Jammers signal power modelling in the Wi-Fi band

Dariusz Czerwinski[1,*], *Slawomir* Przylucki[1], and *Jaroslaw* Nowak[2]

[1]Institute of Computer Science, Lublin University of Technology, Nadbystrzycka 38A Str. 20-618 Lublin, Poland
[2]Polish Air Force Academy, Dywizjonu 303 no. 35 Str, 08-521 Deblin, Poland

Abstract. The distribution of the signal coming from jamming sources is an issue of critical importance to the security and jammer localisation. The paper presents the results of simulations of signal power distribution in the Wi-Fi band conducted for two commercially available jammers, CRJ4000 and CKJ-1502A12. Calculated distributions of signal power were compared with the results from the measurements. The comparison made it possible to assess the correctness of the designed models and out of the simulations. The paper presents the results of simulations and measurements for different scenarios of jammers settings.

1 Introduction

Collecting and reducing the experimental data remains the main method for modelling the radio frequency signal power distribution. However, recent advances in high-frequency simulation software, which is based on ray tracing or path loss modelling, allow assessing signal propagation in different channels [1].

Nowadays, network engineers demand methods for precisely mapping the range of existing and planned networks. The accuracy of those approaches is determined by the good quality of the underlying simulation models. At the basis of the simulations lies the path loss model and the interpolation regime [2].

Path loss model with shadow fading characterization has been shown in [3]. Some fine-tuning of respective models was done in order to compare measurement data with theoretical assumptions. The relative mean error was calculated for each described model [3].

Path loss models are used for localisation purposes for a wide range of applications in 2.4 GHz band. Starting from Bluetooth localisation [4, 5], Wi-Fi devices localisation [6, 7], jammer localisation [8, 9] and finishing on localisation in wireless sensor networks [10, 11].

Near-ground path loss estimation is an important issue in most military and environment monitoring applications of wireless sensor networks. In the article [12] authors present a path loss model for three near-ground scenarios (plaza, sidewalk, grassland). The extensive measurements were carried out and the least-square linear regression was performed. The results indicate that the log-distance-based model is still suitable for path loss modelling in open space near-ground scenarios [12].

This work presents the modelling and measurement results of the signal power generated by two different jammers. Based on the measurement results, distribution of the signal power and theoretical path loss models were elaborated. The remaining parts of the paper are organised as follows: Section 2 describes the modelling of path loss and the signal power propagation. Section 3 describes the modelling and measurement results. Conclusions and future research ideas are presented in Section 4.

2 Modelling the signal power in the Wi-Fi band

Path loss is a basic feature of radio wave propagation, which is often used to calculate the link capacity and determine the range of transmitters.

2.1 Models used in article

In this work, the authors focused on the open space signal propagation. The received signal power in such case is determined by the Friis law, which says that power decreases with the square of distance [13, 14].

In the case of near ground applications signal is dissipated in many different ways, i.e.: coming from obstacles, ground reflections, other devices working in the same band, etc. In such situations, commonly used models are log-distance model with shadowing phenomenon and two-ray ground-reflection model [15-18].

Path loss models can be obtained theoretically [19, 20], but most of them are obtained from the results of measurements [21, 22]. In this article, the authors presented the results of path loss modelling based on experimental results.

If the transmitter and receiver are in the line of sight (LOS) conditions, then commonly used model is the classical log-distance model given by equation (1). In

[*] Corresponding author: d.czerwinski@pollub.pl

this model, a path loss exponent n is introduced to take into account different environments.

$$P_r(d) = P_r(d_0) - 10 \cdot n \cdot \log_{10}\left(\frac{d}{d_0}\right) \quad (1)$$

where: *Pr(d)* – is the power of the signal given in dBm, *Pr(d0)* – is the received signal power at the reference distance *d0* (usually 1 m), *n* – path loss exponent, *d* – is the distance from the transmitter.

