Sensor Array and Self-Adaptive Algorithm for DoA Detection of Uncooperative Wi-Fi Transmitters in Wireless Security Enforcement Applications

ETF-Belgrade: Olja Jakovljević, Vojislava Janković, Ana Ćupurdija and Pavle Petrović

***Abstract*—We propose and demonstrate a cost-effective system for detection and estimation of direction of arrival for uncooperative Wi-Fi transmitters at 2.4 GHz. The antenna array is based on two linear four-element patch arrays governed by two digitally controlled microwave switches. The RF receiver comprises two software defined radios (SDRs) and the system control, processing, and visualization are achieved by in-house adaptive algorithms running on a laptop PC. The system is comprehensive, but simple to operate and reproduce. Hence, it provides a robust and appealing practical educational platform.**

***Index Terms*—Direction-of-arrival estimation, radio communication, communication security, phased arrays, patch antennas, software defined radio.**

I. Introduction

GLOBAL ever-growing appetites for on-demand digital media content and always-on communications paradigm led to proliferation of small wireless devices which typically utilize cellular (e.g., GSM, CDMA, and related newer wideband systems), Wi-Fi, Bluetooth, and NFC technologies. With their sophisticated transceivers and powerful processing units, these devices enable utilization of various wireless applications including messaging, voice and video communications, entertainment, navigation, secure data transfer, and internet of things (IoT).

On one hand, modern urban life cannot be imagined without these applications. On the other hand, miniaturization of wireless devices, their massive utilization and omnipresence, inevitably led to hard-to-enforce secure radio-silent environments (e.g., sensitive-information protected areas, secure airport zones, immigration and other policed checkpoints, academic and school examination amphitheaters, etc.). With this in mind, one can easily appreciate that the need for detection of uncooperative transmitting nodes is nowadays greater than ever.

In this work we propose an antenna array, RF receiver and adaptive algorithms for detection and estimation of direction of arrival (DoA) for uncooperative Wi-Fi transmitters in wireless security enforcement applications. The proposed system is small, cost-effective, easy to manufacture and deploy. The proposed system, with its readily distinguishable main components, i.e., antenna arrays, fast digitally controlled antenna switches, RF receivers within the software defined radios (SDRs), and a processing and visualization unit (e.g., a personal computer – PC), provides a comprehensive, yet highly appealing modern educational platform. Although the proposed system operates within the 2.45 GHz Wi-Fi industrial, scientific, and medical (ISM) band, it can be adapted to other frequencies, thus effectively covering different wireless applications.

This work is supported by the IEEE AP-S Student Design Contest.

O. Jakovljević (jo170204d@student.etf.rs), V. Janković (jv170247d@student.etf.rs), A. Ćupurdija (anacupurdija96@gmail.com), and P. Petrović (pavlebpetrovic@gmail.com) are with the University of Belgrade, School of Electrical Engineering, Belgrade, Serbia.

II. System Description

We here propose and present a passive DoA detection system, a block diagram of which is shown in Fig. 1, with two separate uniform linear antenna arrays – one vertical and one horizontal, required to achieve differentiation of targets in both azimuth and elevation. At any moment, only one antenna in each of the arrays is active. This antenna receives electromagnetic (EM) wave emitted from a non-cooperative user (e.g., a mobile phone) and sends the received signal to an SDR unit for down-conversion and initial processing. The proposed SDR is *HackRF One* [1], and the active antenna is selected by *OperaCake* [2], assembly of switches specifically designed for utilization with *HackRF One*.

The signal from the selected antenna is then down converted by the *HackRF One*. This is done by mixing the signal with the local oscillator with digitally tunable frequency (2.45 GHz in our case). The obtained baseband signal is then filtered and sampled in the analog-to-digital converter (ADC) block, where I and Q channels are sampled separately.

The obtained digital signals are then sent to a personal computer (PC), where the DoA algorithms, which will be explained in Section VI, are performed and the relevant parameters are extracted. It is important to note that synchronization of the data from two antenna array shown in Fig. 1, is not necessary, because the data obtained by each of the antenna arrays pertain to independent orthogonal axes. Finally, estimated DoA obtained from both arrays are combined and a three-dimensional (3-D) DoA of the non-cooperative transmitter can be visually presented.

