This is a post-peer-review, pre-copyedit version of an article published in IEEE EUROCON 2017 -17th International Conference on Smart Technologies. The final authenticated version is available online at: https://doi.org/10.1109/EUROCON.2017.8011161

Improved Jamming Resistance Using Electronically Steerable Parasitic Antenna Radiator

Michal Tarkowski, Mateusz Rzymowski, Lukasz Kulas, Krzysztof Nyka
Department of Microwave and Antenna Engineering
Gdansk University of Technology, Faculty of Electronics, Telecommunications and Informatics
Gdansk, Poland
michal.tarkowski@pg.gda.pl, mateusz.rzymowski@eti.pg.gda.pl, luke@eti.pg.gda.pl, nyx@eti.pg.gda.pl

***Abstract*—This paper presents an idea of using an Electronically Steerable Parasitic Antenna Radiator (ESPAR) for jamming suppression in IEEE 802.11b networks. Jamming (intentional interference) attacks are known to be effective and easy to perform, which may impose connectivity problems in applications concerning Internet of Things (IoT). In our paper, theoretical considerations are presented and the results of experiments performed in anechoic chamber are examined. During the test, IEEE 802.11b standard was used to provide communication between transmitter and receiver, and Software Defined Radio (SDR) device, which was used as a source of an intentional interference (jammer). The results showed that connectivity during jamming attack can be improved by using switched-beam antenna enhancing system's bandwidth.**

Keywords*—*jamming, electronic warfare, Electronically Steerable Parasitic Antenna Radiator (ESPAR) antenna, reconfigurable antenna,

I. INTRODUCTION

After years of developing reliable wireless network technologies for civilian applications, physical layer security is receiving its fair attention only since past few years [1]. The biggest advantage and, simultaneously, drawback of wireless technology is its openness. The communication channel can be accessed freely by anyone who is located in a range of the network. This means that a proper communication should fulfill the best cryptography standards to avoid data interception by an eavesdropper. But sometimes even this is not sufficient as the other important treat is a possibility of presence of unwanted signals, which aim at disrupting the valid ones. Such intentional attack on a wireless communication system is called jamming. The hazard of this treat is higher than ever before, because of low costs and higher accessibility of advanced RF devices, which can be used for malicious intentions. From this respect, fighting jamming in physical layer can be concerned as a race of higher signal power available, because if enemy has an appropriate transceiver, it can interrupt any kind of communication. Hence, usually suppression of jamming instead of increasing signal power seems to be more appropriate approach as it is more energy efficient [2]-[4].

Problem of interferences in wireless networks has been widely investigated, since its presence is inevitable. Unintentional ones are the main purpose of using multiple access control in communication standards, like carrier sense multiple access (CSMA) or by introducing the electromagnetic compatibility certification. The problem emerges, when wireless system is fed by malicious signals, which are designed to disrupt its normal work. This kind of threat is serious especially in military applications, where battle against them fully evolved. One of critical devices, that are prone to jamming, are radars, and in this particular area jamming suppression has mostly been developed [2].

One of the most common jamming suppression techniques is using a digital beamforming antenna array and perform beam synthesis techniques like sidelobe cancellation [3], [4]. This is an efficient concept, but demands complicated and expensive devices. Moreover, such an approach is energy consuming, which is a drawback in IoT networks. Using a few signal sources opens an interesting way to limit effectiveness of interfering signal by using signal processing to cancel disrupting signal. An example of this approach is called "spatial dither" [5], [6]. However this, and similar methods rely on multiplication of the number of transceivers, which increase costs in simple IoT systems.

ESPAR antenna is a type of an antenna that is able to change its characteristic with the use of parasitic elements that surround only one active element. Those passive elements are usually described as electrical reactances as their values can change continuously. There are many publications about forming ESPAR characteristic using reactance elements, but it usually implies using varactors and multiple digital-to-analog converters to achieve required precision [7]. Such ESPAR antenna can be used to suppress unwanted signals by shaping its radiation pattern in a proper way [8].