In the case when transmitter and receiver are in the LOS conditions and signal is propagating over a smooth well-reflecting terrain, than the path loss can be expressed by equation (2) which is known as a two-ray ground-reflection model [18,23,24].

$$P_r(d) = P_r(d_0) - 10 \cdot \log_{10}\left(\frac{1}{d} + \Gamma \cdot \frac{e^{j2\pi\frac{\delta_d}{\lambda}}}{d + \delta_d}\right) \quad (2)$$

where: $P_r(d)$ – is the power of the signal given in dBm, $P_r(d_0)$ – is the received signal power at the reference distance d_0 (usually 1 m), Γ – is coefficient of Fresnel reflection for the signal given by eq. (3), λ – is a wavelength, δ_d – is additional reflected path given by eq. (4) and,

$$\Gamma = \frac{\sin(\alpha) - \sqrt{\varepsilon_r - \cos(\alpha)^2}}{\sin(\alpha) + \sqrt{\varepsilon_r - \cos(\alpha)^2}} \quad (3)$$

where: *α* – is the angle between the ground and reflected path, ε_r – is ground relative permittivity.

$$\delta_d = \sqrt{(h_t + h_r)^2 + d^2} - \sqrt{(h_t - h_r)^2 + d^2} \quad (4)$$

where: h_t, h_r – are the heights of antennas of the transmitter and receiver accordingly,

2.2 Modelling the signal power of the jammers

This work, presents the distribution of the signal power for two commercially available jammers:

- CRJ4000 cell phone and Wi-Fi handheld jammer [25],
- CKJ-1502A12 stationary jammer [26].

Selected parameters of the jammers were presented in Table 1. Both jammers, according to the manufacturers, have omnidirectional antennas and are working in the temperature range of 15-60 oC.

The EIRP power of the jammers was calculated according to equation (5) and (6):

$$P_t(dBm) = 10 \cdot \log\left(\frac{P_t \quad watts}{1 \quad mW}\right) \quad (5)$$

where: P_t – is the output power given in Watts

$$EIRP = P_t(dBm) + G_t(dB) \quad (6)$$

Table 1. Chosen parameters of the jammers.

Model	CRJ4000	CKJ-1502A12
Output power	2.5 W	up to 30 W
Shielding radius	up to 20 meters at -75 dBm	2-40 meters at -75 dBm
Frequencies	2400-2500 MHz	2400-2500 MHz
Antennas gain	2.8 dBi (2.4 GHz)	9 dBi (2.4 GHz)
Power supply	AC 110-240V (50-60 Hz), DC 12V, 1800 mAh Li-Ion	AC 110-240V (50-60 Hz), DC 12V
Calculated EIRP	36.7 dBm	43 dBm for 2.5 W 53.77 dBm for 30 W
Mobility	handheld	stationary

where: *EIRP* is Equivalent Isotropically Radiated Power given in dBm, *Gt* is antenna gain given in dB.

To calculate the theoretical value of power at distance d0 it is necessary to know the near-field antenna path loss. According to [27] this value can be estimated with equation (7) which was derived from Friis formula:

$$P_l(dB) = -21.98 + 20 \cdot \log\left(\frac{\lambda}{d_0}\right) \quad (7)$$

where: *λ* is a wavelength given in meters.

The received signal power at the reference distance ($P_r(d_0)$) can be calculated by summing the EIRP power and path loss, which should be negative. These values were shown in Table 2.

Table 2. Calculated values of $P_r(d_0)$.

Model	CRJ4000	CKJ-1502A12
Calculated signal power at distance d_0=1 m	-3.26 dBm	2.94 dBm for 2.5 W 13.72 dBm for 30 W

The assumptions above enable calculating the path loss models for two jammers and different values of power in the case of the stationary jammer with the use of formula given in eq. (1). According to the literature and measurements described in the next chapter, it was assumed that path loss exponent in LOS conditions and in open space was equal to n=0.7. The calculated distribution of the signal power is shown in Figure 1.