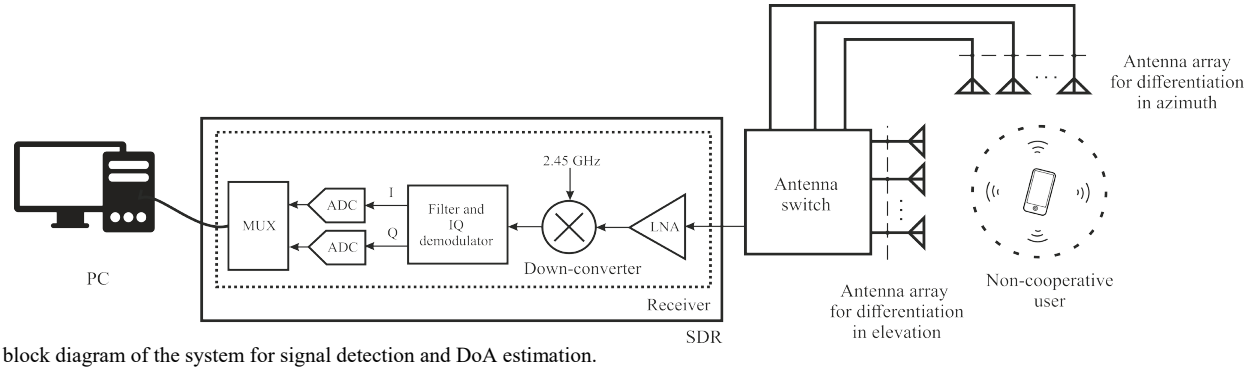

Fig. 1. A block diagram of the system for signal detection and DoA estimation.

III. Bill of Materials

Bill of Materials is summarized in Table I.

TABLE I
BILL OF MATERIALS

Description	Supplier	Amt.	Price $
***HackRF One*, SDR**	DigiKey	2	630.00
Components for *OperaCake*	DigiKey and Farnell	-	100.00
PCB substrate, FR4	Baza M.S.	-	150.00
PCB Manufacturing costs	ETF- Belgrade	-	200.00
Cables and connectors	Farnell	-	300.00
Total price in USD:			**1380.00**

IV. Antenna Array

Eight antennas comprise each of the two linear arrays. This is enough to achieve the desired resolution of 2 m at the distance of 20 m from the system, using Beamformer algorithm. The distance between the antenna elements in each of the arrays is one half of the wavelength at the central frequency, which mitigates the emergence of sidelobes.

The array elements are rectangular microstrip patch antennas. The patches are designed in WIPL-D Pro [3] and fabricated on a double-face metalized 2 mm thick FR-4 substrate. In order to increase the probability of detection for all possible orientations of the transmitter, antennas are designed to have a nearly circular polarization. Patch sides have slightly different lengths (Fig. 3), which leads to two perpendicular modes whose resonant frequencies are similar, but not equal. Each of these modes, alone, would radiate a linear polarization. The feed-point position is optimized so that these two modes are in quadrature at 2.45 GHz. This leads to approximately circular polarization along the main radiation direction, which is practically perpendicular to the antenna plane. Due to manufacturing limitations, the arrays are fabricated in sets of four, one of which is shown in (Fig 2).

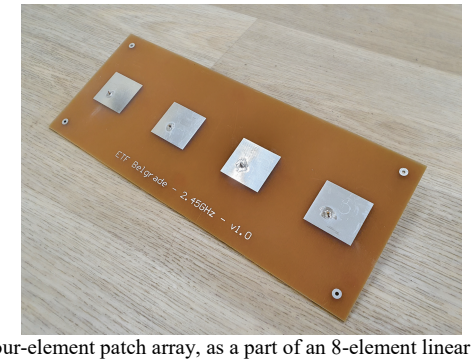

Fig. 2. A four-element patch array, as a part of an 8-element linear array.

