Secure Systems Design and Technology Development. Veliko Tarnovo, Bulgaria
Proceedings of the International Scientific Conference, 2026. Volume I, 233-240

Electromagnetic Protection Using Software-Defined Radio

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 main elements of electromagnetic protection (EP) such as ensuring electromagnetic compatibility measures, communication equipment protection measures, electromagnetic radiation management, preventive countermeasures against enemy radio intelligence have been examined. A definition, basic terms and the architecture of software-defined radio (SDR) have been given. SDR implementation possibilities at electromagnetic protection of military communication systems have been considered. The paper also includes a GNU Radio proof-of-concept simulation of SDR-based spatial signal analysis and discusses practical coherence challenges when moving from simulation to a multi-device SDR implementation.**

Keywords: Electromagnetic warfare (EW), electromagnetic protection (EP), Software-defined radio (SDR).

• INTRODUCTION

During the last three decades, 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.

Combat platforms are 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 [6]. All this assumes the growing importance of electromagnetic warfare (EW) in recent military conflicts.

• ESSENCE OF ELECTROMAGNETIC PROTECTION (EP) AND ITS PLACE IN ELECTROMAGNETIC WARFARE

o *Electromagnetic Warfare and its components*

The Electromagnetic Warfare (EW) is 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.

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 (Fig. 1) consists [1, 2, 3, 4] of three main elements.

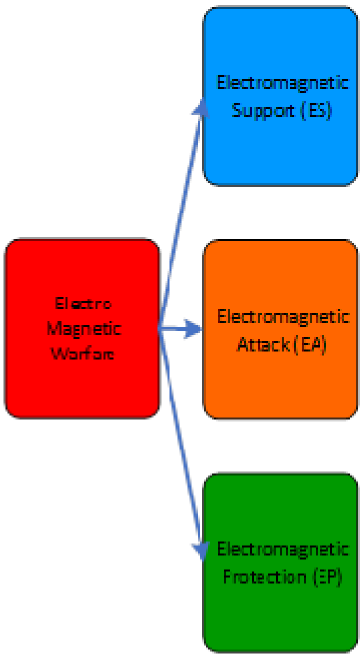

Fig.1 Electromagnetic Warfare's components

Online ISSN 3044-7771
https://doi.org/10.68302/std2026.vol1.156

- *The essence, and main elements of the Electromagnetic Protection (EP)*

Electromagnetic Protection 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.

From an engineering point of view, EP can be understood as a set of measures that reduce the effect of intentional and unintentional electromagnetic interference. These measures include protection against jamming, protection against deception and signal spoofing, reduction of the probability that friendly emissions will be intercepted or detected, electromagnetic compatibility, emission control, spectrum management, and adaptation of systems to new threats.

For the purpose of this analysis, EP is treated as a functional engineering taxonomy rather than as a strict doctrinal hierarchy. From this point of view the EP consists of six main components:

- Anti-jam protection
- Anti-deception / anti-spoofing
- Low probability techniques
- EMI / EMC protection
- Emission control and spectrum management
- Adaptive protection

Each EP component has subcomponents. The deeper EP structure will be considered further in order to organize the protective functions that are relevant to SDR-based implementation.

CHALLENGES IN ELECTROMAGNETIC PROTECTION OF MILITARY COMMUNICATION SYSTEMS. GENERAL INFORMATION ABOUT SOFTWARE-DEFINED RADIO (SDR)

- *Challenges in electromagnetic protection of military communication systems*

Electromagnetic protection (EP) is conducted by electromagnetic warfare units in modern armies. EP has the character of a systematic activity, because it encompasses constructive, technical and organizational measures for protection. Therefore, electromagnetic protection can achieve its maximum effectiveness in EW formations.

On the other hand, electromagnetic protection (EP) in the communication formations of modern armies is not organized on the systematic basis. For example, only a part of the electromagnetic protection functions are built into the communication equipment in terms of circuitry. They include both measures for reducing the output power and readjusting the operating frequency of the transmitters, as well as various schemes for automatically adjusting the gain in their receivers. In this state of arts, the communication equipment does not have a built-in function for detecting interference. Thus, their receivers cannot automatically determine the fact of the presence of interference in order to take the appropriate protection measures. In order to detect the presence of interference and take protection measures, the presence of an operator is necessary.