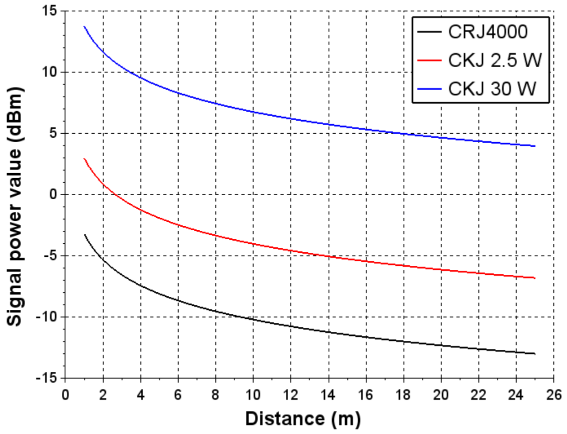

Fig. 1. Signal power versus distance for calculated path loss.

3 Measurement and modelling results

Measurements were performed to verify the model of the power of the signal generated by the jammers in open space in LOS conditions The idea of the measurements is presented in Figure 2.

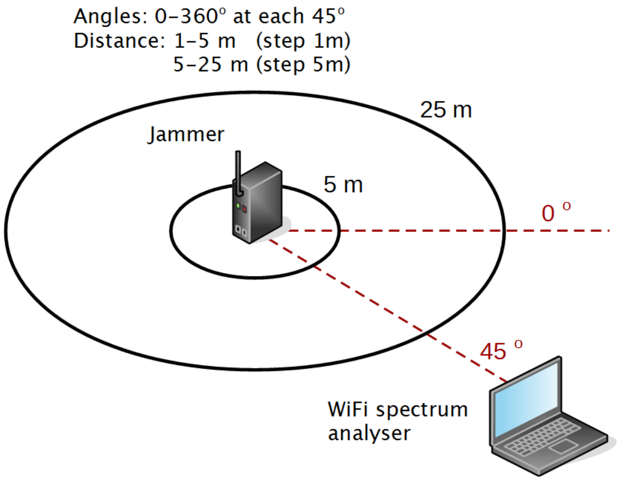

Fig. 2. Idea of the measurements.

3.1 Measurements description

The jammer was placed in the open grassy terrain and the level of the signal power was registered with the use of the Wi-Fi spectrum analyser. The measurements were performed at angles 0–360o with the step 45o and at the 1–25-metre distance (1–5 m step 1 m and 5–25 m step 5 m). Jammers and RF spectrum analyser were placed on the wooden stands 62 cm above the ground level. The devices used during measurements were as follows:

- jammers specified in Table 1,
- RF analyser and data logger - AirMagnet Spectrum XT Fluke [28],
- laptop with AirMagnet Wi-Fi Analyser software.

Measurements were carried out in the Wi-Fi 2.4 GHz wireless ISM (industrial, scientific and medical) band. In the beginning, the background noise was measured with the Fluke XT analyser and its value was in range -110 dBm to -105 dBm. At each measurement point, 100 measurements were recorded. The registered frequency range was 2.402 – 2.493875 GHz with 156 kHz step. The stationary jammer has the ability to set the power fluently. The output power of this jammer was set to produce the signal whose power was equal to the power of the handheld jammer. The values in each measurement point (72 total points with 100 measurements in each) were averaged with the use of median.

In this work authors decided to show the modelling and measurement results for not overlapping channels of the Wi-Fi band *i.e.*: 1 (2.401 – 2.423 GHz), 6 (2.426 – 2.448 GHz), 11 (2.451 – 2.473 GHz). For handheld CRJ4000 jammer the results of measurements are shown in Figure 3, and for stationary CKJ-1502A12 jammer in Figure 4.

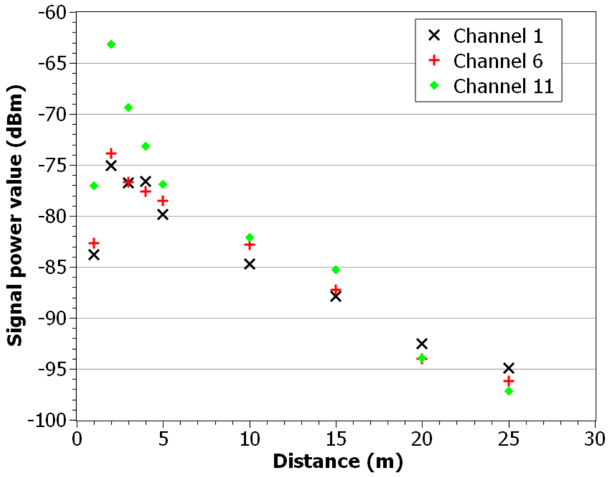

Fig. 3. Results of measurements of handheld CRJ4000 jammer.