Reflection coefficients for each of the antennas in the array were measured and the results are very similar to the results calculated numerically, as shown in Fig. 4. In the entire 2.4 to 2.5 GHz band, reflection-coefficient moduli are smaller than −10 dB, which was the design requirement. Additionally, there are no significant differences in reflection coefficients between the antennas on the same board, which is the result of low coupling between elements. This is very important for array processing techniques.

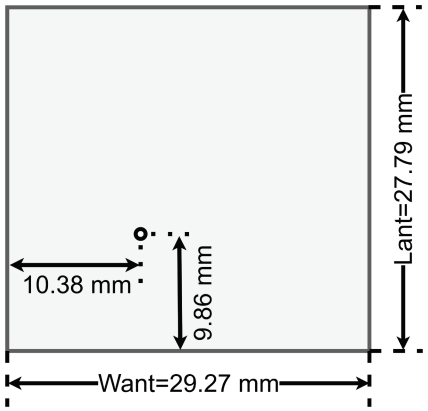

Fig. 3. The footprint of a single patch antenna, with the feed-point position.

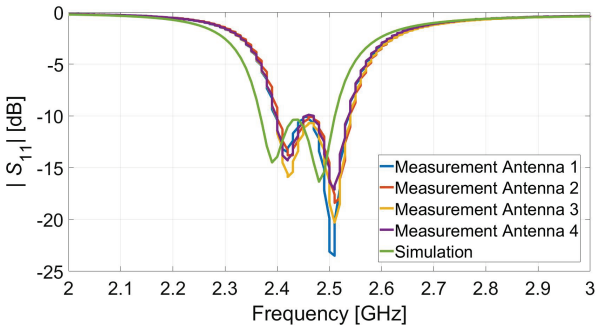

Fig. 4. Reflection coefficients for the four antennas on a single board; comparison of simulated results and measurements.

V. Antenna Switch

A block diagram of the antenna switch (*OperaCake*) is shown in Fig. 5. The corresponding control truth tables are given in Tables II and III. From Fig. 5 and the truth tables, it can be seen that any of the eight antennas on one switch can be selected and connected to any one of the two outputs (PA0 or PB0). From that output, a signal from the selected antenna is transferred to the connected SDR receiver. The board is fabricated on an FR408 substrate [4], and manually assembled. The assembled board can be seen in Fig. 6.

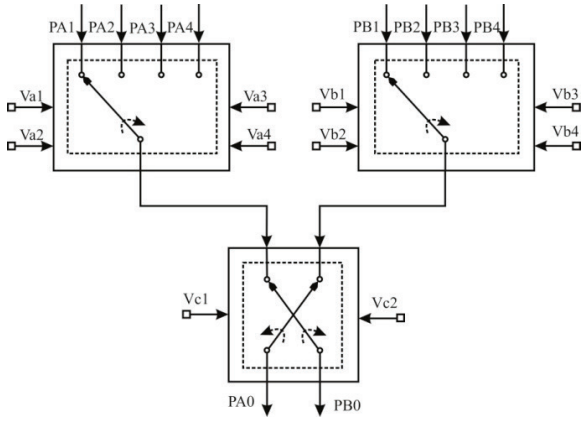

Fig. 5. A block diagram of the antenna switch control.

TABLE II
CONTROL LOGIC FOR THE INPUT SWITCHES.

Vx1	Vx2	Vx3	Vx4	State
1	0	0	0	PX1 on
0	1	0	0	PX2 on
0	0	1	0	PX3 on
0	0	0	1	PX4 on
All other combinations are ill-defined. x ϵ {a, b}.				

TABLE III
CONTROL LOGIC FOR THE OUTPUT SWITCH.

Vc1	Vc2	State
0	0	All off
0	1	PA0 to A section, PB0 to B section
1	0	PA0 to B section, PB0 to A section
1	1	All off

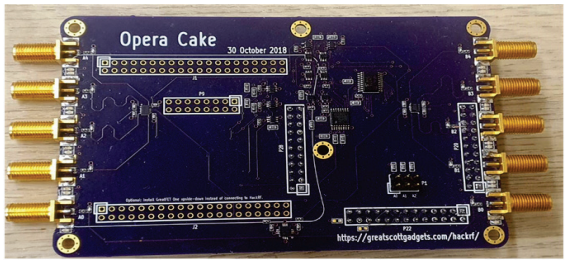

Fig. 6. The assembled *OperaCake* board.

