ATLANTIS PRESS

Advances in Intelligent Systems Research, volume 166

7th Scientific Conference on Information Technologies for Intelligent Decision Making Support (ITIDS 2019)

Improved Method for Estimating Noise Immunity of Global Navigation Satellite Systems

Aleksandr Zhuk
North-Caucasus Federal University
Stavropol, Russia
alekszhuk@mail.ru

Dmitrii Orel
North-Caucasus Federal University
Stavropol, Russia
kde.def@gmail.com

***Abstract*—The task of wireless data transmission system in electronic conflict is to ensure the secrecy of signal parameters to provide the availability of radio signal in conditions of interference. The task of interference transmitter is to suppress the radio channel with interference. Interference transmitter must explore the parameters of the radio signal to form interference which will be the most effective for its suppression. Increasing structural secrecy of radio signal is aimed at increasing a priori uncertainty of its parameters, and is achieved by manipulating them. An improved method for estimating noise immunity of global navigation satellite systems is proposed in the article. The method allows taking into account the dynamics of the conflict between the navigation system and the interference transmitter: changing signal parameters in time and exploring them. The estimation of noise immunity of navigation signals of global navigation satellite systems allowed to conclude that the use of an increased number of binary quasi-orthogonal code sequences sets will provide high noise immunity of the global navigation satellite system for 15 years.**

Keywords—Satellite navigation, noise immunity, electronic conflict, a priori uncertainty, radio intelligence.

I. PROBLEM DEFINITION

In electronic conflict the task of wireless data transmission system is to provide the availability of radio channel in conditions of interference. And the task of interference transmitter is to suppress the radio channel with interference [1]. Interference transmitter must explore the parameters of the radio signal to form interference which will be the most effective for its suppression. In turn of wireless data transmission system it must ensure the secrecy of signal parameters.

The secrecy of signal parameters [2] can be separated on three types:

- energy secrecy.
- structural secrecy.
- information secrecy

Increasing energy secrecy of radio signals can be achieved by expanding their spectrum. This measure can not always be used, because of regulatory procedures for the distribution of radio frequencies. In some cases, it is also ineffective, because, for example, the model of orbital constellation and moving of space vehicles (SVs) is widely known. In this case, the attacker is able to organize automatic following of the SVs by radio monitoring tools for the radio intelligence of all emitted radio signals [3] by spatial selection method.

Increasing information secrecy of radio signals is carried out by encrypting the message and using methods to confirm its authenticity. It allows increasing the noise immunity of radio signal in case of its substitution attempt. However, these methods do not protect against the suppression of the radio signal by simulating interference.

Increasing structural secrecy of radio signal is aimed at increasing a priori uncertainty of its parameters, and is achieved by manipulating them [4]. In particular, the main parameters of the navigation signal with code division multiple access (CDMA) can be used to increase structural secrecy are the following:

- carrier frequency.
- modulation method.
- code sequence (raging code).

In some sources [5,6] it is noted that by means of stochastic use of code sequences sets it is possible to increase structural secrecy of radio signals in CDMA data transmission systems. Since the radio channel “SVs- GNSS Navigation Receiver (NR)” is a CDMA data transmission system, for it can be used the method to increase structural secrecy based on the stochastic use of code sequences as raging codes.

In [6] the method of modeling quasi-orthogonal code sequences sets (QOCSS) is proposed. It is based on functional transformations of pseudo-random arguments. It can be implemented in on-board equipment of SVs and in NRs to improve structural secrecy of the navigation signals (NSs) based on QOCSS stochastic use as ranging codes. Structural secrecy is a constituent element of NSs noise immunity, and increasing the first the last also increases [7]. However, the noise immunity increase should be evaluated taking into account many parameters, among which the quantity and correlation properties of the stochastically used QOCSS are important under the action of simulating noise. In [8] the algorithms allowing to make noise immunity estimation of GNSS are given. However, these algorithms can not be called universal. In this regard, it is necessary to develop an improved algorithm for estimating the noise immunity of GNSS, which allows to be used for any type of

interference, as well as takes into account the dynamics of both GNSS and interference transmitter.