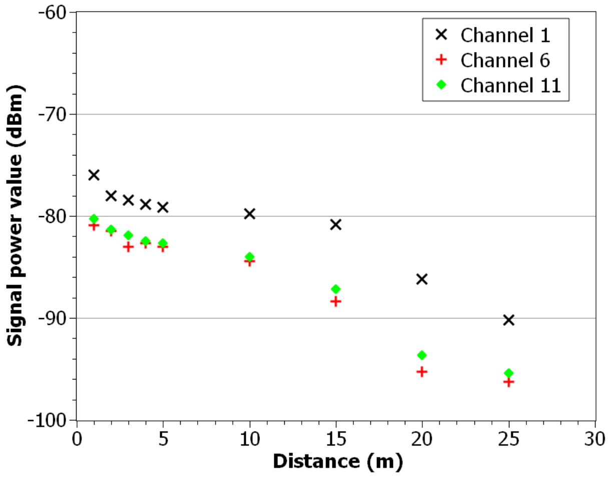

Fig. 4. Results of measurements of stationary CKJ-1502A12 jammer.

It can be noticed that for both jammers the value of signal power differs for different channels. In the case of handheld jammer (Fig. 3), the highest values are recorded for channel 11. For stationary jammer (Fig. 4) the highest values were recorded for channel 1.

3.2 Modelling with the use of log-normal model

Based on measurements of the signal power distribution model with the use of equations described in (1) and (2) model was made.

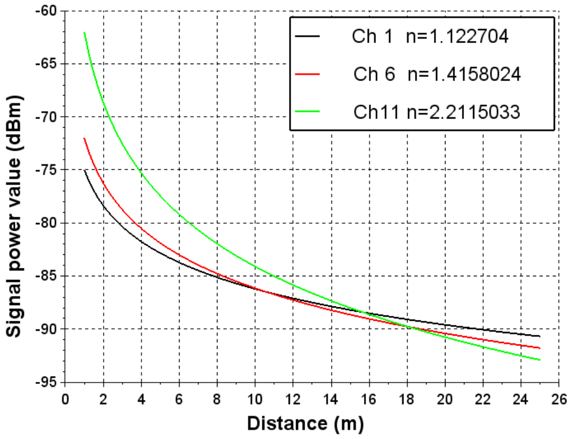

Fig. 5. Results of modelling with the use of the log-normal model for CRJ4000 jammer (based on the measurements).

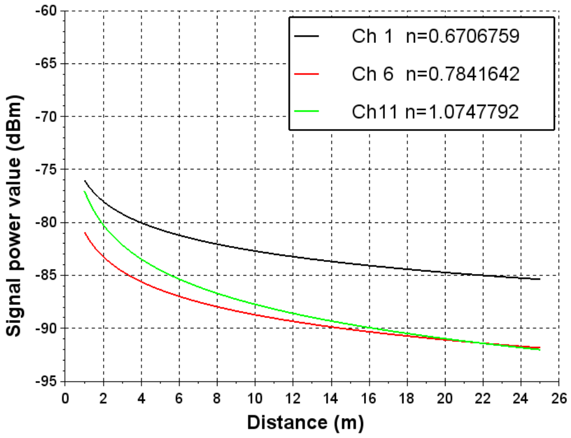

Fig. 6. Results of modelling with the use of the log-normal model for stationary CKJ-1502A12 jammer (based on the measurements).

The results of path loss classical log-distance model for handheld and stationary jammers were presented in Figures 5 and 6 accordingly. It can be noticed that for the handheld jammer (Fig. 5), there are big disparities (even up to 15 dBm) in the signal power between channel 1 and 11. One can also notice that path loss exponent value also changes in the wide range from about 1.123 to 2.212 (the difference is equal to 1.089).