The *S*-parameters of the antenna switch were measured. The isolation, reflection, and transmission coefficients are shown in Fig. 7. It can be seen that at the frequency of interest (2.45 GHz) coupling is about −30 dB between the input port and the antenna ports on the opposite side, and about −37 dB between the input port and the antenna ports on the same side. Reflection coefficients are similar for all antenna ports, whether they are at the same side as the input port, or on the opposite side. The ports are not well matched to 50 Ω (the reflection coefficient is about −3 dB at 2.45 GHz), probably due to uncontrollable board dielectric constant.

From the transmission coefficient shown in Fig. 7, it can be noted that the board adds a significant attenuation to the input signal of about 7 dB at 2.45 GHz. However, this problem can be bypassed by amplifying the signal at the receiver, since *HackRF One* SDR has adjustable gain, both in the RF part of the board, and in the baseband. Of particular significance for the system functionality is the fact that the lengths of transmission lines from the antenna switch to the antennas are constant. This way, the phase differences in signal processing arise from the the object position only, and not from the length differences between the connecting transmission lines. The arguments of the S_{21} parameter from the input port to all the antenna ports were also measured and they are almost constant across the antenna ports.

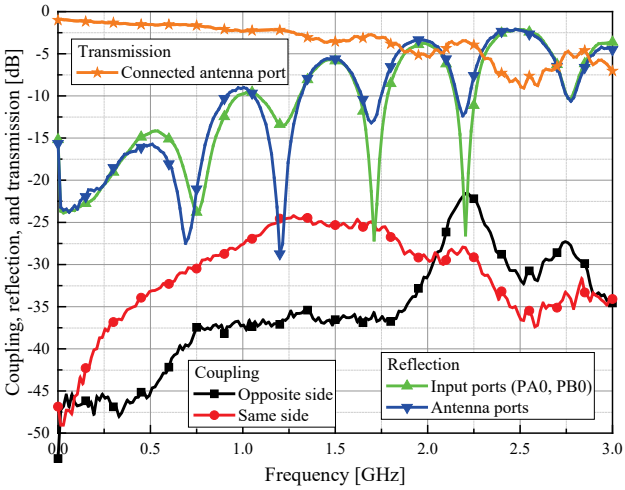

Fig. 7. Isolation, reflection, and transmission coefficients of the *OperaCake*.

This covers all hardware components of the system. Partially completed system, which differentiates targets by their azimuth angle, is shown in Fig. 8. Two *HackRF Ones* are used to simplify the procedure. The connection between *HackRF One* and *OperaCake* boards is done by I2C and GPIO pins.

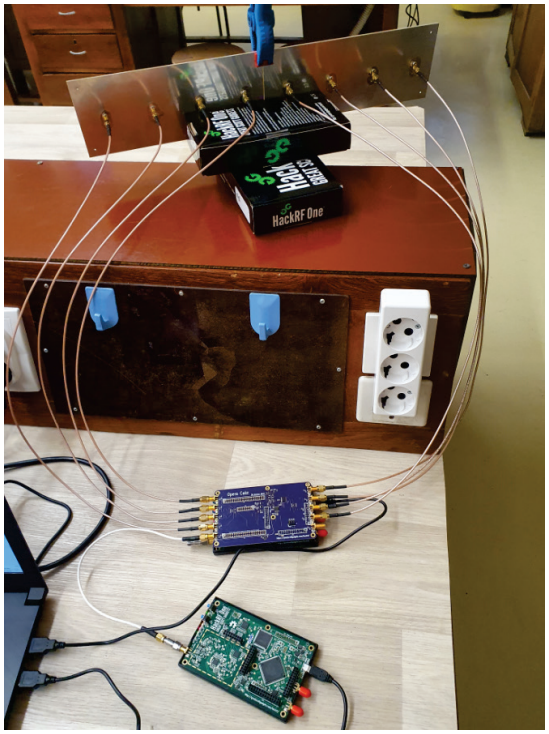

Fig. 8. Two antenna arrays (8 antennas in total) connected to *HackRF One* via the *OperaCake* board.

