www.czasopisma.pan.pl PAN www.journals.pan.pl
jet INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2019, VOL. 65, NO. 1, PP. 65–70
Manuscript received August 14, 2018; revised January, 2019. DOI: 10.24425/ijet.2019.126284

Study of the GNSS Jamming in Real Environment

Tomáš Morong, Pavel Puričer, Pavel Kovář

***Abstract*—GNSS systems are susceptible to radio interference despite then operating in a spread spectrum. The commerce jammers power up to 2 watts that can block the receiver function at a distance of up to 15 kilometers in free space.**

Two original methods for GNSS receiver testing were developed. The first method is based on the usage of a GNSS simulator for generation of the satellite signals and a vector signal RF generator for generating different types of interference signals. The second software radio method is based on a software GNSS simulator and a signal processing in Matlab. The receivers were tested for narrowband CW interference, FM modulated signal and chirp jamming signals and scenarios. The signal to noise ratio usually drops down to 27 dBc-Hz while the jamming to signal ratio is different for different types of interference. The chirp signal is very effective.

The jammer signal is well propagated in free space while in the real mobile urban and suburban environment it is usually strongly attenuated.

***Keywords*—GNSS, GPS, jamming, test method, signal propagation, interference immunity**

I. Introduction

GNSS has become the primary navigation system and currently, more and more applications are dependent on it. GNSS signal jamming by various jammers or by other electronics systems cause a lot of problems and difficulty in the transport systems [1]–[3] and it is one of the main factors that limit the applicability of GNSS in safety-critical applications like GNSS toll systems, civil and general aviation, intelligent transports and smart cities etc. Many studies concerning GNSS receiver behaviour under jamming have been presented in [4]–[6]. GNSS jamming signals are classified in [7]. Chirp or FM jammers that are featured with very high jamming effectivity despite their simplicity and extremely low manufacture cost are very popular.

GNSS jammers are widely used for overcoming the electronics systems of trucks [1] and other vehicles to make it impossible to control the surveillance of the route and driving safety rules etc. These jammers are installed in the track cabs or on other places on the Earth surface. The jammed receiver antennas are also located in truck or car roofs or under windshields, or they are antennas of mobile receivers.

Most of the available jammers have a wider bandwidth the civil signal L1 whose carrier frequency is 1575,42 MHz and has null-to-null bandwidth of a spread spectrum is approximately 2 MHz.

This research was supported by Open Program Research Development Education, MEYS, under the project "CRREAT", "Reg. No. $CZ.02.1.01/0.0/0.0/15_0 03/0000481$" and by the grant VI2VS/439 of the Ministry of Interior of the Czech Republic.

T. Morong, P. Puričer, P. Kovář are with the Department of Radio Engineering, Faculty of Electrical Engineering: CTU, Prague, Czech Republic (e-mail: morontom, puricep, kovar @fel.cvut.cz).

The power level of the jamming signal must be relatively high [7] to stop the operation of the mobile GNSS receiver as the signal is attenuated by the propagation near the Earth surface and blockage by various obstacles. The effect on the receivers in the air (aircraft or drone) is much bigger because of the free space propagation. As the jammers use brute force method by a simple chirp signal to jam the receiver, the distortion of the jammer signal by its propagation like time-delay spreading or frequency spreading is not important. Only signal level or jamming to useful signal ration (J/S) is important [8].

Our intention is to develop a methodology for predicting the jammer effect for various situations and scenarios. The user can use this data for development of the countermeasure that can be based on protection of some critical areas, technical improvement of the GNSS receivers or other technical or organization provisions.

The investigation of the GNSS jamming can be divided into two problems, the investigation of the jamming signal propagation and assessment of GNSS jamming immunity.

We investigated jammer signal propagation, especially signal level for various typical scenarios like an urban, suburban, rural area or in the air.

The theoretical determination of the accepted interference level for GNSS receivers is very complicated because of an absence of the details of the implementation of the signal processing inside the receiver. The usable method is to measure it and for this reason, the two methods for testing receivers were developed.