II. METHOD DEVELOPING

In [9] it is proposed to estimate the noise immunity of GNSS by the probability of electronic suppression of GNSS: $P_{ES} = 1 - P_{NTS}$, where P_{NTS} - the probability of successful navigation task solution, which contains the probability of successful primary processing of information and the probability of successful secondary processing of information:

$$P_{SNT} = P_1 P_2. \quad (1)$$

Evaluation of P_1 in [9] is proposed to do on the basis of four components:

1) Two-dimensional search of the NS by delay and frequency, detection and confirmation of the signal presence (is characterized by the probability of wrong decisions in search and detection P_{sd}) [10].
2) Tracking the Doppler shift of the NS and its evaluation (is characterized by the probability of frequency tracking failure in the phase-locked loop frequency module P_{cf} of the tracking frequency channel in NR) [11].
3) Tracking the envelope delay of the NS and its evaluation (is characterized by the probability of delay tracking failure P_{ct}) [12].
4) Signal demodulation (is characterized by the probability of errors on the information bit P_{eb}) [13].

After successful execution of the primary information processing in NR it is not difficult to carry out secondary information processing which is the solution of navigation task. It is based on the received navigation message and the NS parameters [14]. We can assume that the probability of a successful navigation task solution depends significantly on the probability of successful primary information processing:

$$P_{SNT} = P_1 = (1 - P_{sd})(1 - P_{cf})(1 - P_{ct})(1 - P_{eb}). \quad (2)$$

However, the approach presented in [9] does not allow to estimate the dynamics of the interaction between GNSS and the opposing side - the interference transmitter. Meanwhile, to assess the interference impact on any stage of primary processing in the NR, it is necessary to determine the probability that the interference will be transmitted; the probability that the interference spectrum will fall into the NR reception band; the probability of exceeding the interference power at the input of the NR over the power of the NS.

In [5] it is stated the approach to noise immunity estimation for wireless communication systems which allows to estimate all above-mentioned probabilities. Combining the approaches described in [9] and [5] will allow to develop an improved method for estimating the noise immunity of GNSS. New method would take into account an expanded list of factors affecting GNSS operation.

Developed improved method of estimation the noise immunity of GNSS includes the following steps:

A. Step 1.

Estimation of the probability of successful navigation task solution in absence of interference based on the equation:

$$P_{SNTa} = (1 - P_{sd})(1 - P_{cf})(1 - P_{ct})(1 - P_{eb}). \quad (3)$$

B. Step 2.

Estimation of influence probability on NS GNSS (its suppression) by the equation:

$$P_{SP} = P_{exp} P_{use} P_{inf}. \quad (4)$$

where $P_{exp} = P\{H_{exp}\}$ - probability that the parameters $\Theta = (\Theta_1,\ldots, \Theta_m)$ of navigation signals $s_j(t, \Theta)$, $j = 1{:}M$, $M \geq 1$, $t \in [0, T_0]$ used in GNSS will be determined (explored) by the interference transmitter (hypothesis H_{exp}); $P_{use} = P\{H_{use} \mid H_{exp}\}$ - probability of using interference (hypothesis H_{use}) provided that the parameters ($\Theta = (\Theta_1,\ldots, \Theta_m)$, $m \geq 1$) of the NS are explored with the accuracy necessary for interference transmission (hypothesis H_{exp}); $P_{inf} = P\{H_{inf} \mid H_{use} \cap H_{exp}\}$ - the probability of interference influence on the NR GNSS (hypothesis H_{inf}) provided that the parameters of the NS are explored (evaluated) with a given accuracy (hypothesis H_{exp}) and the interference transmitter is used (hypothesis H_{use}). Probability P_{SP} characterizes the secrecy of GNSS.

C. Step 2.1.

Evaluation of exploration probability for the NS parameters that are necessary for interference transmission. It is necessary to explore various NS parameters for providing various types of interference. In general, the exploration probability of the NS parameters, which are necessary for interference providing is estimated with the following equation:

$$P_{exp} = \sum_{i=1}^{n} p_i P_{exp\,i}, \quad (5)$$

where $P_{exp\,i}$ - the exploration probability of the i-th NS parameter; p_i - the weight factor that determines the importance of exploration of the i-th NS parameter for providing some interference type, $\Sigma p_i = 1$.

The disadvantage of existing approaches to estimate the exploration probability of the NS parameters is the lack of accounting for the accumulation of intelligence information by the radio intelligence subsystem of the interference transmitter, which in most cases significantly accelerates the process of NS parameters exploration. When stochastic change of QOCSS is used in GNSS radio intelligence subsystem has to accumulate information about the used QOCSS. That reduces the a priori uncertainty of the structure of the manipulating functions (ranging codes). Then, the exploration probability of the signal parameter at the i-th moment of time has the form:

$$P_{exp\,i}(t) = \frac{1}{n - mt}, \quad (6)$$

where n - total number of all permissible values, which can take the explored NS parameter; m – number of values of the

NS parameter, explored by the radio intelligence subsystem for selected unit of time; t - time of the radio intelligence subsystem working.