The stationary jammer is much more consistent (Fig. 6). The values of the signal power differ by approx. 7 dBm, which is much less, compared to the handheld jammer. Path loss exponent value changes from about 0.671 to 1.075 (the difference is equal to 0.404).

It can be noticed that stationary jammer is much more efficient and jamming signal exhibits higher uniformity in the wide-range distance. In the distance from 2 meters to 16 metres, the signal power varies from -90 dBm to -77 dBm (Fig. 6). However, the handheld jammer (Fig. 5) is more efficient at shorter distances *i.e.* from 2 to 14 meters. Notwithstanding the jamming signal of that device decreases with the distance much faster comparing to the stationary one.

Comparing results of the models derived from measurement results (Fig. 5 and Fig. 6) and models based on the manufacturer data (Fig. 1) it can be noticed that there is a significant discrepancy between the signal power values. One should keep in mind that in UE, according to ETSI standard, the maximum EIRP power limits for the 2.4 GHz band is 100 mW (20 dBm). It looks like both devices follow that regulation and therefore in the values from measurements are much lower.

3.3 Modelling with the use of the two-ray ground-reflection model

The second applied model was the two-ray ground-reflection one - described in equation (2). The results of modelling for the handheld and the stationary jammers are presented in Figures 7 and 8 accordingly. Measurement points were marked with symbols.

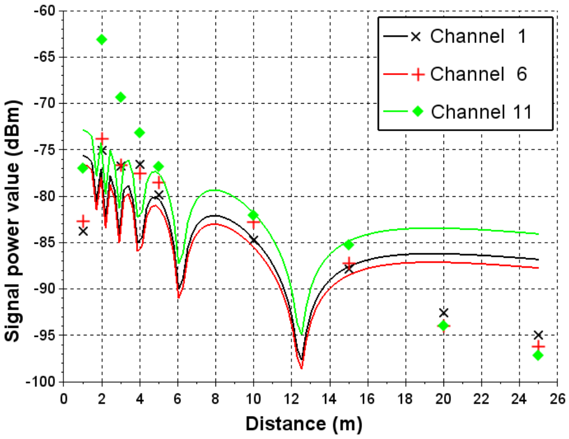

Fig. 7. Results of modelling with the use of the ground reflection model for CRJ4000 jammer (based on the measurements).

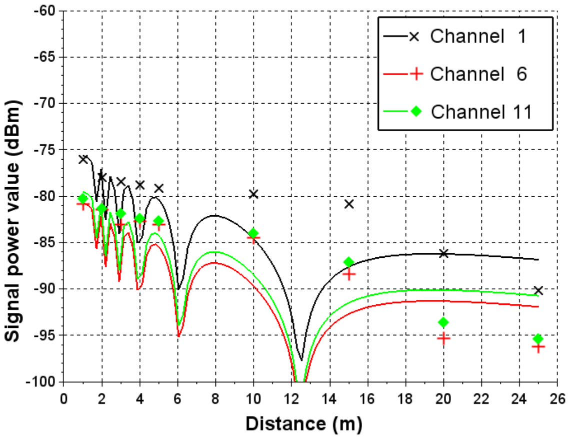

Fig. 8. Results of modelling with the use of the ground reflection model for stationary CKJ-1502A12 jammer (based on the measurements).

It seems that this model gives more condensed values of signal power. In both cases, the maximum differences obtained between channels amounted to approx. 6-7 dBm. Worth noticing is the fact that the model gives good results in short ranges *i.e.* up to 10 meters, and the worst results above that range in comparison with the log-normal model.

In the case of the handheld jammer (Fig. 7), it was difficult to fit the model to the starting values (1-3 meters distance) in channel 11. This could be caused by the jammer design and non-uniform omnidirectional antennas.

The stationary jammer signal power models fit better with the measurements (Fig. 8). It can be noticed that more suitable fitting appeared at the distance of 1-5 meters. This could be due to the length of antennas and placement of the jammer at the desired distance above the ground.

3.4 Models comparison

To compare differences between both models the average values for all channels at each distance measurement point were calculated. These values provided the input data for both models. The results of the modelling for the handheld and the stationary jammers were presented in Figures 9 and 10 accordingly.