The paper is organized as follow, firstly we classify the GNSS interference signals and signal propagation models suitable for mobile receivers or receivers in the air are presented. Secondly, the test methods of the GNSS receiver interference immunity are described.

Thirdly the description of the experimental setup for verification of the signal propagation is introduced, then follows the presentation of the experimental data and conclusions.

II. GNSS Interference

GNSS interference can be classified according to many aspects, for instance, according to the source into artificial or natural. The main natural source of GNSS interference is the Sun. During strong Sun radio bursts, the function of many radio end electronic systems could be degraded or even disabled [8]. Fortunately, the occurrence of strong Sun radio bursts is very seldom.

The artificial interference can be further classified onto the intentional or unintentional. The unintentional interference is produced by human industrial, transport, telecommunication or other systems. Those systems transmit their signals on frequencies close to bands of GNSS.

The intentional interference can be further classified onto jamming, and spoofing [9]. The jamming is usually a simple interference signal of an appropriate level that makes it difficult or impossible to process GNSS signal. There are a few types of possible jamming signals. For example, narrowband noise, broadband noise, tones and pulse etc. [7]

Spoofing is a false signal or signals for confusing the GNSS receiver. The intention is to force GNSS receivers to interpret the spoofing signal as an authentic one.

The generation of spoofing is currently very complicated from a technical point of view, but in the future, the required technology will be much cheaper and more accessible thanks to the software radio.

GNSS systems use Direct Sequence Spread spectrum technique that is featured with the interference immunity. Non-correlated interference is attenuated of processing gain

$$G_p = \frac{B_s}{B_b} \tag{1}$$

where B_s is bandwidth if the spread signal by the so-called ranging code and B_b of the primary modulated signal by navigation message. The maximum processing gain of GPS L1 C/A signal is approximately 43 dB. The real processing gain depends on the signal processing in the receiver, mainly on coherent integration time [10] and reaches up to 30 dB at a standard GPS receiver.

The question is what is the minimal power of GNSS jammer to be able to emit critical level in given environment. The problem is reduced to study the link budget or path loss PL of the radio channel from Jammer to the GNSS receiver [12].

III. Propagation models

The path loss is expressed

$$PL[dB] = 10log\frac{P_t}{P_r} \tag{2}$$

where P_t and P_r are transmitted and received power. In free space for a distance between transmitter and receiver antenna d, the received power in antenna far-field is expressed

$$P_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 L} \tag{3}$$

where G_t and G_r are the gain of the transmitter and receiver antennas, λ is wavelength and L represents system loss, that does not relate with signal propagation. In practical situations, the path loss expresses as the path loss in reference distanced d_0, free space loss form distance d_0 to d [12].

$$PL_d = PL(d_0) + 10\gamma log(d/d_0) + X_\sigma \tag{4}$$

The factor γ represents propagation factor that depends on environment and X_σ is a random zero-mean Gaussian variable of standard deviation σ that reflects the variation of path loss. The propagation factor for free space is 2, 2.8 ÷ 3 for typical outdoor environment, 4 for wet soil and 4 ÷ 6 for indoor environment [13].

The propagation of the radio signal in real environment is effected by reflection, diffraction, scattering and attenuation on various obstacles like buildings, vegetation, Earth surface etc. The propagation is then very complicated.

The most common empirical or statistical model of path loss for outdoor are

- Okumura-Hata Model
- COST Hata model

A. Okumura-Hata model

The median path loss is given

$$L_{50\%}[dB] = L_{FSL} + A_{MU} - H_{MG} - H_{BG} - \sum K_{Corr} \tag{5}$$

where L_{FSL} is a free space attenuation, A_{MU} is a median of additional attenuation, H_{MG} and H_{BG} are mobile and ground stations antenna high factors, and finally K_{Corr} are correction factors gains. All variables are in dB. The correction factors of the model were obtained by the measurements [15]. The range of model validity is: frequency 150 ÷ 1500 MHz, effective ground station antenna high 30 ÷ 200 m, effective mobile station antenna high 1 ÷10 m and distance 1 ÷ 20 km.

The model was then upgraded and extended for frequencies 1150 ÷ 2000 MHz and modified by Okumura.