Equation (6) significantly changes the nature of estimation the GNSS noise immunity by adding a time parameter into it. Thus, the main indicator of GNSS noise immunity - the probability of solving the navigation task - will be a function of time when taking into account the equation (6).

Let us consider the task of the radio intelligence subsystem for monitoring GNSS NSs with CDMA, that have increased structural secrecy. In contrast to a single NS, the identification of a working group from the NSs with CDMA is an ambiguous task. The number of unique choices of different events from the total number is equal to the number of combinations [4]:

$$R = \binom{A}{m} = \frac{A!}{(A-m)!m!}, \quad (7)$$

where $A = 2^N$ - full amount of sequence codes of length N.

In the most unfavorable case, when the interference transmitter does not have information on the algorithm of forming QOCSS, to estimate the maximum possible a priori uncertainty of raging codes structure in (7), the full amount of code sequences A should be replaced by $A_{\beta\mu cf}$. $A_{\beta\mu cf}$ is an amount of code sequences, that satisfy statistic and correlation requirements to be used in NS with CDMA [6]. However, when estimating the secrecy of systems it is assumed that the algorithm for forming QOCSS is known, and only its initial state is unknown. In this case, A in (7) should be replaced by the total number of code sequences A_{pc} that can be derived from the used algorithm.

The equation (7) also should be adjusted taking into account (6). Since the duration of the code sequence period is close to milliseconds, m code sequences structures will be explored during this time interval. Since the radio intelligence subsystem needs to identify the NSs of the available SVs constellation m can take values from the following interval: m = [1:50]. This interval is determined because of the number of code sequences in the set [6]. Taking into account all the above, (7) is transformed as follows:

$$R_k = \frac{(A_{pc} - mt)!}{(A_{pc} - m(t+1))!m!}, \; t = [0,\ldots,n], \quad (8)$$

where t - time of radio intelligence subsystem working, counted in milliseconds.

D. Step 2.2.

Evaluation of the probability of using interference transmitter P_{use} and the probability of interference influence on the GNSS NR P_{inf}.

Probability of using interference transmitter is suggested to estimate with the equation:

$$P_{use} = P_{ud} P_{uf} P_{ua}. \quad (9)$$

where P_{ud} - the probability that the distance between the NR and the interference transmitter will satisfy the necessary energy suppression conditions; P_{uf} - the probability that the operating frequency ranges of the NR and interference transmitter will coincide; P_{ua} - the probability that the antenna system of the interference transmitter is directed at the antenna system of the NR, and the total transmission coefficient in the radio channel is not less than valid.

The probability of interference influence on the NR GNSS is proposed to be estimated on the basis of the following equation:

$$P_{inf} = P_{ib} P_{ip} P_{ii}. \quad (10)$$

where P_{ib} - the probability of getting interference in the NR bandwidth; P_{ip} - the probability of pointing the antenna system of the interference transmitter on the NR antenna with the accuracy necessary to create interference with sufficient power; P_{ii} - the probability that the interference will get to the input of the NR during its operation, at the time when the NS is received.

E. Step 3.

Evaluation of the probability of navigation task successful solution under the influence on the NS of radio interference with the equation:

$$P_{SNTp} = (1 - P_{si1}) (1 - P_{si2}) (1 - P_{si3}) (1 - P_{si4}), \quad (11)$$

which is a product of the successful impact probabilities on each of the stages of the information primary processing in the NR.

F. Step 4.

Estimation of the general indicator of GNSS noise immunity - probability of successful navigation task solution in the conditions of interference influence - on the basis of the equation:

$$P_{NI}(t) = P_{SNTa} + P_{SP}(t) (P_{SNTp} - P_{SNTa}), \quad (12)$$

which, taking into account the previously given equation s, will take the form:

$$P_{NI}(t) = (1 - P_{sd}) (1 - P_{cf}) (1 - P_{ct}) (1 - P_{eb}) + P_{ud} P_{uf} P_{ua} P_{ib} P_{ip} P_{ii} \Sigma p_i P_{exp\,i}(t) ((1 - P_{si1}) (1 - P_{si2}) (1 - P_{si3}) (1 - P_{si4}) - (1 - P_{sd}) (1 - P_{cf}) (1 - P_{ct}) (1 - P_{eb})), \quad (13)$$

Now let us use this improved method for estimating the noise immunity of the GNSS that has the NSs with CDMA. We compare the noise immunity of an open NS that has static publicly known parameters and the NS that has increased structural secrecy due to the stochastic use of a large amount of QOCSS [7].