The combat operations and the radio-electronic environment changes very quickly at the tactical level of the armed forces. Therefore, rapid and adequate technical and organizational actions are required to protect communication means. The detection and analysis of natural and artificial interference in the troops is within the competence of electronic intelligence units. These units are at operational or strategic level, since the results of the analysis of intercepted enemy emissions are used by commanders at these levels. Therefore, communication units at the tactical level do not have an automatic system for detecting, analyzing and responding to intentional interference (jamming). In order to take protective measures, the intervention of an operator is necessary. However, this measure necessarily requires the presence of an operator and his constant monitoring of the radio-electronic environment. This cannot always be done with the necessary speed and reliability. From all that has been said so far, the conclusion is that communication units at the tactical level must have an automatic or automated system for detecting, analyzing, and responding to intentional interference (jamming).

One possible technical solution to this problem could be the use of software-defined radio (SDR.

- *General information about software-defined radio (SDR)*

Software Defined Radio is a suitable technological platform for implementing a significant part of EP functionality because it enables programmable and reconfigurable signal processing. This is due to its structure and properties.

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 [7] 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. 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. 2.

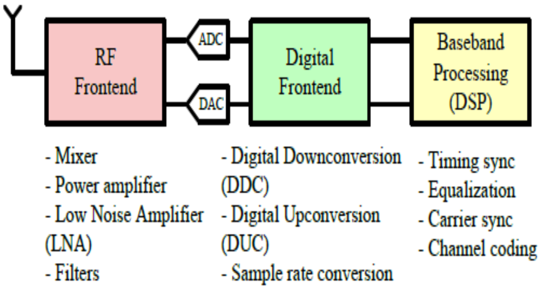

Fig.2 Structural-functional block diagram of SDR

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 signal 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.

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. 3.

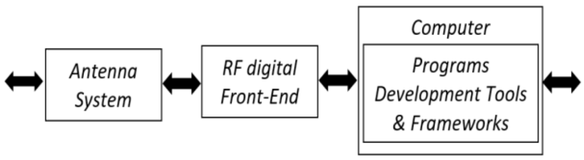

Fig.3 Generalized mass architecture of SDR

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

- SDR IMPLEMENTATION POSSIBILITIES IN ELECTROMAGNETIC PROTECTION OF MILITARY COMMUNICATION SYSTEMS

  - *SDR as a platform for EP*

SDR is a suitable technological platform for implementing a significant part of EP functionality because it enables programmable and reconfigurable signal processing. Through SDR, it is possible to implement adaptive waveforms, frequency agility, spread spectrum techniques, digital filtering, spectrum sensing, interference detection, modulation and coding adaptation, and algorithms for identifying spoofing or deception attempts.

The deeper EP structure below is a practical way to organize the protective functions that are relevant to SDR-based implementation. The Table 1 demonstrates the role of SDR in the individual elements of EP.

THE ROLE OF SDR IN THE INDIVIDUAL ELEMENTS OF EP

1. ANTI-JAM PROTECTION

EP element	*Short explanation*	*How SDR helps*
Anti-jam protection	Protection against intentional jamming in order to preserve communication, navigation, or reception of the useful signal.	SDR enables frequency agility, adaptive parameter changes, interference detection, and switching to a more robust operating mode.
Frequency hopping	Fast or pseudorandom change of the operating frequency to make jamming and interception more difficult.	SDR can change the carrier frequency programmatically according to a predefined or adaptive hopping sequence.
Spread spectrum	Spreading the signal over a wider bandwidth to improve robustness and reduce spectral power density.	SDR can generate and receive DSSS, FHSS, chirp spread spectrum, and other spread spectrum waveforms.
Adaptive filtering	Suppression of narrowband, wideband, or impulsive interference by means of digital filters.	SDR can implement notch filters, adaptive FIR/IIR filters, spectral excision, and interference cancellation.
Beamforming / null steering	Steering receiver sensitivity toward the useful signal and placing spatial nulls toward interference sources.	With a multichannel phase-coherent SDR, digital beamforming, direction-of-arrival estimation, and spatial jammer suppression can be implemented.
Coding, interleaving, redundancy	Increasing robustness against errors, burst interference, and partial signal loss.	SDR allows software-defined changes of FEC schemes, code rate, interleaving depth,

EP element	Short explanation	How SDR helps
		repetitions, and fallback modes.