B. Other models

The COST 231WalfishIkegami Model is an path model for modelling Line of Sights and Non Line of Sights propagation in short distance [16].

For indoor propagation the ITU-R model was developed. The path loss in indoor area is expressed

$$PL(d) = 37 + 30log(d) + 18.3N_{floor}^{\left(\frac{N_{floor}+2}{N_{floor}+1} - 0.48\right)} \tag{6}$$

where N_{floor} is a a number of floors between transmitter and receiver and d is a bistance.

For outdoor the path loss is

$$PL(d) = 40log(d) + 30log(f_c) + 49 \tag{7}$$

IV. Assessment of GNSS Jamming Immunity

Based on [11] we developed two test methods which are suitable for the quality assurance of GNSS receivers. The basic essence of the designed methods is to create a testing signal which can be used as a reliable test of GNSS receivers. Furthermore it is an important creation of a unique method needed to evaluate a behavior of the receiver. This process is based on the processing of NMEA data provided by the receiver.

The goal of the test methods is to find out the threshold value of J/S for which the GNSS receiver is not able to determine its position. This value is determined from the NMEA output of the receiver and we called it a critical value. We analyze an indicated signal to noise ratio C/No. The C/No is accurately described as the carrier wave power to noise power density ratio. The C/No gives a good measure of the Spectral power density of a received signal.

The reason why two different test methods were used is the possibility to compare measured results. The methods are described in the next paragraphs along with obtained results.

A. *Classical method*

This method is based on a combination of the signal of a GPS jammer with a GPS generator. The signal from the GPS jammer is attenuated to the required level by a step attenuator. The combined signal is imputed by coaxial cable to the input connector of the receiver. A block diagram of this method is shown in Figure 1.

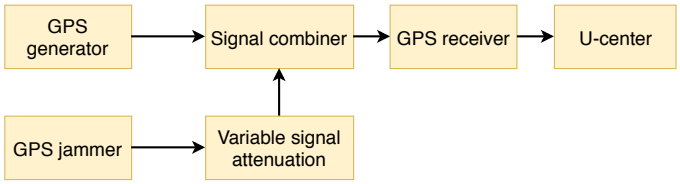

Fig. 1. Block diagram of a testing procedure in the classical method

We are able to gain the value J/S through this method and an effective range of individual jammers as well.

B. *Software radio method*

The software radio method is based on the generation of the test signal by software and replay of this signal by a software radio. The adding of the interference signal is done due to Matlab. This method is more effective than the classical method. The main advantages are:

- The low cost of a software GNSS simulator
- The repeatability of measurement
- Usage any interference signal

The setup of the software method is shown in Fifure 2.

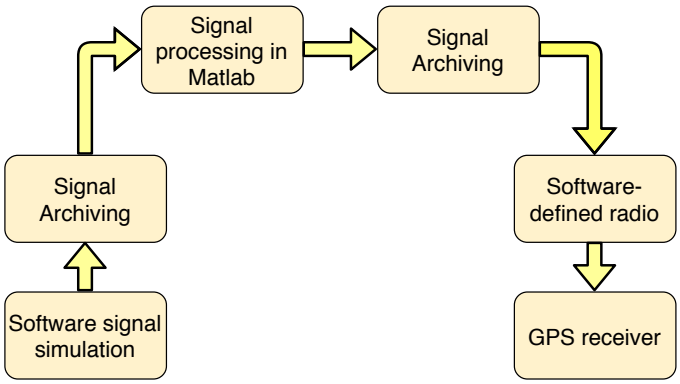

Fig. 2. The setup of the software method

At first, we generated a GPS signal via a software GNSS simulator. The software enables to set up the simulation parameters and trajectory of satellites. The output is in a binary file form and we used one-hour signal duration. The adding of the interference signal was done in Matlab. In our case, the GPS signal was jammed by several different types of signals. For simplification of the receiver testing, we divided the signal into time segments in which the J/S was constant. The jamming intensity was gradually increased. The resulting signal is stored on disk. We used a software-defined radio for replaying the test signal. The output of the SDR was directly connected to the input connector of the GPS receiver.

