHz (2.4 MHz typical)	8 bit	USB 2.0	1 Rx

The SDR technology is supported by numerous software packages for computer modelling and simulation. The most famous of them are: Matlab, GNU Radio, LabVIEW, etc. The advantage of using such packages is the rapid transition from a computer module to a practical implementation.

III. RESULTS AND DISCUSSION

An electromagnetic attack on a Wi-Fi network can be done by SDR by three general concepts. The first of them is to perform electromagnetic jamming, the second one relies on the electromagnetic deception and the third uses electromagnetic neutralization.

A prototype of an electromagnetic jamming system based on software-defined radio has been created in order to proof the first concept. The test scenario is shown at Fig. 6. It includes a mobile device, a Wi-Fi access point and attacking device (jammer), performed by SDR. The Wi-Fi wireless network was chosen, based on its popularity and availability.

SDR functions as a jammer that disrupts the radio connection between a Wi-Fi network access point and a mobile device. The test scenario examines the impact of different jamming types on radio connection between a Wi-Fi network access point and a mobile device.

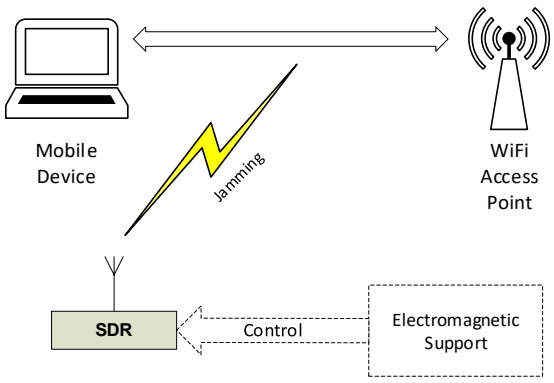

Fig. 6. The Test scenario.

System realization of SDR as a jammer is shown at Fig.7 consisting of the X310 front end, power amplifier and the GNU radio software package.

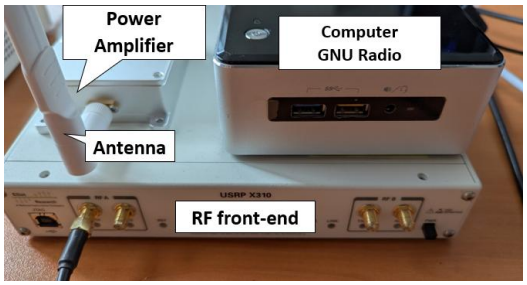

Fig. 7. Implementation of SDR for EA.

The radio framework flow graph of SDR for EA, based on a GNU radio software package is presented on Fig. 8.

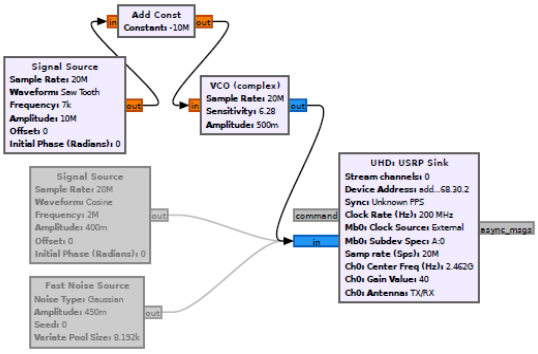

Fig. 8. GNU Radio Framework flowgraph of SDR for EA.

The mobile device has established a stable radio connection with the Wi-Fi network access point. With the help of Electromagnetic Support, the main parameters of the radio network have been determined and submitted to the electromagnetic attack system. The spectral waterfall

diagram of normal Wi-Fi activity on targeted channel is presented on the Fig. 9.

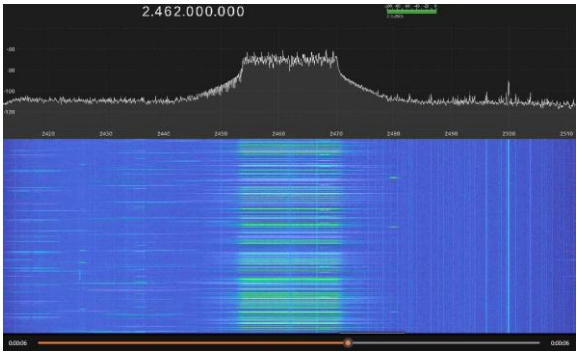

Fig. 9. A spectral waterfall diagram of Wi-Fi activity on targeted channel.