In out paper we have simplified the approach presented in [8] by using switches, instead of varactors to shape ESPAR antenna's radiation pattern. This implies the main design difference: absence of many DACs (Digital-analog Converter), which would be necessary to control each varactor. Using discrete binary values (key switches) instead of voltage levels makes communication protocol easier too, because a whole pattern can be coded by 12 bits. All of those amendments allow to simplify the concept and adapt it to common IoT applications. Our approach assumes using cheap and compact steerable ESPAR antenna to effectively reduce jamming impact on wireless communication. Switching main beam is realized by setting 12-bit sequence by UART protocol, which is possible for most modern radio transceivers, while the approach presented in [8] requires six 12-bit digital control voltages set-up by TMS320C6701 DSP chip. Proposed solution was tested in laboratory conditions in anechoic chamber for IEEE 802.11b standard.

II. APPLICATION CONCEPT

In wireless communication systems, the RF signal is exchanged between the communication parties in a form of the electromagnetic waves that propagates from the transmitter antenna to the receiver antenna that are at a certain distance from each other. This means that, along this way, signal can be influenced by different factors related to a propagation phenomena (e.g. fading, reflections etc.), but also by the intentional or non-intentional interferences e.g. jamming. In the proposed approach the receiver is equipped with an ESPAR antenna that can form and switch main directional beam in such manner that the signal power received from the authorized transmitter is maximized. For the concept verification the communication system model with two desired communication parts and the active jammer without reception capabilities is considered. As the receiving side is the one that can be jammed, it is necessary to analyze jamming influence from the perspective of the receiver. From Friis equation it is known that the amount of power received by the receiver antenna depends on power radiated by the transmitter $P_T G_T$, a distance between the transmitter and the receiver d_{RT}, wavelength λ, and receiving antenna's gain G_R:

$$P_R = G_R P_T G_T \left(\frac{\lambda}{4\pi d_{RT}} \right)^2 . \quad (1)$$

Considering a number of geometrically located signal sources transmitting towards the receiver equipped with a reconfigurable antenna, with the capability to switch the main directional beam, the angular dependencies between them should be introduced. This is due to the fact, that the receiving antenna gain value can differ depending on the incoming signal direction so receiving antenna's gain G_R should be written as:

$$G_R = G_R(\varphi, \theta), \quad (2)$$

where φ and θ are azimuthal and polar angles, respectively. Hence based on (1) and (2) the received power from the transmitter can be calculated using the following formulae:

$$P_{RT} = G_R(\varphi_T, \theta_T) P_T G_T \left(\frac{\lambda}{4\pi d_{RT}} \right)^2 , \quad (3)$$

where $G_R(\varphi_T, \theta_T)$ is receiver's antenna gain in the direction of the transceiver, while the power of jamming signal received by the receiver can be obtained from:

$$P_{RJ} = G_R(\varphi_J, \theta_J) P_J G_J \left(\frac{\lambda}{4\pi d_{RJ}} \right)^2 , \quad (4)$$

where $G_R(\varphi_J, \theta_J)$ is receiver's antenna gain in the direction of the jammer, $P_J G_J$ is power transmitted by jammer towards the receiver and d_{RJ} is a distance between jammer and transmitter. Relating (4) to (3) gives the following formula:

$$\frac{J}{S} = \frac{P_{RJ}}{P_{RT}} = \frac{G_R(\varphi_J, \theta_J) P_J G_J d_{RT}^2}{G_R(\varphi_T, \theta_T) P_T G_T d_{RJ}^2} , \quad (5)$$

which is jamming to signal ratio (JSR) and is an elementary measure for jamming influence analysis which determines the degree to which jamming will be successful [9]. In a case when all parties are equipped with monopole antennas, the gain of the receiving antenna is symmetrical in azimuth. Thus, the gain toward the jammer will be the same as the gain toward the desired receiver, so the last two terms (G_{RJ} and G_{RT}) cancel each other. In this case, JSR depends only on radiated powers and distances from each antennas, which the receiver usually cannot change. In the proposed concept, by switching the main directional beam, the relation (5) can be minimized by modifying the receiver's antenna gain towards both jammer and transceiver. The geometrical interpretation of this situation is presented in Fig. 1.