2. ANTI-DECEPTION / ANTI-SPOOFING

EP element	Short explanation	How SDR helps
Anti-deception / anti-spoofing	Protection against false, misleading, or manipulated signals.	SDR enables analysis of time, frequency, phase, power, and correlation consistency, as well as anomaly detection in the received signal.
Signal authentication	Verification that a signal or message originates from a legitimate source.	SDR can carry and process authenticated waveforms, but reliable authentication also requires cryptographic architecture and key management.
Consistency checks	Checks between expected and measured signal parameters.	SDR can compare Doppler, phase, time of arrival, power, correlation peaks, and other features to detect inconsistencies.
Multi-sensor validation	Confirmation of information through comparison with independent sensors or channels.	SDR can provide radio-channel measurements that are compared with GNSS, inertial navigation, other frequencies, or external sensors.
False-target rejection	Rejection of false targets or misleading responses, especially in radar and navigation systems.	SDR enables analysis of waveform parameters, delays, Doppler, correlation structure, and mismatch between expected and received signals.

3. LOW PROBABILITY TECHNIQUES

EP element	Short explanation	How SDR helps
Low probability techniques	Techniques that reduce the probability that a signal will be intercepted, detected, or successfully jammed.	SDR enables programmable control of waveform, power, bandwidth, time profile, and emission mode.
LPI - Low Probability of Intercept	Reducing the probability that the signal will be intercepted by an adversary ES receiver.	SDR can generate noise-like, wideband, short-duration, or frequency-mobile signals with low spectral power density.
LPD - Low Probability of Detection	Reducing the probability that the emission itself will be detected.	SDR enables control of power, duration, frequency, bandwidth, and the temporal pattern of the emission.
LPJ - Low Probability of Jam	Making effective jamming of the signal more difficult.	SDR enables adaptive change of waveform, frequency, coding, data rate, and operating mode.
Emission shaping	Shaping the spectral, temporal, or spatial profile of the emission.	SDR can control spectral masks, envelope shaping, pulse shaping, duty cycle, and other parameters of the transmitted signal.

4. EMI / EMC PROTECTION

EP element	Short explanation	How SDR helps
EMI / EMC protection	Protection from unintentional electromagnetic interference and ensuring compatibility between friendly systems.	SDR helps through spectrum monitoring, interference detection, adaptive filtering, and selection of a cleaner channel, but hardware EMC protection remains a separate requirement.
Filtering	Limiting or suppressing unwanted frequency components.	SDR implements digital filtering, but it often needs to be complemented by hardware RF filters before the ADC.
Shielding	Shielding sensitive electronic blocks from external electromagnetic effects.	SDR does not replace shielding, but it can support diagnostics by measuring residual interference and spectral contamination.
Grounding	Proper grounding to reduce noise, parasitic currents, and interference.	SDR does not implement grounding, but it can be used to measure and evaluate the influence of noise and parasitic interference on the received signal.
Frequency coordination	Coordination of used frequencies to avoid mutual interference.	SDR can monitor spectrum occupancy and support the selection of suitable operating frequencies.

5. EMISSION CONTROL AND SPECTRUM MANAGEMENT

EP element	*Short explanation*	*How SDR helps*
Emission control and spectrum management	Management of friendly emissions and the used frequency resources.	SDR enables software control of frequency, power, mode, bandwidth, time windows, and emission profile.
EMCON	Control of when, for how long, and under what conditions the system emits.	SDR can switch between active, restricted, burst, passive, or listen-only modes.
Restricted frequency lists	Lists of frequencies that must be avoided or protected.	SDR can apply programmed restrictions on allowed frequencies and automatically exclude prohibited or vulnerable channels.
Power control	Control of transmitted power according to the mission and electromagnetic environment.	SDR can dynamically control transmit power through digital and RF control loops, within the limits of the hardware.
Time/frequency planning	Planning when and on which frequencies the system should transmit or receive.	SDR can execute predefined or adaptive time-frequency plans.