V. Investigation of Jamming Signal Propagation

As we evolve the methodology for predicting jammer effect in various situations the study of the propagation of the jammer signal is a building block for us. To begin with, we have made a simple measurement based on transmitting and a receiving signal that is close to the jamming signal.

For experimental measurement an amateur radio frequency 0.23 meters has been used. This band is allocated in the middle of the lower and upper GNSS bends. Power Level is low to avoid jamming of primary radio services around. The attenuation of the signal is very similar to the attenuation of GNSS signals.

The test signal is generated by a tiny RF generator based on the ADF 4361 chip to be able to use a drone for carrying it.

Before each measurement, the system was calibrated to obtain path loss in reference distance 10 meters.

Basically, the power level of a peak of the receiving signal has been measured. The test receiver antenna has been placed to the height 1.5 meters above ground in a specific position. The position of the RF generator was changed in distance and height.

Our measurements were performed during clear sky to not have to assume atmospheric attenuation.

Fig. 3. Illustration of measurement

VI. Results of Interference Immunity of the GNSS Receiver

This section presents tests results of two U-blox GNSS receivers, EVK-6H and EVK-M8T. Tested receivers are used in a wide range of mass market and industrial systems including drones. The receiver manufacturer provides a U-center software that enables analysis of the receiver measurement and saves data for further processing. The software simplifies the measurement processing and receiver performance determination. The following paragraph present test results for the typical jamming signal as a chirp signal. The receiver operation is investigated as an indicated signal to noise ration C/No as a function of the J/S value.

A. *Critical value of J/S*

The chirp jamming wave in a classical signal was generated by a real jammer TG-5CA that is ilustrated in Figure 4. The jamming signal power level is 32 dBm and the bandwidth of the signal is 18.5 MHz.

Fig. 4. Jammer TG-5CA

In software method, the chirp signal of bandwidth 6 MHz was generated as the used SDR is featured with bandwidth is only 8 MHz. The results are shown in graphs and Table I. The results of the classical method are shown in Figure 5 whereas the software method in Figure 6.

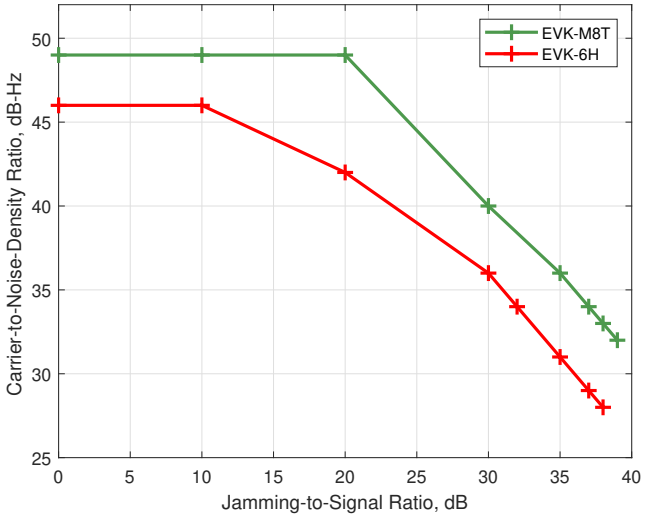

Fig. 5. Classical method Jamming: chirp signal from the jammer TG-5CA

TABLE I
RESULTS OF TEST METHODS

	Classical method		Software radio method	
Receiver	C/No [dB-Hz]	Critical J/S [dB]	C/No [dB-Hz]	Critical J/S [dB]
EVK-6H	28	38	32	37
EVK-M8T	32	39	30	39

The result of those methods is a knowledge that the receiver is able to process narrow-band interference of J/S 50 dB, the signal to noise ratio drops down to 27 dBc-Hz. The immunity to the wide interference is approximately 10 dB lower.