Two types of jamming signals have been generated in the GNU radio environment. These jamming signals have the same radiated power, but have different bandwidths. The first signal is a barrage radio jamming in the entire width of the Wi-Fi network bandwidth of 20 MHz. The second signal is a narrowband jamming that scans the entire width of the Wi-Fi radio network bandwidth.

Two experiments have been conducted in a controlled, rather than public, environment to avoid risks of violating legal and ethical requirements. The result of the impact of electromagnetic jamming on the radio connection between the mobile device and the Wi-Fi network has been evaluated. The desired effect is to achieve a failure in the performance of a basic function in the targeted Wi-Fi radio network, such as a lack of communication between the access point and the mobile device.

The results of the experiments are shown on the Fig. 10 and Fig. 11. The waterfall view of the barrage jamming on the Wi-Fi radio connection is shown on Fig. 10. It covers the whole Wi-Fi radio bandwidth by almost equal power of the jamming.

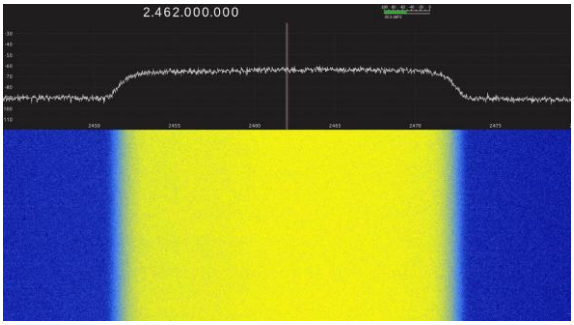

Fig. 10. The barrage jamming on the Wi-Fi radio connection.

The waterfall view of the second disturbance signal - scanned jamming on the Wi-Fi radio connection is shown on Fig.11.

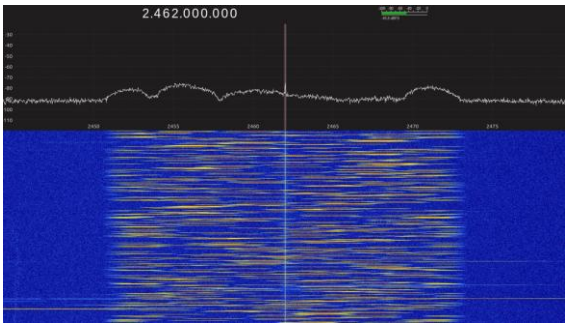

Fig. 11. The scanned jamming on the Wi-Fi radio connection.

A low-speed scanned jamming has been used in the entire Wi-Fi channel passband. The scanned jamming covers almost the whole network bandwidth by noise with fluctuating power, visible in Fig. 11. The power of the scanned jamming isn't uniform distributed across the entire frequency band of the Wi-Fi radio network. This is a weakness of frequency-scanning jamming. To achieve denser coverage of the entire Wi-Fi channel bandwidth, the frequency change of the scanned jamming must be increased.

The searched effect - lack of communication in the targeted Wi-Fi radio network has been achieved. These results validate the concept in Fig.6.

The second way to make electromagnetic attack on a Wi-Fi network can be done by means of electromagnetic deception (ED). An example of a GNU Radio Framework flowgraph of SDR Wi-Fi transmitter performing ED is shown on Fig. 12. By the GNU Radio block "WiFi MAC" SDR pretends as the access point (AP) and constantly addressing the mobile device. Preliminary results of degradation of the communication was achieved as a validation of the concept.

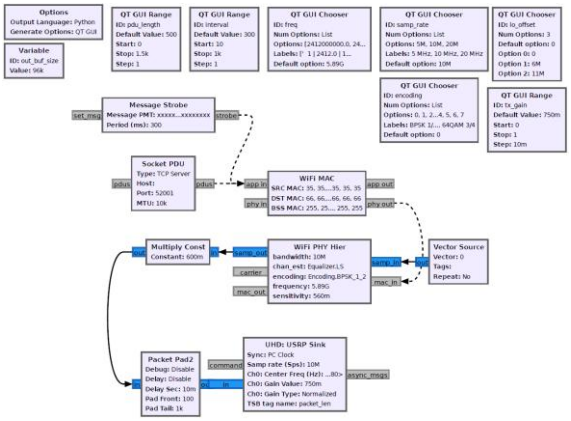

Fig. 12. GNU Radio Framework flowgraph of SDR Wi Fi transmitter performing ED.

