DOI: 10.18721/JCSTCS.14304
УДК 621.37

SEMI-NATURAL MODELING FOR GNSS INTEGRITY MONITORING ALGORITHM

A.P. Rachitskaya

Peter the Great St. Petersburg Polytechnic University,
St. Petersburg, Russian Federation

The paper considers the suboptimal version of GNSS integrity monitoring algorithm involving multichannel signal processing. This algorithm was examined in terms of probability-based characteristics obtained during semi-natural modeling. Such modeling assumes that multichannel snapshots are getting from real channels of multichannel GNSS receiver including antenna array when all subsequent procedures are implemented in Matlab later. Probability-based characteristics obtained in such way consequently checked with similar characteristics obtained by Matlab simulation ideal model, which ignored probable effects of signal transmission and reception in real environment. It was shown the level of similarity between characteristics of both types, and also clarified the conditions when the characteristics are close to each other, and the conditions when the difference between them is significant. The main reason of such difference was found out empirically.

Keywords: generalized maximum likelihood ratio test, probability-based characteristics, confidence interval, non-identity of channels, multichannel receiver.

Citation: Rachitskaya A.P. Semi-natural modeling for GNSS integrity monitoring algorithm. Computing, Telecommunications and Control, 2021, Vol. 14, No. 3, Pp. 43–55. DOI: 10.18721/JCST-CS.14304

ПОЛУНАТУРНОЕ МОДЕЛИРОВАНИЕ АЛГОРИТМА КОНТРОЛЯ ЦЕЛОСТНОСТИ НАВИГАЦИОННОГО ПОЛЯ ГНСС

А.П. Рачицкая

Санкт-Петербургский политехнический университет Петра Великого,
Санкт-Петербург, Российская Федерация

Рассмотрен алгоритм контроля целостности навигационного поля (КЦНП), синтезированный в соответствии с обобщенным критерием отношения правдоподобия для прямой многоканальной обработки сигналов с элементов антенной решетки (АР). Произведена оценка эффективности алгоритма с помощью полунатурного моделирования, с использованием записи реальных навигационных сигналов с элементов АР и их обработкой в среде Matlab в соответствии с рассматриваемым алгоритмом КЦНП. Проведено сравнение результатов измерения вероятностных характеристик алгоритма, полученных на основе такого моделирования, с аналогичными результатами идеализированного моделирования в среде Matlab, когда формирование сигналов производится искусственно без учета возможных факторов (на пути распространения сигналов или при их приёме), возникающих при работе алгоритма в реальных условиях. Выявлена степень соответствия результатов обоих типов моделирования. Определены условия, когда получаемые результаты оказываются близки и когда расхождения значительны. Экспериментальным путем установлена одна из возможных причин найденных различий между характеристиками.

Ключевые слова: обобщенный критерий максимального правдоподобия, вероятностные характеристики, доверительный интервал, неидентичность каналов, многоканальный приёмник.

Ссылка при цитировании: Rachitskaya A.P. Semi-natural modeling for GNSS integrity monitoring algorithm // Computing, Telecommunications and Control. 2021. Vol. 14. No. 3. Pp. 43–55. DOI: 10.18721/JCSTCS.14304

Introduction

Various faults occurring in the process of receiving and processing signals of the global navigation satellite system (GNSS) [2–5] can lead to significant errors in the navigation object (NO) devices. If the errors exceed a certain permissible level (for example, the level of normal errors caused by the thermal noise of the NO receiver), it is interpreted as a breach of the integrity of the navigation field (NF) [1, 6–9]. To detect such situations, specialists develop methods of GNSS integrity monitoring [9–16]. Each of the methods is usually optimized for specific types of faults. In addition, the effectiveness of the developed methods of GNSS integrity monitoring aimed at identifying critical failure caused by the false navigation signal sources (FNSS) in a number of cases either proves to be unacceptably low or inapplicable for all NO types [13, 15, 17–19]. Failures caused by spoofing are especially hazardous as the NO may receive signals identical to the signals of navigation satellites (NS) at the input. However, they have different values of time-frequency parameters, which results in bias errors in the results of the NO devices operation [11, 13, 20–22].

There are various approaches that consider the features of such faults [13, 14, 20, 23, 24, 26], but in the majority of cases, the task of GNSS integrity monitoring can be re reduced to decision-making on whether or not there is any spoofing involved. To improve the effectiveness of such a check, it is possible to use statistical synthesis of a decision-making algorithm based on the a *priori* known data on the position of GNSS satellites at the orbit. Moreover, the best effectiveness is achieved by "direct" analysis of the processes observed in the antenna array (AA) elements [27, 28].