The most effective interference for the suppression of NS GNSS with CDMA in relation of the probability of suppression to the required energy potential of the interference transmitter is imitation interference [9]. Based on the data from [9] on the basis of the proposed improved method, the noise immunity of GNSS for the following NS GNSS with CDMA will be estimated [15]:

1) In the NS is used the only QOCSS structure as raging codes, which is described in detail in the publicly available ICD.

2) In the NS, all the QOCSS with length 4095 bits from table 1 are used stochastically and their correlation peaks do not exceed 0.06.

3) In the NS all the QOCSS with length 8191 bits from table 1 are used is stochastically and their correlation peaks do not exceed 0.06.

4) In the NS all the QOCSS with length 10230 bits from table 1 are used is stochastically and their correlation peaks do not exceed 0.06.

5) In the NS are stochastically uses the QOCSS obtained on the basis of the developed method of providing the QOCSS [6]. The method is based on functional transformations of pseudorandom arguments, which allows to obtain the QOCSS with a high structure complexity. The correlation peaks do not exceed the values of 0.06 for the lengths of 4095, 8191 and 10230 bits.

It should be noted, that 2-4 cases of protection the NS GNSS with CDMA suggest mixed use of well-known code sequences of different types, but the same length.

TABLE I. AMOUNT OF QOCSS WITH WARIOUS LENGTH

Algorithm of QOCSS developing	**Code sequences length**	**Number of sets with 50 sequences volume**
Gold codes	8191	51345
	10230	118320
Kasami codes	4095	335
	10230	48698145
Kamaletdinov codes	4095	8
	8191	12
	10230	20
Kerdock codes	4095	15170080
	8191	417476,268
Weil codes	4095	18630
	8191	70416
	10230	109344
Bent-functions	4095	335
QOCSS based on the developed method [5]	4095	$4{,}73\cdot10^{11}$
	8191	$4{,}73\cdot10^{11}$
	10230	$4{,}73\cdot10^{11}$

III. ESTIMATION OF GNSS NOISE IMMUNITY ON THE BASIS OF THE DEVELOPED METHOD

On the basis of the developed improved method, we estimate the noise immunity of NS GNSS with CDMA for the five cases described above.

A. Step 1. Estimation of the probability of successful navigation task solution in the absence of interference influence

In the absence of interference influence in accordance to [8] GNSS has the following qualities: $P_{sd} = 1{,}75\cdot10^{2}$, $P_{cf} = 5\cdot10^{2}$, $P_{ct} = 3\cdot10^{-3}$, $P_{eb} = 2\cdot10^{-12}$.

Then the probability of a successful navigation task solution of the GNSS in the absence of interference influence is:

$$P_{SNTa} = (1 - 0.0175)\ (1 - 0.05)\ (1 - 0.003)\ (1 - 2\cdot10^{-12}) = 0.9306. \quad (14)$$

This value is enough to solve the navigation task in most transport and telecommunication systems.

B. Step 2. Estimation of the probability of interference influence to the NS GNSS

The most important component of the second step is the estimation of the probability of exploration of the NS parameters necessary for the organization of imitation interference.

C. Step 2.1. Estimation of the probability of eploring interference parameters necessary for the interference organization

GNSS is characterized by a large amount of a priori information on the trajectories of SVs flights, energy, frequency, time and statistical characteristics of existing open NSs. At the same time, a priori unknown parameters to be estimated as a result of radio intelligence are amplitude, Doppler frequency shift and time delay of the signal envelope. The carrier frequencies L of all open NSs are described in the GNSS ICDs. According to [9] in the process of radio intelligence carrier frequency can be explored with probability $P_{inL} = 0.9825$. The NR channel bandwidth can also be determined based on the NSs parameters described in the ICD. The probability of frequency exploration will be $P_{inF} = 0.95$. The NS amplitude can be determined in the process of establishing energy contact during the time $t = [2\cdot10^{-2};0.5]$ seconds [3] with probability $P_{inU} = 0.997$. Given the continuous nature of GNSS operation there are no time constraints on the operation of the interference transmitter. According to [3] the above NS parameters can be explored in a time not exceeding 22 minutes for any of the existing and projected public NS GNSS with CDMA.