6. ADAPTIVE PROTECTION

EP element	*Short explanation*	*How SDR helps*
Adaptive protection	Adaptation of protective modes according to the electromagnetic environment and the type of threat.	SDR is especially suitable because it allows rapid changes of algorithms, waveforms, filters, frequencies, coding, and modes.
EW reprogramming	Updating parameters, modes, and algorithms in response to new threats.	SDR allows updates of waveforms, filters, classifiers, frequency plans, and protocols through software or FPGA reconfiguration.
Threat library updates	Updating databases of signatures, parameters, and models of threats.	SDR can collect IQ data and spectral features that support the update of classifiers and threat libraries.
Mode switching	Switching between different operating modes according to conditions.	SDR can switch between normal, anti-jam, LPI/LPD, emergency, low-rate, or passive modes.
Cognitive/adaptive radio techniques	Use of sensing, assessment, and automatic parameter selection according to the environment.	SDR provides the basis for spectrum sensing, decision logic, and adaptive selection of frequency, waveform, modulation, and coding.

In summary, SDR is most applicable to those parts of EP that depend on digital signal processing, adaptability, and reconfigurability [5]. It is particularly effective for anti-jam protection, spread spectrum, frequency hopping, adaptive filtering, low probability techniques, and adaptive protection. Its limitations are most significant in the purely hardware-related aspects of EP, such as shielding, grounding, RF preselection, hardware EMC protection, and physical robustness of the receiver front-end.

- *Why SDR cannot implement the entire EP domain by itself*

SDR should not be treated as the complete EP system by itself. It is better understood as the core of an adaptive EP architecture. It provides flexibility, reconfigurability, and intelligent signal processing, but it must be complemented by appropriate RF hardware, antennas, EMC/EMI measures, cryptographic protection, and organizational control of electromagnetic emissions.

Several EP functions are primarily hardware-dependent or system-level in nature. For example, if a powerful jammer saturates the RF front-end before the analog-to-digital converter, the digital processing inside the SDR may no longer be able to recover the useful signal. In such cases, protection depends on RF preselectors, limiters, filters, high-dynamic-range receivers, automatic gain control, and careful front-end design.

Similarly, beamforming and null steering require more than software. They require a multichannel, phase-coherent SDR architecture, a suitable antenna array, common timing and frequency references, and calibration of the RF channels. EMI/EMC protection also requires shielding, grounding, cabling discipline, hardware filtering, and good RF and PCB design. Authentication and secure communication may use SDR waveforms, but reliable protection also requires cryptographic architecture, key management, trusted firmware, and platform security.

• SIMULATION AND IMPLEMENTATION ISSUES OF SDR-BASED SPATIAL SIGNAL ANALYSIS

This section complements the functional mapping of SDR capabilities by considering one selected capability in more detail: spatial signal analysis based on angle-of-arrival (AoA), also commonly referred to as direction-of-arrival (DOA), estimation. The section combines a GNU Radio proof-of-concept simulation with implementation-related issues that appear when the same processing chain is moved toward a physical multichannel SDR realization. The simulation is therefore used not as a complete electromagnetic protection (EP) demonstration, but as a controlled example of how SDR can support source localization, spatial consistency checking, beamforming/null-steering preparation, and anti-deception/anti-spoofing indication.

- *AoA model and practical MUSIC algorithm*

In a multichannel receiver, AoA estimation exploits the phase differences observed at spatially separated antenna elements. For a narrowband far-field emitter, the received signal vector at a uniform linear array (ULA) can be represented by a steering vector whose phase progression depends on the inter-element spacing and the arrival angle. This is the basic physical mechanism used by practical algorithms such as MUSIC [12].