Because of utilizing spatial discrimination, the worst case for our concept is when jammer occludes transmitter at the same propagation line (is located between transmitter and receiver). In this situation our concept may fail as it is impossible to distinguish signals from jammer and transmitter. When angular distance is less than main beam's 3 dB beam width, the possibility of jamming suppression declines.

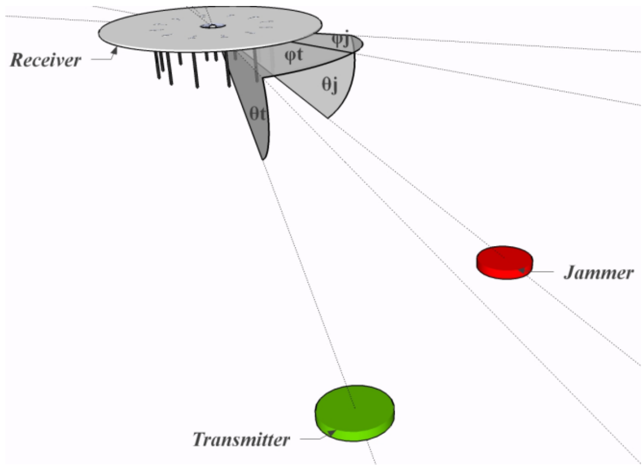

Fig. 1 Geometrical interpretation of the proposed concept. Jammer and transmitter are located at different angular positions around the receiver.

III. The Antenna

The antenna is realized to operate in 2.4 GHz frequency and a whole design is based on [10] which had been adopted for radio localization in indoor environments [11], [12]. This is a twelve elements ESPAR array with one monopole radiator at its center. Parasitic elements around the monopole can be shortened to the ground or opened by the SPST (Single Pole, Single Throw) switches. Opened elements can be considered as directors and shortened ones as reflectors. This gives an opportunity to form a beam of the antenna by manipulating SPST switches. Realized ESPAR antenna is depicted at Fig. 2 and Fig. 3. Antenna employs a classic PCB base with 1.55 mm thick dielectric ground with ε_r = 4.5. Besides antenna, the design includes NXP JN-5168 microcontroller which allows for steering the SPST switches by the UART protocol.

Fig. 4 presents measured antenna's maximum characteristic on f = 2.45 GHz and θ = 50°, which corresponds with a measurement set-up used in our experiments. In this setup, four of twelve switches are acting as directors toward beam direction. This implies beam switching resolution of 30° (in horizontal plane, 360° divided by number of parasitic elements). Measured width of 3-dB main beam equals about 60°.

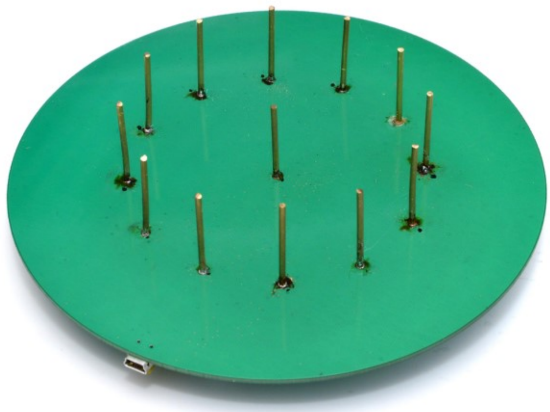

Fig. 2 The realization of ESPAR antenna used in this paper (front side).

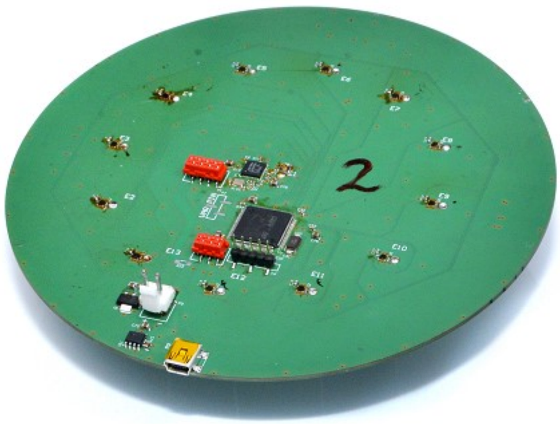

Fig. 3 The realization of ESPAR antenna used in this paper (rear side).