VI. ALGORITHMS

Once signals from each of the receiving antennas have been acquired, different signal processing algorithms can be used to

estimate the DoA. Three different approaches are implemented in this system:

- Beamforming (with null-steering),
- MUltiple SIgnal Classification (MUSIC), and
- Neural network-based DoA estimation.

For almost every antenna-array signal-processing algorithm, one important common factor is the steering vector

$$[v(\mathbf{k})] = \begin{bmatrix} w_0 \exp(-j\mathbf{k}\cdot\mathbf{p_0}) \\ w_1 \exp(-j\mathbf{k}\cdot\mathbf{p_1}) \\ \vdots \\ w_{N-1}\exp(-j\mathbf{k}\cdot\mathbf{p_{N-1}}) \end{bmatrix}, \quad (1)$$

where $\mathbf{k}$ stands for the wave vector of an incident wave, $\mathbf{p}_i$ is the vector position of the i-th element of the antenna array, and w_i represents a real weighting coefficient. Different weighting functions can be used to reduce the level of side lobes.

Beamforming is a method for shaping of the received signals, so it can be used for estimation of the DoA. The goal of beamforming is selection of the signal from the desired direction without degradation, while improving signal-to-interference and noise ratio (SINR), and attenuating the signals from other directions. Out of the three algorithms, the beamforming is the easiest to implement, as it consists of scalar multiplication of a steering vector and the vector that contains samples from each of the receiving antennas,

$$P_{\mathrm{BF}} = [v]^{\mathrm{T}}_{N\times 1} \cdot \left[M_{\mathrm{samples}}\right]_{N\times 1}, \quad (2)$$

where N is the number of antennas, T stands for matrix or vector transposition operator, and P_{BF} is the criterion function for the beam forming algorithm.

The MUSIC algorithm is specially designed for estimation of DoA parameter using samples of received signals, rather than extracting the signal arriving from a certain direction. It decomposes the received signals into signal subspace and noise subspace, so as to leverage special properties of these subspaces for estimating the DoA. The criterion function for the MUSIC algorithm can be written as

$$P_{\mathrm{MUSIC}} = \frac{1}{[v]^{\mathrm{T}}[E_n][E_n]^{\mathrm{T}}[v]}, \quad (3)$$

where v represents the steering vector, while $[E_n]$ is a matrix containing eigen vectors of the noise subspace. MUSIC requires extensive calculations since the eigen-value-decomposition of the spatial covariance matrix is required in the DoA estimation process. Due to this approach, it can achieve much finer resolution than beamforming at the expense of higher sensitivity to noise and computational cost.

As a final algorithm for the estimation of DoA, we will consider radial basis function neural networks (RBF-NNs). RBF-NNs have a highly parallel distributed architecture that enables fast data transfer from the input to the output of a neural network, which is suitable for dimensional and nonlinear problems. The second, nowadays popular approach, is deep learning when the network consists of many types of hidden layers, giving rise to the name *deep* learning. The basic principle of convolutional neural networks (CNNs) is that they make intensive use of a moving filter. Usually, there are several filters for each layer which enable extraction of many different features, rather than just one.

With overall DoA detection system goals in mind, we propose the concept of a multi-layer detection. When a high DoA resolution is required, we would use the MUSIC algorithm. If the space in which the system is deployed produces a lot of interference, we can suppress some of the components using a null steering method. Moreover, if we have a good set of training data, an artificial neural network is a good choice for real-time and accurate DoA detections. Finally, if there is a lot of noise, or the signal is weak, or an unknown scenario occurs, the beamforming method would be used, as it is the least sensitive to poor signal quality and can be used in the most general case.