Direct suboptimal algorithm is of special practical interest. It is obtained as a result of statistical synthesis taking into account several simplifications, in particular, an assumption of significant difference between the NO coordinates estimates and its actual position in case of FNSS impact, as well as some other conditions (see below) [28]. The feasibility of using this algorithm is due to its low computational complexity in comparison with other similar algorithms (the number of multiplications omitted can reach up to one order or more) combined with its high level of effectiveness, which is proved with modeling in the Matlab environment [27, 28]. At the same time, this modeling was conducted in ideal conditions disregarding possible factors emerging in real conditions (features of satellite and FNSS signals propagation, nonidentity of NO device channels, etc.). Therefore, the conclusions drawn on the basis of such an ideal (hereafter referred to as "conventional") modelling cannot be considered fully objective. We can make the results obtained before more accurate by means of semi-natural modeling, when we use the records of actual navigation signals from AA elements and process them in the Matlab environment according to the GNSS integrity monitoring algorithm under study.

We evaluated the effectiveness of the considered GNSS integrity monitoring algorithms [27] based on the analysis of such characteristics as:

1) the probability of a false decision that there is interference, while it is actually absent (P_{FA} probability of false alarm);

2) the probability of a false decision that there is no interference, while it is actually present (P_{MD} probability of missed detection).

Both probabilities are calculated, if there are GNSS signals present. In addition, according to the Neyman – Pearson criterion [25], the considered algorithms were optimized by means of minimizing the P_{MD} probability at a fixed value of the P_{FA} probability, which determines the value of decision-making threshold Λ_0.

Direct suboptimal algorithm of GNSS integrity monitoring

Let us consider a direct suboptimal algorithm of GNSS integrity monitoring obtained on the basis of a comparison between the likelihood ratio and the threshold for the processes snapshots in the AA elements.

The likelihood functions for column-vector $\mathbf{x}(t)=\left[x_1(t), x_2(t), ..., x_M(t)\right]^{\mathrm{T}}$ of $x_m(t)$ processes snapshots on each m^{th} of M antenna elements is formed separately if one of the two possible hypothesis H_0 and H_1 is valid in case of observing a constellation from L satellites and the presence of additive white Gaussian noise (AWGN) in the AA elements. H_0 corresponds to the situation when the FNSS influence is absent, while H_1 takes place when there is FNSS influence present, moreover, we consider a single FNSS emitting all L radio-navigation signals from one point [11]. The parameters of the satellite radio-navigation signals (initial phases, amplitudes), as well as the NO parameters (its coordinates $\mathbf{P}_{NO}$, velocity, attitude angles α_1, α_2, α_3) are considered unknown. We assume the FNSS parameters (coordinates $\mathbf{P}_S$ of the FNSS itself), false coordinates $\mathbf{P}'$ and velocity vector $\mathbf{v}'$ of the NO generated by the FNSS to be unknown as well. We exclude the indicated unknown ("interfering") parameters in accordance with the generalized likelihood ratio test [25].

The test involves maximization (either analytical directly during the algorithm synthesis or numerical during the consequent algorithm running) with respect to the values of these parameters. The "initial" direct optimal algorithm obtained in this manner requires considerable computations as the majority of the maximization procedures with respect to unknown parameters can be solved numerically only in the process of running the considered algorithm. We can significantly simplify it by a conversion into a suboptimal algorithm: to reduce the computing costs, we use a justified assumption on a significant deviation of the NO coordinates from the actual position if the H_1 hypothesis is valid [29]. We can achieve additional simplification by means of substituting the numerical maximization with respect to unknown values of $\mathbf{P}'$ coordinates and $\mathbf{v}'$ velocity vector with a numerical maximization directly with respect to time-frequency parameters $\boldsymbol{\tau}'_1, \Delta\boldsymbol{\omega}'_d$ of the FNSS radio-navigation signals. Here, $\boldsymbol{\tau}'_1=\left[\tau_1'^{(1)}, \tau_1'^{(2)}, ..., \tau_1'^{(L)}\right]$ is a vector the elements of which comprise the propagation times of l^{th} FNSS signal to the AA antenna element chosen as a reference one, while $\Delta\boldsymbol{\omega}'_D=\left[\Delta\omega_D'^{(1)}, \Delta\omega_D'^{(2)}, ..., \omega_D'^{(L)}\right]$ is a vector of Doppler shifts of the FNSS signals frequencies.

The "direct suboptimal algorithm" obtained this way presupposes a numerical maximization with respect to angular directions μ_S and η_S (azimuth and incline respectively) in the FNSS [28]:

$$\frac{1}{ME_0N_0}\left\{\max_{\substack{\boldsymbol{\tau}'_1,\Delta\boldsymbol{\omega}'_d\\ \mu_S,\eta_S}}\sum_{l=1}^{L}\left|\mathbf{V}_l'^{T}\mathbf{H}_S\right|^2\right\}\underset{H_0}{\overset{H_1}{\gtrless}}\Lambda_0, \tag{1}$$