Based on the information in table 1, we can find the sum of all QOCSS with length 4095, 8191 and 10230 bits considered there can be found. The correlation peaks of QOCSS do not exceed 0.06. Knowing the number of QOCSS, united in three groups according to the sequence length, we can find the probability of raging code intelligence. Table 2 shows the total number of QOCSS united into three groups according to length, as well as the probability of exploring the raging codes structure for each QOCSS group at a time $t = 0$.

TABLE II. THE PROBABILITY OF EXPLORING THE RAGING CODES STRUCTURE FOR THREE GROUPS OF QOCSS, UNITED BY LENGTH

Code length	4095	8191	10230
Total nunber of QOCSS	15189388	121773	466402097
Probability of exploring the raging codes structure at a time $t = 0$	$1{,}63 \cdot 10^{-359}$	$1{,}04 \cdot 10^{-254}$	$8{,}1 \cdot 10^{-434}$

As can be seen from table 2, the probability of exploring the raging codes structure at a time tends to zero $P_{exQ} \to 0$. However, since the equation (13) is a time function, the probability of raging codes structure exploration will decrease as the radio intelligence subsystem receives and processes received NS. At a time when all code sequences, reserved for use of certain SV will be used and will start their recurrence, the probability of exploring the raging codes structure will be equal to one.

D. Step 2.2. Estimation of the probability of interference transmission and the probability of interference influence on NR GNSS

Determining the capabilities of the opposing side (interference transmitter) is a task difficult to formalize. Therefore, to simplify estimation of the probability of a successful navigation task solution in the conditions of interference influence in this paper will be made the assumption that the probability of interference transmitting and the probability of the interference influence on the NS will be equal to one: $P_{use} = 1$ and $P_{inf} = 1$. It will be regardless of the successful exploration of the NS parameters.

E. Step 3. Evaluation of the probability of successful navigation task solution under the interference influence on the NS

According to the third step of the method, the probability of a successful navigation task solution under the imitation interference influence on the NS is estimated. It should be noted that the considered indicator will be the same for both open and protected NS. Since it expresses the interference influence, organized with a complete and reliable exploration of all NS parameters by the radio intelligence subsystem:

$$P_{SNTp} = (1-0.67)(1-0)(1-0.67)(1-0) = 0.1089. \quad (15)$$

F. Step 4. Estimation of GNSS general noise immunity - probability of the successful navigational task solution in conditions of interference transmission

Figure 1 shows the graphs of the function described by equation (13) for the five cases of NS parameters described above.

Figure 1 presents the following graphs: 1 – noise immunity of open NS that uses a single QOCSS structure; 2 - noise immunity of the NS, stochastically using known QOCSS with length 8191 bits; 3 - noise immunity of the NS, stochastically using known QOCSS with length 4095 bits; 4 - noise immunity of the NS, stochastically using known QOCSS with length 10230 bits; 5 - noise immunity of the NS, stochastically using QOCSS obtained by the developed method of developing QOCSS, based on functional transformations of pseudo-random arguments.

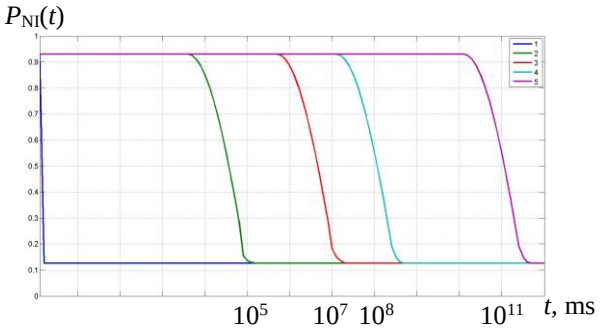

Fig. 1. Graphs of the function $P_{NT}(t)$ expressing noise immunity of NS GNSS with CDMA for five considered cases

As can be seen on figure 1, the probability of navigation task solving at the moment of time $t = 0$ ms. is the same for all five NS and equals 0.93. However the open NS, using the only QOCSS structure as raging codes, the probability of navigation task solving drops to 0,1265 already at the moment of time $t = 1$ ms. as the radio intelligence subsystem explores the QOCSS structure that was used. For protected NSs, that stochastically use a variety of known QOCSS, the probability of solving navigation task remains of 0.93 for a long time. Thus, using all the structures of known QOCSS with length 4095 bits will protect the NS from imitation interference influence for a period of a little more than 4 hours; using all the structures of known QOCSS with length 8191 bits - for a period of a little more than 2 minutes; using all the structures of known QOCSS with length 10230 - for a period of a little less than 6 days. Figure 1 also shows that the stochastic use of the QOCSS obtained by the developed [5] method on the basis of functional transformations of pseudorandom arguments will protect the NS from imitation interference influence for a period of 15 years, which was originally intended for its development.