VII. System Setup and Measurement Results

The final system setup is shown in Fig. 9. In the figure, the *HackRF One* is controlled by *GNURadio* [5], with the sampling frequency of 1 MHz, and local oscillator (LO) frequency set to 2.45 GHz. The *GNURadio* flowgraph is shown in Fig. 10. The SDR acquires the data from the antennas and, using a buffer, packs them into a block of 4096 samples. A custom code is written in *Python*; it obtains a block of data from each antenna and writes it into a binary file. A binary file contains samples from one switch rotation, namely from all of the eight antennas. A binary file containing all of the sample indices is also created, for synchronization purposes. As soon as the data from one antenna is saved, the switch changes its position to the next one. The obtained data is further processed with beamforming and MUSIC algorithms. After processing, a modified constant-false-alarm-rate (CFAR) algorithm was implemented in order to find peaks in the resulting signal. Peaks maxima are indicators of the signal coming from a target and they determine its azimuth and elevation. Estimated signal DoA is then shown in real time using *Python* graphical-user-interface (GUI) application.

As mentioned, all hardware control and signal processing algorithms are implemented in *Python*, hence, for *Python* processing, a more suitable model of the neural network was a deep learning CNN model. Inputs of the model are autocorrelation values of samples from each of the antennas given in the form of a vector and the outputs are classes that represent the DoA of a signal. Each output class represents one angle and values of the output are numbers between 0 and 1. The maximal output value determines the DoA of the signal. Our future work will be aimed at completing substantial number of additional measurements in order to collect enough data to establish a reliable dataset. In addition, we will complete the training of the network and comparison of the results obtained using different DoA estimation methods.

In Fig. 9 a vector network analyzer was used as the signal source, connected to an antenna to simulate a non-cooperative transmitter. Please note that there is no synchronization between the system and the source. Transmitting antenna is located about 30° off the boresight axis of the receiving array.

Beamforming and MUSIC algorithms are applied to calculate the azimuth and elevation angle of the transmitter in this scenario. The criterion functions for azimuth calculation are shown in Figs. 11 and 12. The peaks in the functions correspond to the system estimation of the direction of arrival.

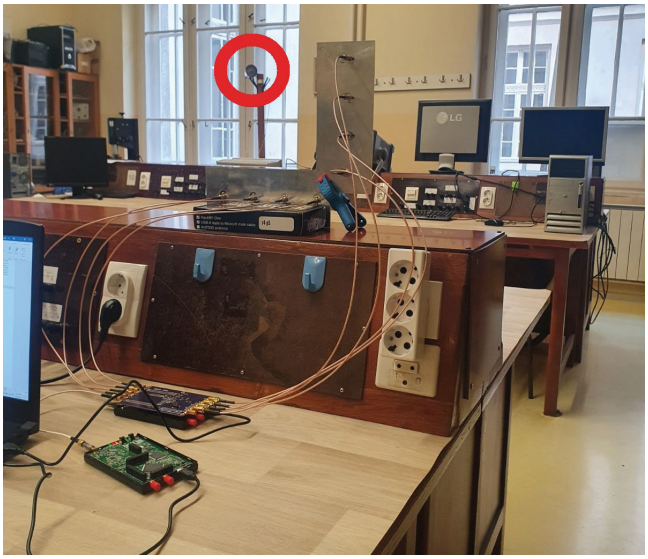

Fig. 9. Test setup. The transmitting antenna is marked with a red circle.

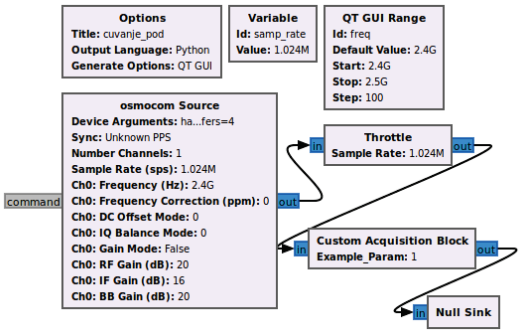

Fig. 10. *GNURadio* flow graph for the *HackRF One* control.