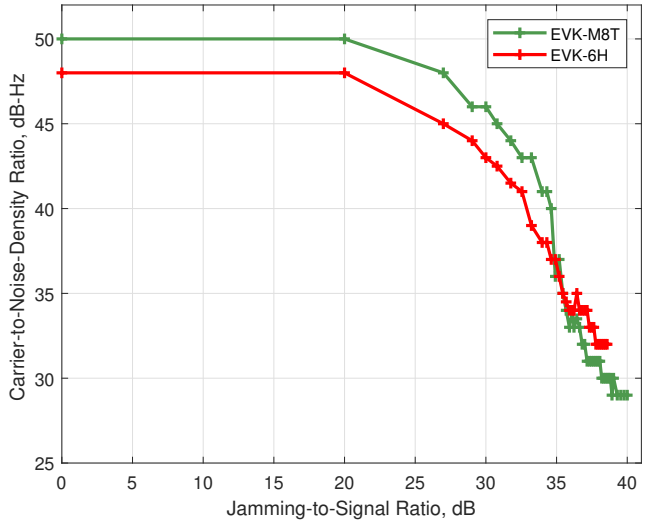

Fig. 6. Software method Jamming: chirp signal

B. *Effective range of Jammer*

The key parameter of the jammer or GNSS receiver used is an effective range. The effective range is a range in which the jammer can evoke the signal of critical power level or higher. For determination of the critical range, we consider ideal (free space) jammer signal propagation without the impact of the Earth surface and other obstacles that can block or attenuate jammer signal. The effective range was calculated based on the formula 3 as the jammer operation is illegal. The standard power level -158.5 dBW of GPS signal on an ideal hemispheric antenna of gain 3 dB was considered [21]. The jammer effective range for interference signal power 32 dBm is in Table II.

TABLE II
RESULTS - EFFECTIVE RANGE OF JAMMER

Receiver	Max Effective Range [km]
EVK-6H	16
EVK-M8T	14

VII. RESULTS OF JAMMING SIGNAL PROPAGATION

Our measurement took place in four different environments as urban, suburban, rural and vegetation. All results are shown in tables below. The value of the power level of the peak of the receiving signal is label as P_r in dB.

The position of the RF generator was being changed manually in all environments except in rural. In that case, the position was being changed by a drone to reach higher altitude.

Based on formula 3 for free space the value of power level decreases by 6 dB if the distance between the transmitter and receiver enlarges two times. This corresponds to the theoretical value of $\gamma = 2$.

In the real environment, the value of the power lever decreases more. This corresponds with the higher value of the propagation factor γ.

In our case the propagation factor γ has been estimated as a slope of linear regression of path losses that were measured.

A. Propagation in forest

Two parts of results are presented within this measurement. Both of them come from a forest but one is from a footpath and the second one is from impermeable vegetation. The results are shown in tables III and IV.

TABLE III
FOOTPATH

Height of Tx [m]	**0**	**1.5**	**4**
Distance [m]	P_r [dB]		
10	-18	-4.2	-1.5
20	-23	-12	-6.3
30	-30	-22	-14.5
γ	**2.4**	**3.6**	**2.6**

TABLE IV
FOREST

Height of Tx [m]	**0**	**1.5**	**4**
Distance [m]	P_r [dB]		
10	-8.2	-3.8	-12
20	-20	-18	-11
30	-30.5	-18.5	-25.5
γ	**4.6**	**3.3**	**2.5**

B. Propagation above grass in rural environment

TABLE V
RURAL ENVIRONMENT

Height of Tx [m]	**1.5**	**5**	**10**	**15**	**20**
Distance [m]	P_r [dB]				
20	-11	-15	-21	-17	-33
30	-15.5	-19	-17	-19	-23
50	-21	-24	-34.5	x	x
γ	**2.5**	**2.3**	**3.6**	x	x

C. Propagation in urban environment

The RF generator was placed in different places in the urban environment. Some potential positions of the source of jamming were simulated. Some positions of the RF generator were behind buildings some were not. Results from this part of the measurement are shown in Table VI.

Figures 8 and 7 show the selected positions of the RF generator in the urban environment.