IV. CONCLUSION

An improved method for estimating the noise immunity of global navigation satellite systems is proposed. That allows to take into account the dynamics of the confrontation between the navigation system and the interference generator and transmitter, including radio intelligence subsystem.

The estimation of noise immunity of global navigation satellite systems navigation signals allowed to conclude that the use of an increased number of binary quasi-orthogonal code sequences sets obtained by the developed [4] method of their developing will provide high noise immunity of the global navigation satellite system for 15 years.

ACKNOWLEDGMENT

This work was supported by the Russian Foundation for Basic Research, project No. 18-07-01020.

REFERENCES

[1] T. Morong, P. Puričer, P. Kovář, “Study of the GNSS jamming in real environment”, International Journal of Electronics and Telecommunications, Vol. 65, Issue 1, 2019, pp 65-70.

[2] V. I. Borisov, V. M. Zinchuk, “Noise immunity of radio communication systems. Probabilistic-time approach. 2-nd issue, corrected” Moscow: RadioSoft, 2008, p. 260.

[3] A. P. Dyatlov, B. H. Kulbikayan, “Radio monitoring of radiation of satellite radio navigation systems” Moscow: Radio and communication, 2006, p. 270.

[4] Z. M. Kanevskij, V. P. Litvinenko, G. V. Makarov, D. A. Maksimov, “Fundamentals of the secrecy theory: textbook” Voronezh: VGU publishing, 2006, p. 197.

[5] D. Orel, A. Zhuk, E. Zhuk, L. Luganskaia, “A method of forming code sets for CDMA in communication, navigation and control systems” CEUR Workshop Proceedings 2. Cep. “YSIP2 2017 - Proceedings of the 2nd Young Scientist's International Workshop on Trends in Information Processing”, 2017, pp. 158-167.

[6] A. P. Zhuk, D. V. Orel, L. A. Luganskaia, “Method of forming signal sets with the required correlation properties for wireless infocommunication system” Information and communication technologies in science, production and education i (Infokom-6), Proceedings of the sixth international scientific and technical conference, 2014, pp. 24-28.

[7] D. V. Orel, A. P. Zhuk, “Method of increasing noise immunity of navigation signal of satellite radio navigation system” Proceedings of the Moscow Institute of physics and technology, vol. 6, #4(24), 2014, pp. 119-125.

[8] A. A. Apollonov, “Improvement of accuracy and reliability characteristics of the user segment of satellite radio navigation systems in high latitudes” Thesis for the degree of candidate of technical Sciences, Moscow: MSTUCA, 2010, p. 84.

[9] A. P. Dyatlov, P. A. Dyatlov, B. H. Kulbikayan, “Electronic warfare with satellite radio navigation systems” Moscow: Radio and communication, 2004, p. 226.

[10] S. Zhao, Y.S. Shmaliy, F. Liu, “Fast Kalman-like optimal FIR filter for time-variant systems with improved robustness”, ISA Transactions, Vol. 80, 2018, pp. 160-168.

[11] M. Guan, L. Wang, B. Peng, “Adaptive Separation of Subcarrier for Wireless Link of Satellite Communication”, Wireless Personal Communications, Vol. 103, Issue 1, 2018, pp. 159-166.

[12] Y. Choe, C.H. Kang, S.Y. Kim, C.G. Park, “INS/GPS deep integration using Frobenius norm based adaptive filter with two adaptation parameters”, Journal of Institute of Control, Robotics and Systems, Vol. 24, Issue 8, 2018, pp 716-721.

[13] J.a,b. Yu, W.a. Yang, W.a. Lu, S.a. Liang, “Analysises and comparisons on noise performances of PLL, DLL and data demodulator in GNSS receiver”, 2011 IEEE International Conference on Signal Processing, Communications and Computing, ICSPCC 2011, Xi'an; China, 2011, #6061636.

[14] B. Xu, L.-T. Hsu, “Open-source MATLAB code for GPS vector tracking on a software-defined receiver”, GPS Solutions, Vol. 23 Issue 2, #46, 2019.

[15] S.-J.a Ko, B.a Eissfeller, J.-H.a Won, T.b Pany, “Assessment of vector-tracking-loop performance under radio frequency interference environments”, 25th International Technical Meeting of the Satellite Division of the Institute of Navigation 2012, ION GNSS 2012, Vol. 3, 2012, pp 2333-2341