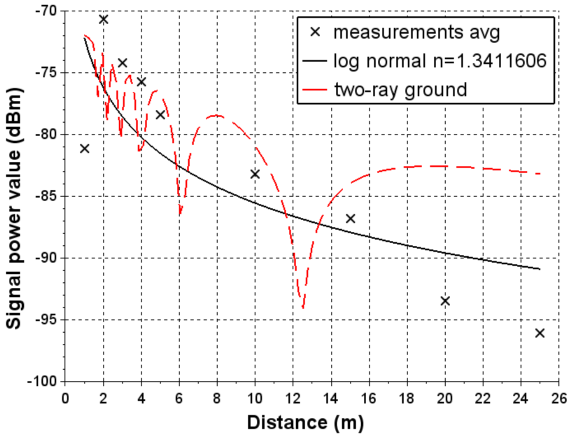

Fig. 9. Results of both models with the use averaged measurement values for CRJ4000 jammer.

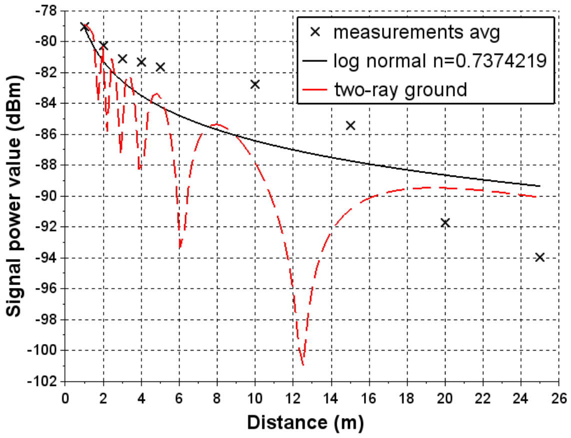

Fig. 10. Results of both models with the use averaged measurement values for stationary CKJ-1502A12 jammer.

In the case of CRJ4000 jammer (Fig. 9) both models differ much at longer distances, while in the case of CKJ-1502A12 jammer, the results obtained from both models are similar (Fig. 10). It is worth noticing that the path loss exponent in the case of the stationary jammer is almost half the value of that obtained in the case of the handheld one. This means that the signal power values versus distance do not drop so fast as in the case of the higher values of the path loss exponent.

4 Conclusions and future works

The article presented the results of modelling based on the measurement results of the signal power generated by jammers in the Wi-Fi ISM band. Based on the results it can be noticed that the jammers work differently for different channels of the Wi-Fi band. The handheld jammer is more efficient in channel 11 while the stationary one in channel 1.

The shielding radius given by the manufacturers of the jammers does not match the measurements results. In case of CRJ4000 model, the shielding radius is about 10 m (signal power -75 to -85 dBm in Fig. 9); the stationary model, CKJ-1502A12, has better shielding radius amounting to approx. 15 m (Fig. 10).

The results obtained from modelling show a reasonably good fit with the measurements. It is noticeable that two-ray ground-reflection model is better at shorter distances, while the log distance one alt longer.

The important issue is that the jammers do not have the same ability for generating the jamming signals over the entire Wi-Fi ISM band. In the future, the authors plan to extend the measurements with emphasis on the differences in the power level in different channels and construction of relevant models, which will exhibit better fit with the real results.

References

1. T.S. Rappaport, J.N. Murdock, D.G. Michelson, and R. Shapiro, IEEE Veh. Technol. Mag., 24-32 (2011)
2. C. Phillips, D. Sicker, D. Grunwald,. IEEE Commun. Surveys Tuts., **15(1)**, 255-270 (2013)
3. T. Chrysikos, S. Kotsopoulos, *Proceedings of the International MultiConference of Engineers and Computer Scientists 2013*, **II**, (2013)
4. M. Mackowski, A. Kwiecien, M. Kojder, M. Manczyk , *Proceedings of the 22nd International Conference on Computer Networks (CN) 2015*, ISBN: 978-3-3191-9419-6, 444-454 (2015)
5. D.E. Grzechca, P. Pelczar, L. Chruszczyk, Int. J. Electron. Telecommun., **62(4)**, 371-378 (2016)
6. K. Budniak, K. Tokarz, D. Grzechca, *Proceedings Man–Machine Interactions 4 Springer, Cham.*, 487-498 (2016).
7. T.V. Haute, E.D. Poorter, I. Moerman, F. Lemic, V. Handziski, A. Wolisz, T. Voigt, Int. J. Ad Hoc Ubiq. Co., **23(1-2)**, 92-114 (2016)