$$\mathbf{x}[n] = \mathbf{A}\mathbf{s}[n] + \mathbf{w}[n] \tag{1}$$

In (1), the vector s[n] contains the source signals, A is the array steering matrix, x[n] contains the samples observed at the antenna elements, and w[n] represents noise and disturbances. For an M-element ULA with normalized inter-element spacing d, the m-th component of the steering vector for an emitter arriving from angle θ can be written as:

$$a_m(\theta) = e^{-j2\pi m d \sin\theta} \tag{2}$$

where m = 0, ..., M − 1. For several emitters, the steering matrix is formed by collecting the steering vectors corresponding to the individual source directions:

$$\mathbf{A} = [\mathbf{a}(\theta_1)\ \mathbf{a}(\theta_2)\ \dots\ \mathbf{a}(\theta_D)] \tag{3}$$

where D is the assumed number of spatially separable sources. The practical MUSIC procedure starts from the estimation of the spatial covariance matrix using N samples collected from the antenna channels:

$$\mathbf{R}_x = \frac{1}{N}\mathbf{X}\mathbf{X}^H \tag{4}$$

The covariance matrix is decomposed into signal and noise subspaces by eigenvalue decomposition. The eigenvectors associated with the largest eigenvalues span the signal subspace, while the remaining eigenvectors form the noise subspace:

$$\mathbf{R}_x = \mathbf{E}_s\mathbf{\Lambda}_s\mathbf{E}_s^H + \mathbf{E}_n\mathbf{\Lambda}_n\mathbf{E}_n^H \tag{5}$$

The MUSIC pseudo-spectrum is then evaluated by testing candidate steering vectors against the noise subspace. Peaks of the pseudo-spectrum indicate directions whose steering vectors are nearly orthogonal to the estimated noise subspace:

$$P_{\text{MUSIC}}(\theta) = \frac{1}{\|\mathbf{E}_n^H\mathbf{a}(\theta)\|^2} \tag{6}$$

In practical implementations, the number of assumed sources D must be configured or estimated. In the GNU Radio implementation used in this work, the source dimension is a configuration parameter of the DOA MUSIC block. This parameter determines the dimension of the signal subspace and, consequently, the dimension of the noise subspace used in (6).

- *GNU Radio simulation setup and preliminary DOA estimation results*

The GNU Radio flowgraph models a four-element ULA. The Signal Source blocks represent independent simulated emitters, while the Multiply by Matrix block applies the steering matrix and generates the four antenna-channel signals. Therefore, the inputs of the matrix block correspond to signal sources, whereas its outputs correspond to the antenna elements. The resulting antenna-channel streams are converted into vectors and processed by the DOA MUSIC block.

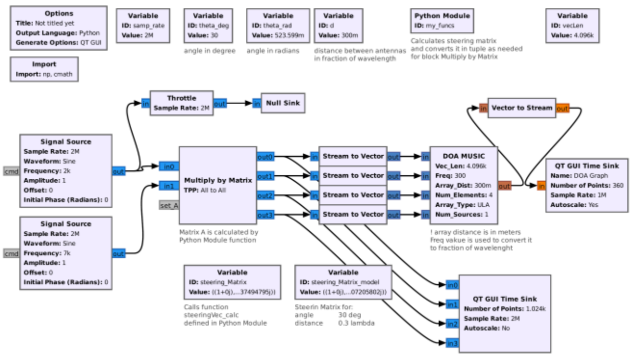

Fig. 4. GNU Radio flowgraph for simulated multichannel SDR-based spatial signal analysis.

For the simulation, the array type is ULA, the number of antenna elements is four, and the inter-element spacing is 0.3λ. The vector length used by the MUSIC processing block is 4096 samples, and the sample rate of the GNU Radio flow graph is 2 MS/s. In the reference scenario, a single source is placed at 30°. In the two-source scenario, a second source is introduced at 80°, while the reference source remains at 30°.

In the single-source case, the steering matrix contains one active steering vector and the MUSIC block is configured for one source. Within an unambiguous observation sector, the expected result is one dominant pseudo-spectrum peak near 30°. However, because the simulated array is a ULA and the displayed scan covers the full 0°–359° angular interval, a mirror peak may also appear. This effect is a geometrical ambiguity of the array rather than a second physical emitter. The case therefore verifies the consistency between the simulated array model and the DOA estimation chain, while also illustrating the angular ambiguity of linear arrays.