where $E_0=\int\limits_{(T_a)}\left(\sum\limits_{l=1}^{L}C_0^{(l)}(t)\right)^2 dt$; $N_0/2$ is the spectral density of the average AWGN power at the input of the receiver channels (the channels are assumed to be identical); $C_0^{(l)}(t)$ is a pseudorandom sequence modulating signal of the l^{th} satellite; $\mathbf{H}_S=\left[\mathrm{e}^{j\delta\varphi'_1}, \mathrm{e}^{j\delta\varphi'_2}, ..., \mathrm{e}^{j\delta\varphi'_M}\right]^{\mathrm{T}}$ is the directing vector column for a pos-

sible direction μ_S, η_S in the FNSS, where $\delta\varphi'_m = \frac{\omega_0^{(l)}}{c}\left(\mathbf{k}_0^S(\mu_S,\eta_S)\right)^{\mathrm{T}}\tilde{\mathbf{P}}_m$; $\mathbf{k}_0^{(S)}(\mu_S,\eta_S) = \left[x_{k0}^{(S)}, y_{k0}^{(S)}, z_{k0}^{(S)}\right]^{\mathrm{T}}$; $x_{k0}^{(S)} = \sin\mu_S\cos\eta_S; y_{k0}^{(S)} = \cos\mu_S\cos\eta_S; z_{k0}^{(S)} = \sin\eta_S$; c is the speed of light in vacuum, $l = 1 \ldots L$, $\omega_0^{(l)}$ is the carrier frequency of the radio signal emitted by the l^{th} satellite; $\tilde{\mathbf{P}}_m = \left[\tilde{x}_m, \tilde{y}_m, \tilde{z}_m\right]^{\mathrm{T}}$ are the coordinates of the AA elements in the local coordinates system of the NO [2, 3];

$$\mathbf{V}'_l = \left[V_1'^{(l)}, V_2'^{(l)}, \ldots, V_M'^{(l)}\right]^{\mathrm{T}}, \tag{2}$$

where $V_m'^{(l)} = \int\limits_{(T_a)} F_{xm}(t)C_0^{*(l)}\left(t-\tau_1'^{(l)}\right)e^{-j\Delta\omega_D'^{(l)}t}e^{-j\Delta\omega_0^{(l)}t}dt$ and integration are performed in the analysis interval the T_a value of which is defined by the duration of the pseudorandom sequence $C_0^{(l)}(t)$; $F_{xm}(t)$ is a complex envelope of the $x_m(t)$ snapshot; $\Delta\omega_0^{(l)} = \omega_0^{(l)} - \omega_0$ is a deviation of the l^{th} satellite radio signal frequency from the carrier receiver frequency ω_0.

Semi-natural modeling

In the course of the semi-natural modeling, a GPS simulator of L1 range (1575.42 MHz) emits L signals of FNSS. An experimental simulation device of GNSS integrity monitoring includes a multichannel signal recorder, 6-element AA receiver (layout presented in Fig. 1), and a standard navigation receiver (Ublox-M8T) for the monitoring of radio navigation signals present. The multichannel signal recorder makes snapshots of the processes from the AA elements via a multichannel radio frequency (RF) receive path and digitizes the respective $x_m(t)$ processes using an analog-to-digital converter. The reference values of the $F_{xm}(t)$ complex envelope of the $x_m(t)$ processes digitized at the sampling rate of 2.046 MHz are stored as .dat-files.

In the course of the semi-natural modeling, the GPS simulator emitted the FNSS signals with the power level significantly exceeding the radio navigation signals of the satellite (the interference/signal ratio was $\gamma \approx 6$ dB). The signals were received and recorded in real conditions in the presence of tress, urban buildings, moving objects, etc. Fig. 2*a* shows the satellite group observed in the process of the experiment.