8. K. Pelechrinis, I. Koutsopoulos, I. Broustis, S.V. Krishnamurthy, Comput. Commun., **86**, 75-85 (2016)
9. T. Wang, X. Wei, J. Fan, T. Liang, Comput. Netw., **141**, 17-30 (2018)
10. S. Shue, L.E. Johnson, J.M. Conrad, *IEEE SoutheastCon*, 1-6 (2017).
11. D. Czerwinski, S. Przylucki, P. Wojcicki, J. Sitkiewicz, *Proceedings of International Conference on Computer Networks (CN) 2017*, 106-117 (2017)
12. D. Wang, L. Song, X. Kong, Z. Zhang, Int. J. Distib. Sens. N., **8**, 1-10 (2012).
13. T. Thewan, A.H. Ismail, M. Panya, K. Terashima, *Preceedings of the IEEE 19th International Conference on Information Fusion (FUSION),* 855-860 (2016)
14. R.W. Heath, N. Gonzalez-Prelcic, S. Rangan, W. Roh, A.M. Sayeed, IEEE J. Sel. Topics Signal Process., **10**, 436-453 (2016)
15. D. Balachander, T.R. Rao, G. Mahesh, *Proceeding of IEEE Conference on Information & Communication Technologies (ICT)*, 755-759 (2013)
16. A.I. Sulyman, A.T. Nassar, M.K. Samimi, G.R. MacCartney, T.S. Rappaport, A. Alsanie, IEEE Commun. Mag., **52(9)**, 78-86 (2014)
17. A. Alsayyari, I. Kostanic, C. E. Otero, *Proceedings of IEEE 16th Annual Wireless and Microwave Technology Conference (WAMICON)*, 1–6 (2015)
18. O. Olasupo, C. E. Otero, K. O. Olasupo, I. Kostanic, IEEE Trans. Antennas Propag., **64**, 4012–4021 (2016)
19. T. Li P. Cheng, S. Zhu, D. Torrieri, Integr. Comput-Aid E., **21**(1), 19-34 (2014)
20. P.M. Santos, T.E. Abrudan, A.Aguiar, J.Barros, IEEE Trans. Wireless Commun., **13**, 2353–2361 (2014)
21. S. Tomic, M. Beko, R. Dinis, IEEE Trans. Veh. Technol., **64(5)**, 2037-2050 (2015)
22. S. Sun, T.S. Rappaport, T. A. Thomas, A. Ghosh, H.C. Nguyen, I.Z. Kovács, A. Partyka, IEEE Trans. Veh. Technol., **65(5)**, 2843-2860 (2016)
23. C. Sommer, F. Dressler, *Proc. ACM MobiCom*, 1–3 (2011)
24. W. Khawaja, I. Guvenc, D. Matolak, U.C. Fiebig, N. Schneckenberger, arXiv preprint arXiv:1801.01656, (2018)
25. Ecer - cell mobile phone jammer company, Cell phone and Wifi jammer [CRJ4000] parameters, http://www.ecer.com/products/cell_phone_and_wifi_jammer_crj4000-mpz234a62a-z1fcb0dd/showimage.html, (Dec 2016)
26. CKJ-1502A12 Jammer, ChingKong Technology, http://www.szckt.com/ckj-1502a12-p00079p1.html, (Dec 2016)
27. M. Hillbun, Practical Antennas, www.diamondeng.net/library/AntennaMeasurement.pdf, (Apr 2012)
28. Fluke Networks, Air Magnet Spectrum XT analyser datasheet, http://airmagnet.flukenetworks.com/assets/datasheets/AirMagnet_SpectrumXT_Datasheet.pdf, (Dec 2017)…