TABLE VI
PROPAGATION ABOVE ASPHALT IN SUBURBAN ENVIRONMENT

Height of Tx [m]	**0**	**1.5**
Distance [m]	P_r [dB]	
18	-18	-21
21	-35	-19
34	-35	-22
38	-36	-36
44	-36	-33
45	-43	-37
58	-35	-35
72	-43	-33
76	-37	-18
78	-42	-42
79	-34	-34
92	-37	-37
106	-41	-41
107	-44	-43
133	-35	-35

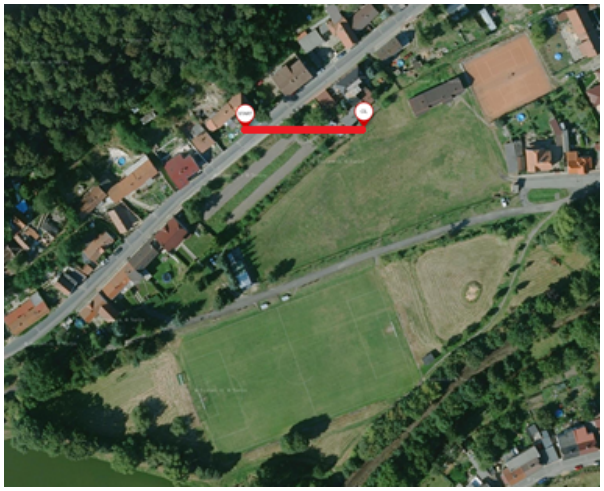

Fig. 7. Distance between RF generator and receiver 58 m

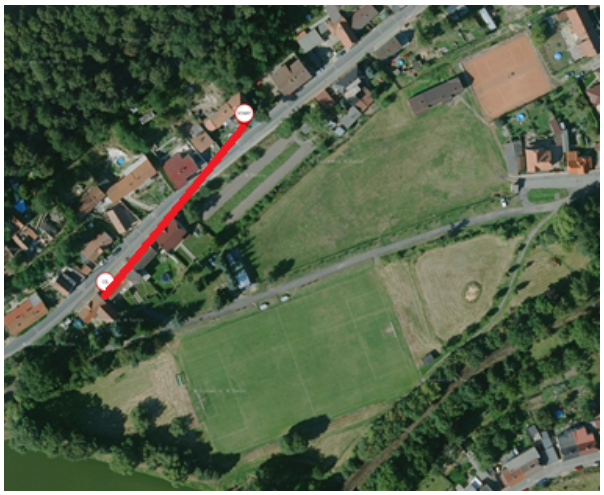

Fig. 8. Distance between RF generator and receiver 106 m

D. Propagation above concrete in suburban environment

TABLE VII
SUBURBAN ENVIRONMENT

Height of Tx [m]	**0**	**1.5**
Distance [m]	P_r [dB]	
10	-6.7	-0.5
20	-23.5	-5.5
30	-31.3	-8.4
40	-29.5	-12.2
50	-32.5	-15.5
60	-36.8	-18.2
γ	**3.6**	**2.2**

VIII. DISCUSSION

Based on the results of both test methods the threshold value J/S is almost the same. The bandwidth of the jamming signal must be wider than 2 MHz to effectively jam GPS L1 signal.

The wideband jamming signals seem to be more effective than the narrowband ones because the narrowband interference can be effectively suppressed by the adaptive notch filter while the wideband ones cannot. This is why the bandwidth of the efficient jamming signal should be wider than 2 MHz for GPS L1 frequency.

Carrier-to-Noise-Density Ratio measured by both receivers are different. The receiver EVK-M8T has always the higher value of C/No. It might be caused by different algorithmics of signal processing.

The important result in case of the jamming signal propagation is the propagation factor γ. This value has been higher than the theoretical value $\gamma = 2$ in all environments. The worst propagation of the signal is in vegetation where $\gamma = 4.6$.

IX. CONCLUSION

We present two methods for testing the interference immunity of the civil GNSS receivers. The advantage of the classical method is the possibility to use a real jammer. The second software method is based on an application of software radio. The method is featured by a high flexibility and repeatability. Both methods were used for practical testing of two GPS receivers. The obtained results are in good conformity.

The minimal values of C/No have been from 28 dB-Hz to 32 dB-Hz for chirp jammer.