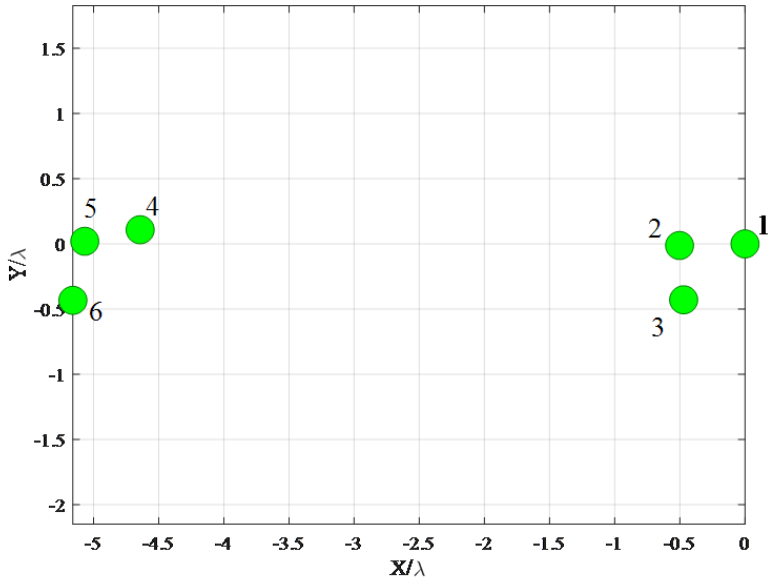

Fig. 1. Configuration of the 6-element AA used in the study

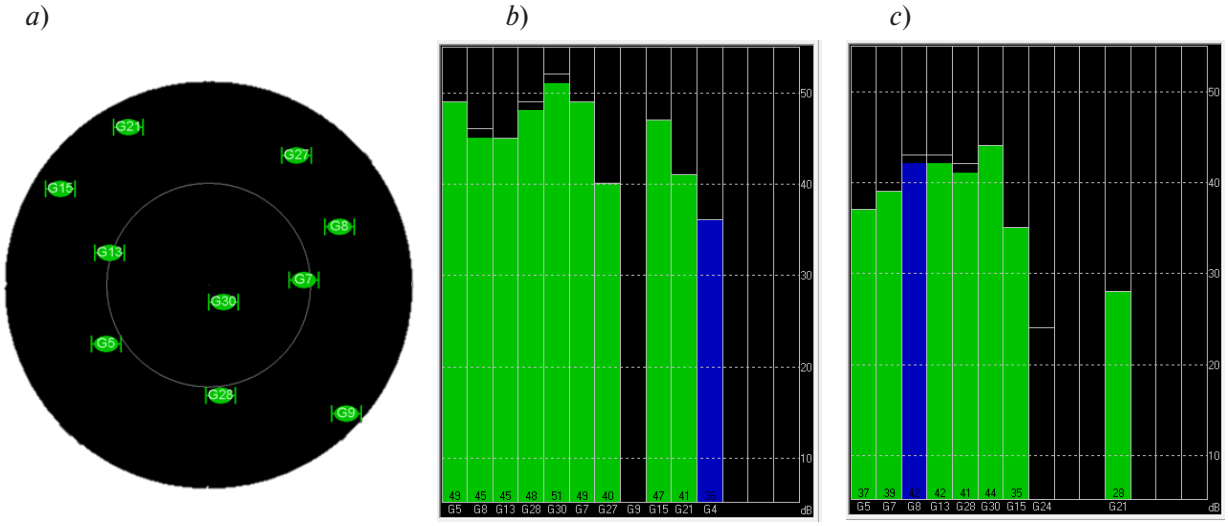

Fig. 2. View of the observed satellite constellation (*a*), visual representation of the detected radio navigation signals in the absence of FNSS signals (*b*) and in their presence (*c*) in the indicator of the Ublox-M8T receiver

Simultaneously with recording the signals from the AA elements, we were monitoring the readings of the standard navigation receiver connected to one of the AA elements. Fig. 2*c* shows an example of the results of processing legitimate GNSS satellite group signals in the interface of the standard navigation receiver Ublox-M8T in case there is no GNSS integrity failure. Each column depicted in Fig. 2*b* corresponds to the observed radio navigation signal the number of which (satellite number) is located in the bottom; the height of a column is proportional to the value of the C_0/N_0 ratio of C_0 carrier power of the radio navigation signal under consideration to the doubled spectral power density of the AWGN. Fig. 2*b* shows an example of indicating the results of processing the radio navigation signals by the same navigation receiver under the influence of FNSS. There is an obvious absence of any identifying attributes of the fact that in the second case the coordinates were measured according to the FNSS signals with significant mistakes. At the same time, in the presence of the FNSS the measured values of the NO coordinates considerably differ from the coordinates measured in case the FNSS influence is absent.

Thus, Table 1 shows an example of the measurements for the coordinates in both cases under study obtained in one of the experiments. The measured coordinates clearly differ by approximately 1600 m.

Table 1

Results of processing navigation signals by the Ublox-M8T receiver in the absence and in the presence of FNSS signals

Presence of FNSS signals	Latitude, deg	Longitude, deg	Altitude, m	Standard deviation of measurements caused by AWGN, m	Absolute deviation from the actual NO position caused by FNSS, m
–	59.9937998	30.3795120	56.5	3...7	–
+	59.9874327	30.3536052	2.7	4...8	1611.5

Results of the semi-natural modeling

We used Matlab algorithm model (1) for the semi-natural modeling, while the recordings of the real signals from the AA elements were incoming to the input of the model for analysis. The obtained charac-