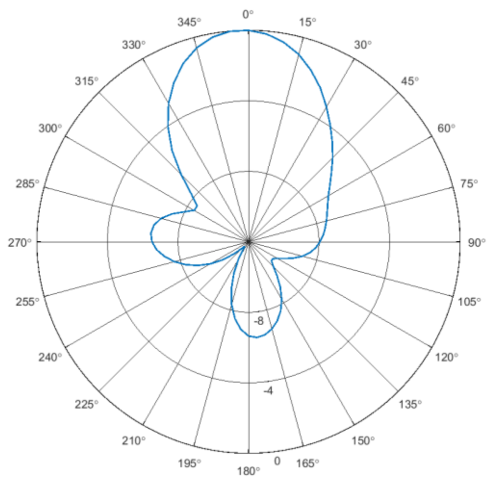

Fig. 4 ESPAR antenna characteristic measured in anechoic chamber across azimuth angle φ.

Table 1 presents measured antenna gain calculations, which can be considered as JSR reduction when transceiver lies on φ = α angle and jammer is localized at φ = β.

TABLE I. JSR REDUCTION AT DIFFERENT POSITIONS OF JAMMER AND TRANSCEIVER

Jammer angular position β	Transceiver angular position α		
	α = 0°	*α = 90°*	*α = 180°*
0°	0	6.527	6.655
30°	**-3.18**	3.4	3.51
60°	-6.78	-0.24	-0.13
90°	-7.94	-1.4	-1.3
120°	-10.1	-3.59	-3.462
150°	-8.22	-1.68	-1.59
180°	-6.65	-0.13	0
210°	-10.8	-4.33	-4.17
240°	-9.52	-3.01	-2.85
270°	-6.52	0	0.12
300°	-8.42	-1.88	-1.792
330°	-2.94	3.6	3.71

As can be seen, jamming suppression capabilities depend on angular positions of jammer and transceiver and varies from −10.8 dB to 6.655 dB. In this paper, we want to examine not favorable, yet common arrangement when jammer and transceiver are 30° from each other.

IV. THE EXPERIMENT

A. *Methodology and measurement setup*

To examine jamming impact, JSR value can be directly measured for each antenna configuration. To calculate this value, legitimate and interference signals have to be measured separately. To do this, we used handheld N9340B RF spectrum analyzer with 22 MHz channel average power measurement. Additionally, we found more convenient to measure an effective network bandwidth between transmitter and receiver, because it takes into consideration correction mechanisms of higher ISO/OSI layers and show degeneration of channel's quality more practically. To accomplish this, we used *iperf3* [13] software which allows for traffic simulation and measurement in client-server architecture. As communication protocol we used IEEE 802.11b standard in order to utilize DSSS modulation scheme which is commonly found in IoT applications (e.g. IEEE 802.15.4 standard). As receiver and transmitter we used Portwell Nano6060 embedded computer with Gentoo Linux and software needed for wireless communication (*hostapd* for an access point, *wpa-supplicant* for a client). As a jammer, we used National Instruments USRP SDR device, connected to dedicated computer with LabView 2013 controlling its operation. Interference signal was a continuous waveform tone at channel's center frequency which was, for 9th IEEE 802.11b channel, 2.452 GHz. This method is considered as one of the most efficient for DSSS modulation jamming [9]. Both jammer and transmitter were equipped with the same Ettus Vert 2450 monopole 2.4 GHz omnidirectional antenna. Each component of measurement set was connected to the Ethernet switch and controlled by PC outside the anechoic chamber. Described setup can be seen in Fig. 5.

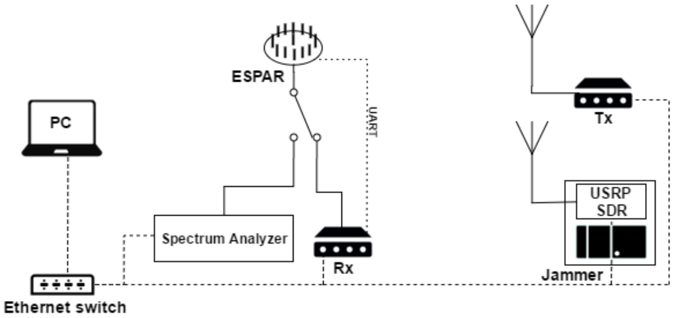

Fig. 5 Scheme of measurement setup for conducted experiments.