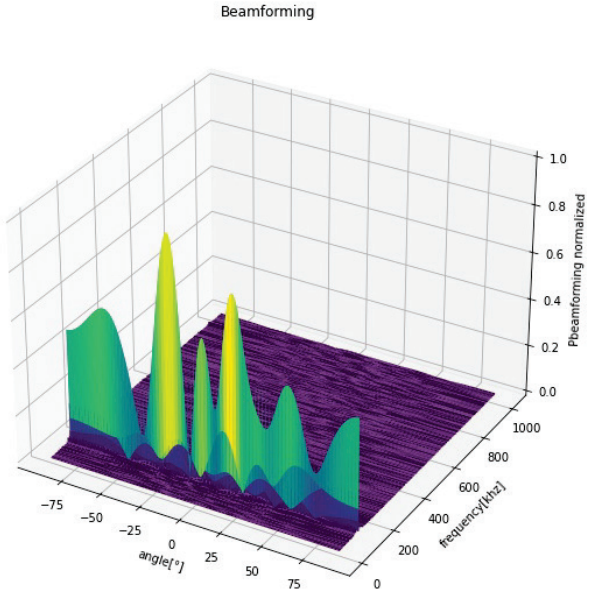

Fig. 11. Criterion function of the Beamformer algorithm vs. the azimuth angle and baseband frequency.

Due to the nature of the employed algorithms, Beamforming is done with respect to both the angle and the frequency, while MUSIC is performed at a single frequency.

Finally, Fig. 13 shows the results presented in a minimalistic GUI application which depicts probable detections calculated from the criteria functions using a CFAR algorithm.

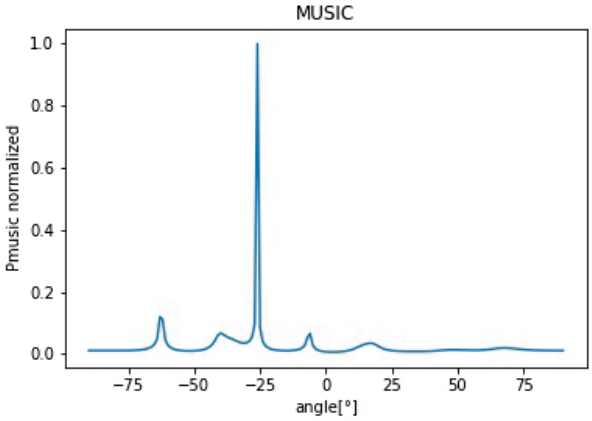

Fig. 12. Criterion function of the MUSIC algorithm vs. azimuth angle.

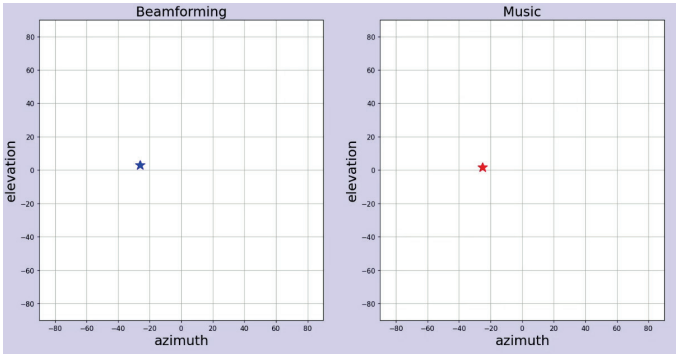

Fig. 13. Detected transmitter with estimated DoA presented in the GUI of the developed application using two algorithms; Beamformer (left) and MUSIC (right).

ACKNOWLEDGMENT

The authors would like to thank IMTEL Komunikacije a.d. for invaluable technical support in the board assembly.

REFERENCES

[1] *HackRF One*. Available: https://greatscottgadgets.com/hackrf/one/
[2] *OperaCake*. Available: https://greatscottgadgets.com/hackrf/antennaswitch/
[3] WIPL-D Pro. Available: https://wipl-d.com/
[4] Isola Group. Available: https://www.isola-group.com/pcb-laminates-prepreg/fr408/
[5] GNURadio. Available: https://www.gnuradio.org/