The experiments proved the theoretical assumptions that the GNSS jammer signal is propagated very well in free space while the propagation in real indoor and outdoor environment is much worse and that is the problem. As the jammer users usually jam the mobile receivers they are inclined to use high power jammers that are featured with long range in free space. The GNSS jammers are then very dangerous for aircraft or UAV, especially in low heights.

REFERENCES

[1] S. Pullen and G. X. Gao, GNSS jamming in the name of privacy: Potential threat to GPS aviation, Inside GNSS, Mar./Apr. 2012.
[2] GPS jammingOut of sight, Economist, Jul. 27 2013. [Online]. Available: http://www.economist.com/printedition/ 2013-07-27
[3] A Grant, P. Williams, N. Ward, S. Basker, GPS Jamming and the Impact on Maritime Navigation, Journal of Navigation, April 2009.
[4] G. X. Gao, AU - M. Sgammini, AU - M. Lu, AU - N. Kubo, Protecting GNSS Receivers From Jamming and Interference, Proceedings of the IEEE, pp. 1327 - 1338, 2016.
[5] D. Borio, Swept GNSS jamming mitigation through pulse blanking, ENC pp. 1 8, 2016.
[6] Y. Hu, S. Bian, B. Li, L. Zhou, A Novel Array-Based Spoofing and Jamming Suppression Method for GNSS Receiver, IEEE Sensors Journal, Vol. 18, No. 7, April 1, 2018.
[7] R. H. Mitch, R. C. Dougherty, M. L. Psiaki, S. P. Powell, and B. W. OHanlon, Signal Characteristics of Civil GPS Jammers, ION GNSS, pp 1907 1919, 2011.
[8] S. Fang, Y. S. Yang, The Impact of Weather Condition on Radio-Based Distance Estimation: A Case Study in GSM Networks With Mobile Measurements, IEEE Trans. on Veh. Tech, Vol. 65, No. 8, 2016.
[9] M. L. Psiaki, T. E. Humphreys, GNSS Spoofing and Detection Proceedings of the IEEE, pp. 1327 - 1258, 1270.
[10] G. Arul Elango, G.F. Sudha, Bastin Francis, Weak signal acquisition enhancement in software GPS receivers Pre-filtering combined post-correlation detection approach, Applied Computing and Informatics, Vol. 13, Iss. 1, pp 66-78, 2017.
[11] Ryan, H, et al.,Know Your Enemy: Signal Characteristics of Civil GPS Jammers, GPS world, no. 1, p. 8, 2012.
[12] T. K. Sarkar, Z. Ji, K. Kim, A. Medouri, M. Salazar-Palma, A survey of various propagation models for mobile communication, IEEE Ant. and Propag. Mag. June 2003.
[13] RF Range Calculator,https://www.silabs.com/community/wireless/proprietary/knowledge-base.entry.html/2017/05/02/rf_range_calculator-SYIA.
[14] T. S. Rappaport, Wireless Communications: Principles & Practice, Upper Saddle River, NJ, Prentice Hall PTR, 1996.
[15] M. Hata, Empirical formula for propagation loss in land mobile radio services, IEEE Trans. Veh. Technol., vol. VT-29, pp. 317325, Aug. 1980.
[16] J.Walfisch and H.L. Bertoni, A Theoretical model of UHF propagation in urban environments, IEEE Trans. Antennas Propagat., vol.36, 1988, pp.1788-1796
[17] M. D'Souza, B. Schoots, M. Ros, Indoor position tracking using received signal strength-based fingerprint context aware partitioning, IET Radar Sonar Navig., Vol. 10 Iss. 8, pp. 1347-1355, 2016.
[18] A. Bose, Ch. Foh, A Practical Path Loss Model For Indoor WiFi Positioning Enhancement, ICICS 2007.
[19] J. He, E. P. Li, S. Zhou, K, Liao, Experimental Characterization of Radio Channel in Ruins Environment, IEEE Ant. end Wireless Prop. Letters, VOL. 15, 2016
[20] I. Joo, C. Sin. GNSS Jamming Propagation Prediction Simulator Based on ITU-R P.1546 Model, ICCAS, pp. 1002 1006, 2016.
[21] E. D. Kaplan, Understanding GPS: principles and applications, 1st ed. Boston: Artech House, c1996.