Sweeping main beam in ESPAR was realized by connecting microcontroller with the receiver using UART. Microcontroller controlled switches on ESPAR's board digitally and a special script was developed to communicate remotely with receiver's UART. According to [10], main beam in a given direction was realized by opening four consecutive elements via SPST switches, while the rest were shortened to the ground.

Output power of both, transceiver and jammer, was measured using handheld spectrum analyzer. For the transceiver we measured 8.9 dBm/22MHz (IEEE 802.11b channel) and −28.77 dBm peak value, which is constant for each experiment we performed. Jammer's output power stands at −8.3 dBm/22MHZ and −25.4 dBm tone's peak value and every jammer's power level in this paper is presented referring to this value.

B. Measurement scenario

Measurements were performed in anechoic chamber to reduce common propagation effects (like reflections, diffractions and others) and to separate test's environment from the exteriors. We placed tested devices on a plan of a triangle with jammer and TX separated using electromagnetic absorbers, mainly for safety reasons. ESPAR antenna was mounted using metallic stand and directed at θ = 50° elevation angle towards jammer and TX device. We assumed φ = 0° azimuth angle towards TX device. This set-up is presented in Fig. 6.

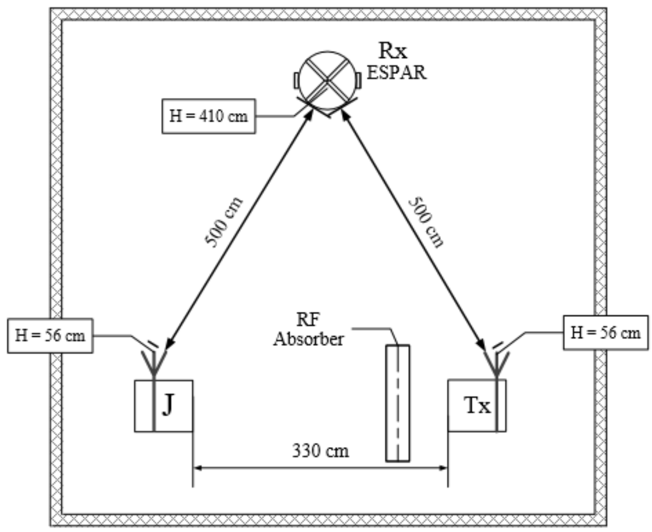

Fig. 6 Geometrical configuration of experiment's components.

After placing each component in anechoic chamber, we performed every experiment in a two stages. Firstly, we connected ESPAR antenna into the spectrum analyzer for channel power measurement. We swept beam angle of ESPAR antenna and we were changing jammer output power. With jammer turned off and transceiver turned on, we were able to measure P_{RT}. By deactivating transceiver, we measured P_{RJ}. Obtained quantities let us to calculate JSR coefficient at receiver's input for each beam angle φ. The next step was to measure network bandwidth for a different jamming output powers. For this, we connected ESPAR to the receiver and swept both beam angle and jamming power during *iperf3* UDP test.

C. Results

In Fig. 7 the results of JSR measurement are shown. The transceiver and the jammer were positioned at angle φ = 0° and φ = 30° respectively (as indicated on the figure). As it can be seen, JSR differs by about 2 dB at those directions. The biggest jamming suppression can be observed at transceiver location and about 240° from jammer (φ = 270°). This effect emerges directly from antenna characteristic. Nevertheless, this scenario clearly shows that it is possible to change JSR significantly at some direction even if angular distance between transceiver and jammer is relatively small.