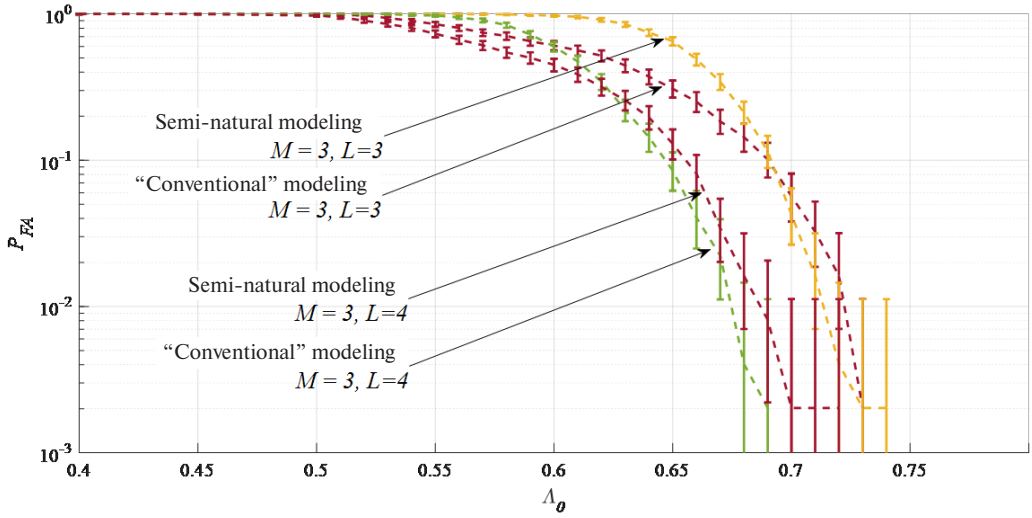

Fig. 3. Probability of false alarm at $M = 3$, $L = 3$, 4 and $C_0/N_0 = 45...50$ dB·Hz

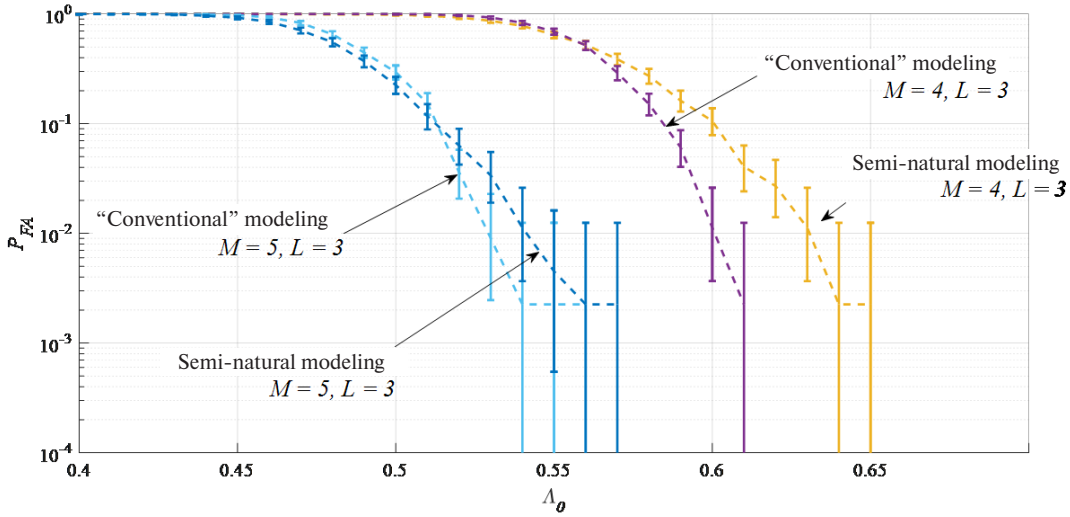

Fig. 4. Probability of false alarm at $L = 3$, $M = 4$, 5 and $C_0/N_0 = 45...50$ dB·Hz

teristics (P_{FA} and P_{MD}) of algorithm (1) were compared with the similar characteristics resulting from the "conventional" modeling in the identical conditions, when $C_0/N_0 = 40...50$ dB·Hz, $\gamma = 6$ dB. Fig. 3 presents dependencies of the P_{FA} probability on the decision-making threshold Λ_0 for $M = 3$, $L = 3$ (satellites no. 5, 7 and 8 in Fig. 2).

A comparison of the dependencies of the P_{FA} probability on the decision-making threshold obtained in the process of the semi-natural modeling with the results of the "conventional" modeling revealed a certain divergence (less than a half an order of magnitude). Similar conclusions can be also drawn while using the signals of 4 satellites ($L = 4$ in Fig. 3), as well as with a larger number of elements ($M = 4$, 5 in Fig. 4).

At the same time, when calculating the P_{MD} probability, we registered strong influence of the AA design on the degree of proximity of the characteristics obtained by two types of modeling under study. Thus, we found little difference in the P_{MD} values obtained in the course of the "conventional" and semi-natural modeling at the small number of the AA elements ($M = 3$ in Fig. 5); at the larger numbers ($M = 4$ in Fig. 6), this difference was growing. Therefore, at $M = 5$ (Fig. 7), the difference in the P_{MD} characteristics obtained by means of two different ways of modeling exceeded several orders.