There are numerous limitations, challenges, and risks associated with the application of SDR to EA. It is a challenge for an SDR to simulate an access point and overload the targeted mobile device by continuous addressing and data flow. There are a number of limitations, such as simulating a real data stream for the purpose of deception and transmitting it over the Wi-Fi

radio network to the end mobile device. There is also a risk of improper jamming of public Wi-Fi radio networks if the experiment is conducted in a controlled environment that is close to such radio networks. All these limitations, challenges, and risks associated with the application of SDR to EA have to be considered in the future experiments.

IV. CONCLUSIONS

Two approaches are considered for implementing an electromagnetic attack with SDR on a WiFi radio network.

The first approach involves electromagnetic jamming. A prototype of an electromagnetic jamming system based on software-defined radio has been created in order to proof the concept. Two types of jamming signals have been generated in the GNU radio environment - a barrage radio jamming and a scanned jamming in the entire width of the Wi-Fi network. The barrage jamming on the Wi-Fi radio connection jams the whole Wi-Fi radio bandwidth by almost equal power on each frequency. Compared to it, the scanned jamming signal hasn't uniform power distribution across the entire frequency band of the Wi-Fi radio network. The power distribution of the scanned jamming depends of its sweeping speed.

The desired effect - loss of basic function such as lack of communication in the targeted Wi-Fi radio network – has been achieved in both experiments. Additional experiments are to be conducted in various real-world conditions to compare the impact of barrage jamming and frequency-scanned jamming on Wi-Fi radio networks.

The second approach to make electromagnetic attack on a Wi-Fi network can be done by means of electromagnetic deception. An example of a GNU Radio Framework flowgraph of SDR Wi-Fi transmitter performing ED has been done. No experiments have been conducted yet in real conditions to assess the impact of electromagnetic deception on Wi-Fi radio networks. Field tests should be done in a controlled environment and in various real-world conditions to prove this concept and to assess the impact of this jamming on Wi-Fi radio networks.

ACKNOWLEDGMENTS

This work was supported by the NSP SD program, which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement № Д01-74/19.05.2022.

REFERENCES

[1] Department of the Army, "FM 3-12: Cyberspace operations and Electromagnetic Warfare", US Army, August, 2021. Available: https://irp.fas.org/doddir/army/fm3-12.pdf. [Accessed: Feb. 04, 2025].

[2] US Air Force, "Air Force Doctrine Publication 3-85: Electromagnetic Spectrum Operations", US Air Force, Dec. 14, 2023. Available: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-85/AFDP%203-85%20Electromagnetic%20Spectrum%20Ops.pdf. [Accessed: Feb. 05, 2025].

[3] NATO, "AAP-06: Glossary of terms and definitions", NSO, 2021. Available: https://standard.di.mod.bg/pls/mstd/f?p=600:1:8391929042894131. [Accessed: Feb. 05, 2025].

[4] NATO, „Electromagnetic Warfare", Mar. 22, 2023. [Online]. Available: https://www.nato.int/cps/en/natohq/topics_80906.htm. [Accessed: Feb. 05, 2025].

[5] S. Spassov, K. Paraskov, P. Kokudeva, J. Petrov, Concept of use and operational requirements for passive defense software-defined radar systems: ARTDEF Conference, November 28-29, 2023, Sofia, Bulgaria. Sofia: BDI Acad. Publishing, 2024.

[6] H. Pirayesh and H. Zeng, "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey", IEEE Communications Surveys & Tutorials, vol. 24, Issue: 2, pp. 767 – 809, Secondquarter 2022.

[7] NATO, "Allied Joint Doctrine for Electronic Warfare", NATO Standard AJP-3.6, March 24, 2020.

[8] R. J. Lackey and Donald W. Upmal, "Speakeasy: The Military Software Radio", IEEE Communications Magazine, vol. 33, Issue 5, pp. 56 - 61, May 1995.

[9] J. Mitola III, "Software Radios: Survey, critical evaluation and future directions", IEEE Aerospace and Electronic Systems Magazine,Vol. 8, Issue 4, pp. 25 – 36, April 1993.

[10] J. Mitola III, "The Software Radio Architecture", IEEE Communications Magazine, vol. 33, Issue 5, pp. 26 - 38, May 1995.

[11] A. Margulies and J. Mitola III, Software Defined Radios: A Technical Challenge and a Migration Strategy: IEEE 5th International Symposium on Spread Spectrum Technologies and Applications, September 2-4, 1998, Sun City, South Africa. Piscataway NJ: IEEE Service Center, 1998.

[12] A. Wyglinski, T. Collins, D. Pu, and Robin Getz, Software-Defined Radio for Engineers. Norwood, MA, Artech House, 2018.