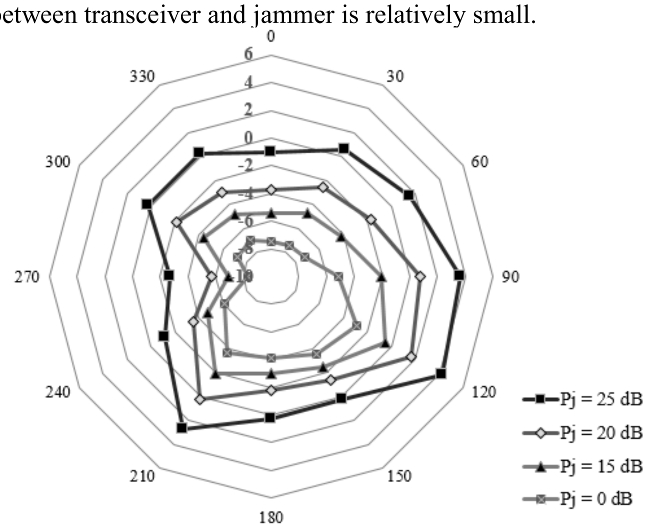

Fig. 7 JSR levels for different beam's azimuth angles φ and for selected jammer's output powers.

In Fig. 8, similar results are shown, but considering more practical benchmark – jamming impact on connection's bandwidth. As it can be seen, beam angle's direction has great influence on communication's quality. For small jammer's output values *Pj*, both parties are able to retain connection for each beam angle value, but the impact of jamming already exists. Especially on three angles φ = {120°, 210°, 300°}, where bandwidth decreases fiercely, even for the weakest jammer gain *Pj* = 0 dB. As it was expected, bandwidth declines as jammer's power increases until first communication breakdown appears at *Pj* = 15 dB for two angles. Under the heaviest jamming signal, the basis of our concept can be seen in the most obvious way. For the majority of beam angles, connection is interrupted. But for two of them (φ = {0°, 270°}) is still possible.

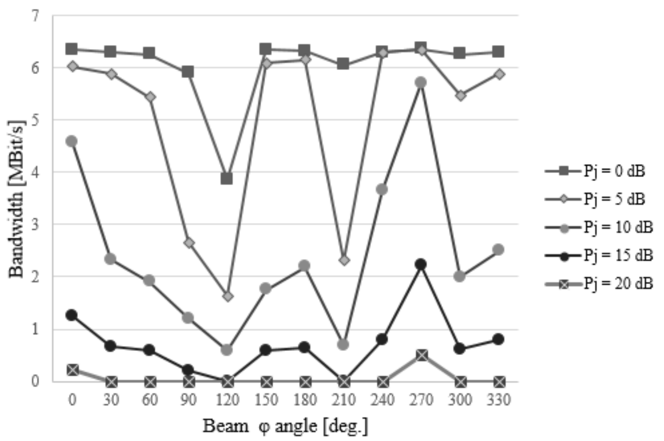

Fig. 8 Network bandwidth for different beam's azimuth angles φ and for selected jammer's output powers.

The last trial illustrates more detailed examination of jammer's power impact on network's bandwidth in selected directions. And, in addition, omni-directional configuration (open switches) was shown to proof the benefits of using steerable antenna. As can be seen in Fig. 9, in both unfavorable situations connection is interrupted definitely above 20 dB jammer's power. In φ = 0°, which is the transceiver direction, communication retains nearly under 10 dB higher jammer's gain. This proves usefulness of ESPAR antenna in jamming suppression.

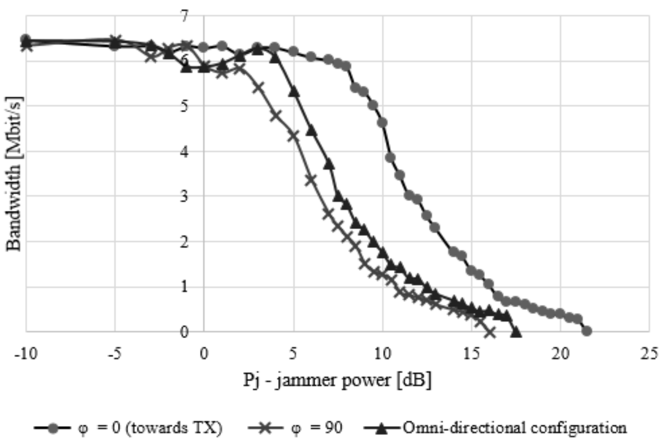

Fig. 9 Network bandwidth for different jammer's output power and for selected beam's azimuth angles.