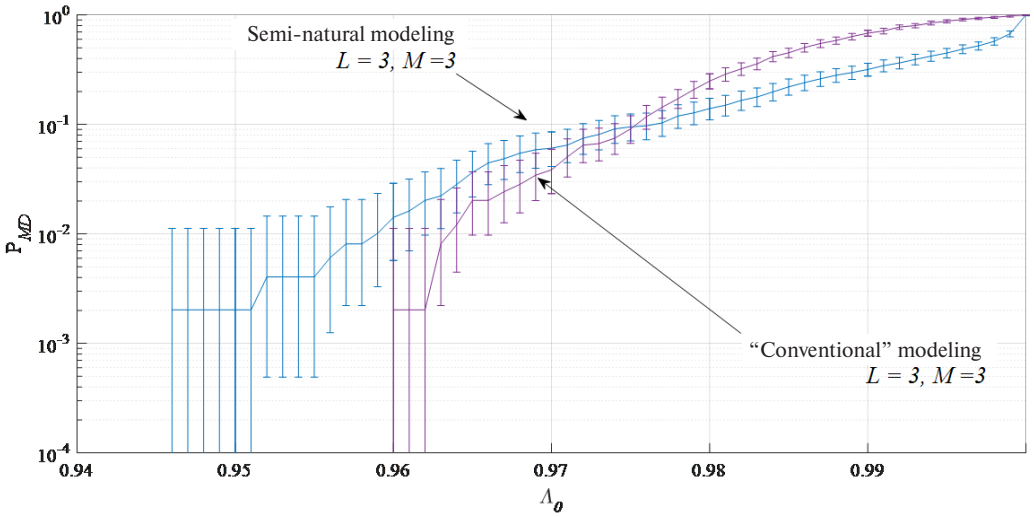

Fig. 5. Probability of missed detection at $M = 3$, $L = 4$, $C_0/N_0 = 45...50$ dB·Hz and $\gamma = 6$ dB

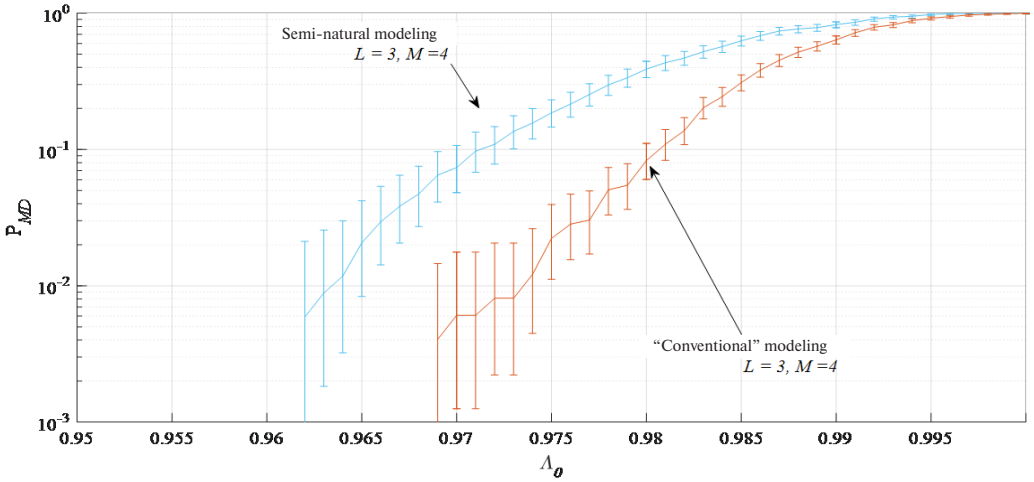

Fig. 6. Probability of missed detection at $M = 4$, $L = 3$, $C_0/N_0 = 45...50$ dB·Hz and $\gamma = 6$ dB

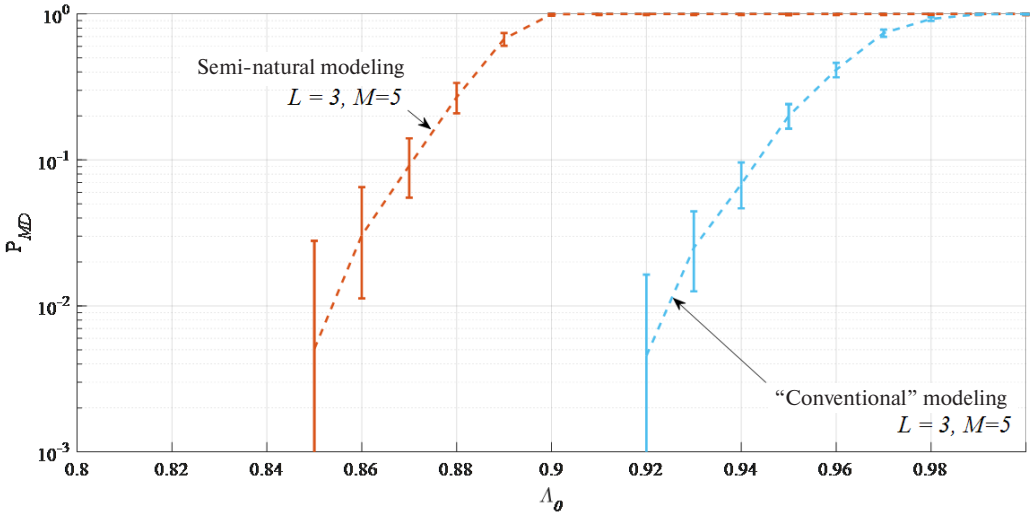

Fig. 7. Probability of missed detection at $M = 5$, $L = 3$, $C_0/N_0 = 45...50$ dB·Hz and $\gamma = 6$ dB

We can assume that the cause of the discovered divergence between the probability characteristics obtained by both the above mentioned types of modeling is a possible nonidentity of the channels of the receive path used for recording of the signals from the respective AA elements. Testing this assumption is of interest.