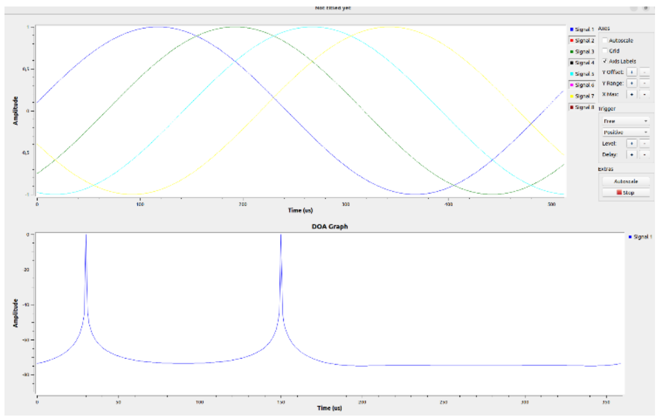

Fig. 5. MUSIC pseudo-spectrum for the reference single-source scenario at 30°.

In the two-source case, the steering matrix is extended to two columns corresponding to 30° and 80°, and the MUSIC block is configured for two sources. In an unambiguous sector, the expected result is the appearance of two distinguishable pseudo-spectrum peaks. In the full 0°–359°

scan used for visualization, each of these directions can also produce its mirror counterpart due to the ULA geometry.

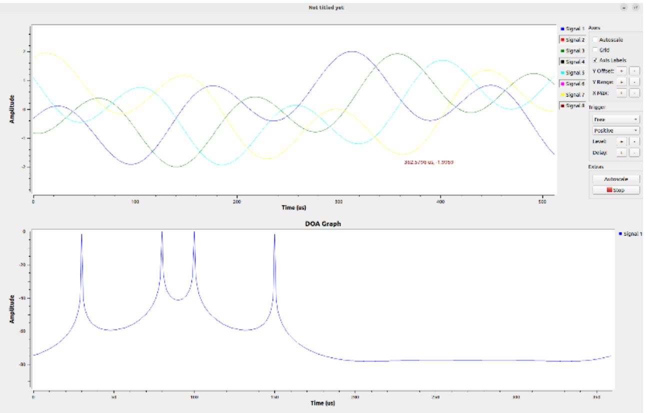

Fig. 6. MUSIC pseudo-spectrum for the two-source spatial inconsistency scenario with emitters at 30° and 80°.

From an EP perspective, the second peak may be interpreted as a spatial inconsistency when only one legitimate emitter direction is expected. This condition does not by itself prove deception or spoofing, but it provides an additional spatial indicator that can be combined with time, frequency, phase, power, and correlation consistency checks.

- *Practical implementation and coherence issues*

Although the simulation demonstrates the conceptual feasibility of SDR-based spatial signal analysis, physical implementation is considerably more demanding. Practical AoA/DOA estimation, beamforming, null steering, and spatial consistency analysis require a phase-coherent multichannel receiver. This requirement is difficult to satisfy with commonly available SDR platforms, because they are typically two-channel devices. For a four-element array, a practical low-cost approach may require two USRP B210 devices operated as a combined receiver.

The initial practical configuration considered in this work uses two USRP B210 devices synchronized by an external OctoClock. The OctoClock distributes common timing and frequency references, which is a necessary step toward coherent operation. However, a common 10 MHz reference and PPS do not automatically guarantee deterministic inter-device carrier phase alignment. Even when both B210 devices are locked to the same external references, an unknown phase offset may remain between the channels belonging to different devices.

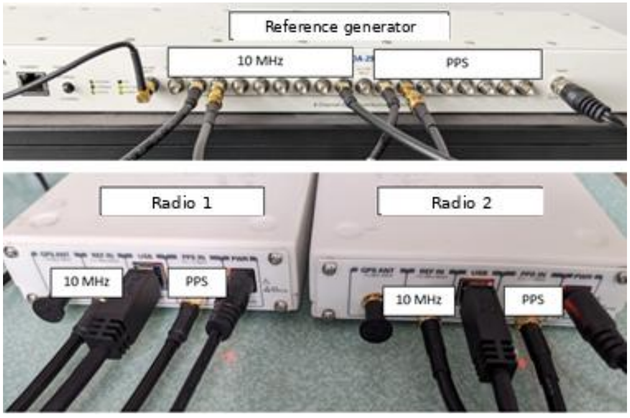

Fig. 7. Initial experimental setup for coherence establishment between two USRP B210 devices using an external OctoClock/reference generator distributing 10 MHz and PPS signals.