V. Conclusion

In this paper it has been shown that jamming resistance can be improved using electronically steerable parasitic antenna radiator (ESPAR) antenna. Even when angular distance between jammer and transceiver is small, a receiver equipped with ESPAR antenna can suppress interference signal, thus boost communication quality and retain connection. For the concept verification, tests in anechoic chamber were prepared and conducted. Jamming to signal ratio (JSR) as well as transmission bandwidth has been measured and clearly showed that by modifying antenna's characteristic, it is possible to find the antenna configuration where the JSR is the lowest, so the system can still operate.

Acknowledgment

This work has been conducted within the ENABLE-S3 project that has received funding from the ECSEL Joint Undertaking under Grant Agreement no. 692455. This Joint Undertaking receives support from the European Union's HORIZON 2020 research and innovation programme and Austria, Denmark, Germany, Finland, Czech Republic, Italy, Spain, Portugal, Poland, Ireland, Belgium, France, Netherlands, United Kingdom, Slovakia, Norway. This work was also partially supported by Polish Ministry of Science and Higher Education grant for statutory activities at Faculty of ETI, Gdansk University of Technology.

References

[1] M. J. Marcus, "Growing consumer interest in jamming: spectrum policy implications [Spectrum Policy and Regulatory Issues]," in IEEE Wireless Communications, vol. 21, no. 1, pp. 4-4, February 2014.

[2] L. Neng-Jing and Z. Yi-Ting, "A survey of radar ECM and ECCM," in IEEE Transactions on Aerospace and Electronic Systems, vol. 31, no. 3, pp. 1110-1120, Jul 1995.

[3] R. Baseri, K. B. Yu and M. A. Hussain, "Testing adaptive jamming cancellation algorithms using a digital beamforming array," Proceedings of the 1997 IEEE National Radar Conference, Syracuse, NY, 1997, pp. 314-319.

[4] O. G. Vendik and D. S. Kozlov, "Phased Antenna Array With a Sidelobe Cancellation for Suppression of Jamming," in IEEE Antennas and Wireless Propagation Letters, vol. 11, no. , pp. 648-650, 2012.

[5] B. Widrow, K. Duvall, R. Gooch and W. Newman, "Signal cancellation phenomena in adaptive antennas: Causes and cures," in IEEE Transactions on Antennas and Propagation, vol. 30, no. 3, pp. 469-478, May 1982.

[6] T. Hanson, "Subarrays, spatial dither and coherent interference rejection," Southeastcon '92, Proceedings., IEEE, Birmingham, AL, 1992, pp. 238-241 vol.1.

[7] J. J. Luther, S. Ebadi and X. Gong, "A Microstrip Patch Electronically Steerable Parasitic Array Radiator (ESPAR) Antenna With Reactance-Tuned Coupling and Maintained Resonance," in IEEE Transactions on Antennas and Propagation, vol. 60, no. 4, pp. 1803-1813, April 2012.

[8] Chen Sun, A. Hirata, T. Ohira and N. C. Karmakar, "Fast beamforming of electronically steerable parasitic array radiator antennas: theory and experiment," in IEEE Transactions on Antennas and Propagation, vol. 52, no. 7, pp. 1819-1832, July 2004.R.

[9] A. Poisel. Modern Communications Jamming Principles and Techniques. Artech House Publishers, 2006

[10] M. Rzymowski and Ł. Kulas, "Design, realization and measurements of enhanced performance 2.4 GHz ESPAR antenna for localization in wireless sensor networks," Eurocon 2013, Zagreb, 2013, pp. 207-211.

[11] M. Rzymowski, K. Nyka and Ł. Kulas, "Enhanced switched parasitic antenna with switched active monopoles for indoor positioning systems," 2014 20th International Conference on Microwaves, Radar and Wireless Communications (MIKON), Gdansk, 2014, pp. 1-4.

[12] M. Rzymowski, P. Woznica and L. Kulas, "Single-Anchor Indoor Localization Using ESPAR Antenna," in IEEE Antennas and Wireless Propagation Letters, vol. 15, no. , pp. 1183-1186, 2016.

[13] Iperf3 website: http://iperf.fr/ (accessed 11.2016)