Influence of nonidentity of the receive path channels on the efficiency of the GNSS integrity monitoring system

As additional researched results [30] showed, the semi-natural modeling employed a multichannel receiver with a significant difference in the gain characteristics between the channels, so the phase difference $\Delta\varphi_m$ between the channels reached 2π rad and more (Table 2).

Table 2

Change in the unknown $\Delta\varphi_m$ phase tune-outs between the AA channels

	Channel 1	Channel 2	Channel 3	Channel 4	Channel 5	Channel 6
$\Delta\varphi_m$, rad	0	1.699130	–1.650571	0.985480	–1.128182	–0.255712

By compensating the phase tune-outs (according to Table 2) during the semi-natural modeling, we can improve the characteristics of the GNSS integrity monitoring algorithm and make them approach the respective characteristics obtained by means of the "conventional" modeling (Fig. 8–10). The improvement of the probability characteristics after compensation is especially significant at $M > 3$, so at $M = 5$ it reaches 3 or more orders. Thus, we can confirm the assumption that the main reason for the divergence in the results of the semi-natural modeling from the "conventional" modeling lies in the nonidentity of the receiver channels.

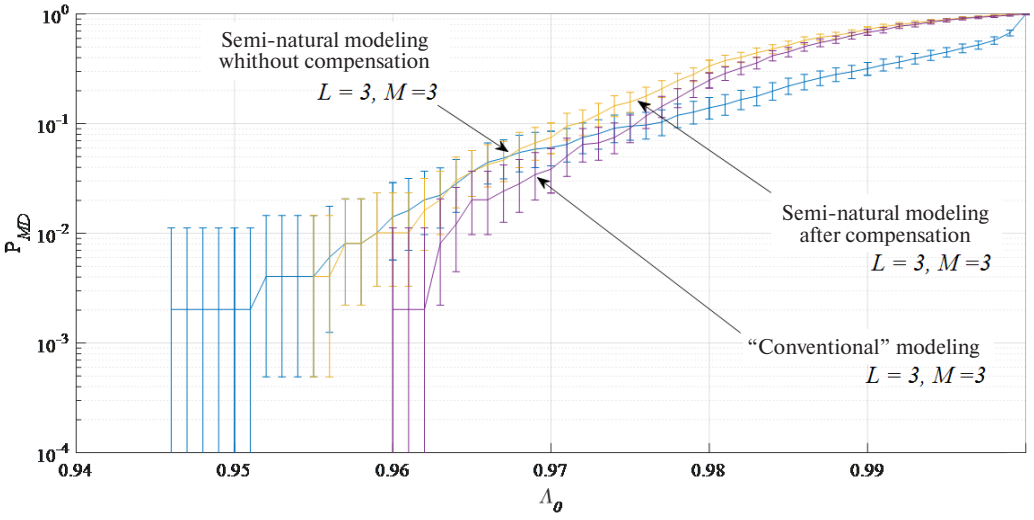

Fig. 8. Probability of missed detection at $M = 3$, $L = 3$, $C_0/N_0 = 45...50$ dB·Hz and $\gamma = 6$ dB