The residual phase ambiguity is critical for array processing because the steering model in (2) assumes known and stable inter-channel phase relationships. If the actual received channel contains an additional unknown phase term, the effective received samples can be represented as:

$$\tilde{x}_m[n] = x_m[n]e^{j\phi_m} \qquad (7)$$

where φ_m is the residual phase offset of the m-th receiver channel. For channels located inside a single coherent SDR device, this term may be stable or easier to calibrate. For channels distributed across separate B210 devices, the inter-device component of ϕ_m may be unknown after startup, retuning, or local oscillator relocking. Therefore, external synchronization must be complemented by explicit phase calibration.

A typical digital compensation step applies an estimated calibration phase to each channel:

$$\hat{x}_m[n] = \tilde{x}_m[n]e^{-j\hat{\phi}_m} \qquad (8)$$

The calibration phase φ̂_m can be estimated by injecting a common reference signal, using a splitter-based calibration path, transmitting a known pilot signal from a fixed direction, or periodically estimating inter-channel phase differences during operation. Without such calibration, MUSIC peaks may be shifted, broadened, or become unstable, and subsequent beamforming or null-steering weights may be incorrect.

- *Discussion and limitations*

The simulation and initial coherence considerations show that SDR can be used not only as a waveform implementation platform, but also as a platform for spatial signal analysis. The GNU Radio model demonstrates how steering-matrix-based antenna-channel generation and MUSIC-based DOA estimation can support source localization and spatial inconsistency detection. These functions are relevant to EP mechanisms such as beamforming, null steering, jammer/source localization, and anti-deception or anti-spoofing indication.

At the same time, the results should be interpreted as proof-of-concept evidence rather than as a complete operational

EP implementation. The simulation does not include RF front-end impairments, antenna mutual coupling, multipath propagation, finite ADC dynamic-range effects, synchronization errors, phase calibration drift, or coherent replay signals. In a real multichannel SDR system, these factors may significantly affect DOA accuracy and may require hardware calibration, spatial smoothing, temporal decorrelation, multi-frequency processing, and joint time-frequency-spatial consistency analysis.

Consequently, the main implementation challenge is not only the MUSIC algorithm itself, but also the establishment and preservation of phase coherence across all receiver channels. This is especially important when the required number of antenna channels exceeds the native coherent channel count of a single SDR device and multiple SDR platforms must be synchronized and calibrated as a single array receiver.

VI. CONCLUSIONS

SDR is a suitable platform for implementing a big part of EP functionality. SDR, enables implementation of adaptive waveforms, frequency agility, spread spectrum techniques, digital filtering, spectrum sensing, interference detection, modulation and coding adaptation, and algorithms for identifying spoofing or deception attempts.

Instead of this cannot implement the entire EP domain by itself. For example, several EP functions are primarily hardware-dependent or system-level in nature. Similarly, beamforming and null steering require more than software. They require different technics such as suitable antenna array, common timing and frequency references, and calibration of the RF channels.

Therefore, the most accurate statement is that SDR is a powerful and convenient implementation platform for adaptive EP, but it is not sufficient as a stand-alone solution for the full EP domain.

The GNU Radio proof-of-concept further shows that SDR can support spatial signal analysis through DOA estimation. This capability can contribute to source localization, beamforming and null steering preparation, and spatial consistency checking for anti-deception and anti-spoofing. However, practical implementation requires a coherent multichannel receiver architecture. Initial considerations with two USRP B210 devices synchronized through an external OctoClock indicate that common timing and frequency references must be complemented by explicit inter-device phase calibration.

REFERENCES

[1] “FM 3-12: Cyberspace operations and Electromagnetic Warfare”, US Army, August, 2021. [Online]. Available: https://irp.fas.org/doddir/army/fm3-12.pdf

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

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

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

[5] 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, Second quarter 2022.

[6] “Allied Joint Doctrine for Electronic Warfare”, NATO Standard AJP-3.6, March 24, 2020.

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

[8] 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.

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

[10] 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.

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

[12] R. O. Schmidt, “Multiple emitter location and signal parameter estimation,” IEEE Transactions on Antennas and Propagation, vol. 34, no. 3, pp. 276–280, Mar. 1986.