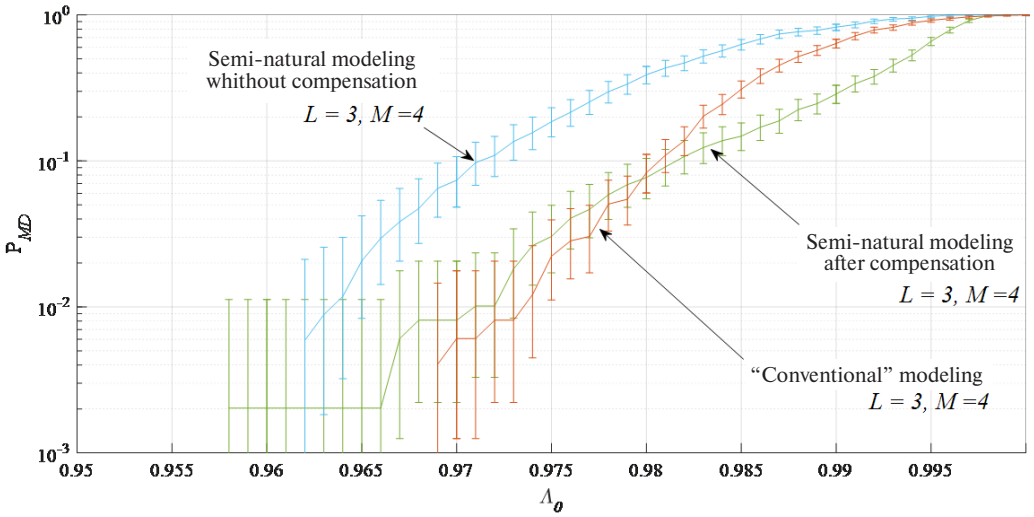

Fig. 9. Probability of missed detection at $M = 4$, $L = 3$, $C_0/N_0 = 45...50$ dB·Hz and $\gamma = 6$ dB

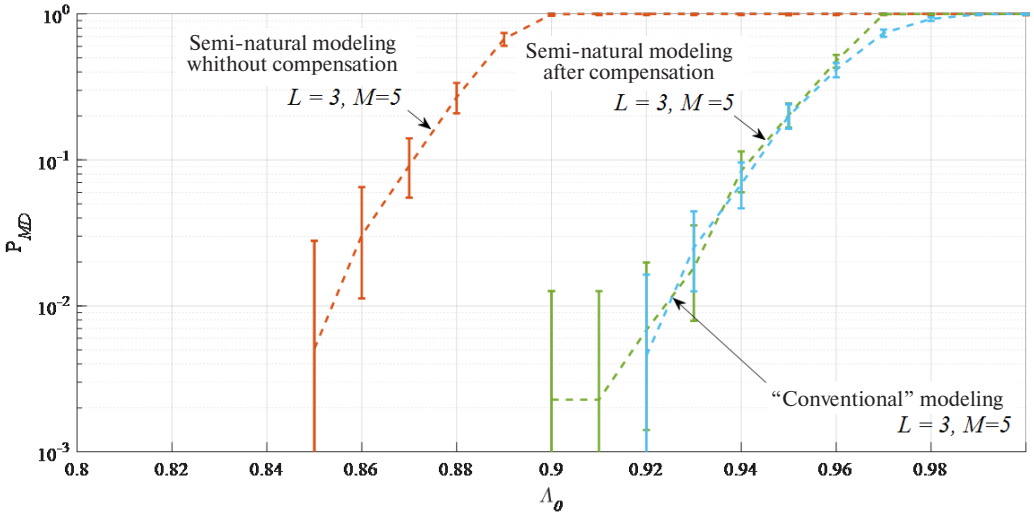

Fig. 10. Probability of missed detection at $M = 5$, $L = 3$, $C_0/N_0 = 45...50$ dB·Hz and $\gamma = 6$ dB

Conclusions

In the process of the conducted research, we showed that the “conventional” modeling in ideal conditions (rectilinear propagation of satellite signals, absence of the multipath propagation effect, identity of the receive path channels, etc.) allows us to evaluate the considered GNSS integrity monitoring algorithm for the simplest antenna arrays (2–3 elements) quite accurately in real receiving conditions even in case of a considerable nonidentity of the receive path channels. On the other hand, when more complex antenna arrays (4 or more elements) are involved, the results of the “conventional” modeling adequately reflect the efficiency of the GNSS integrity monitoring algorithm built only on the basis of radio receive path with a compensation of phase tune-outs between the channels.

The considered method of the semi-natural modeling obviously allows evaluating the efficiency of the GNSS integrity monitoring algorithm with various geometric properties of the GNSS groups and in different conditions of receiving signals from satellites and false sources.

REFERENCES

1. **Teunissen P.J.G., Montenbruck O.** (eds.). *Springer handbook of global navigation satellite systems*. Springer, 2017.

2. **Cheng J., Wang J., Zhao L.** A direct attitude determination approach based on GPS double-difference carrier phase measurements. *Journal of Applied Mathematics*, 2014, No. 6, Pp. 1–6. DOI: 10.1155/2014/548083

3. **Daneshmand S., Sokhandan N., Lachapelle G.** Precise GNSS attitude determination based on antenna array processing. *Proceedings of the 27th International Technical Meeting of the Satellite Division of the Institute of Navigation* (*ION GNSS 2014*), Tampa, FL, USA, 2014, Vol. 812.

4. **Niu X., Yan K., Zhang T., Zhang Q., Zhang H., Liu J.** Quality evaluation of the pulse per second (PPS) signals from commercial GNSS receivers. *GPS Solutions*, 2015, No. 19(1), Pp. 141–150. DOI: 10.1007/s10291-014-0375-7

5. **Karutin S.N., Lerner D.V., Kharisov V.N.** Synthesis of synchronization algorithms based on the retransmission of navigation signals from a ground station [Synthesis of algorithms based on relaying navigation signals from a ground station]. *Radiotekhnika*, 2016, No. 9, Pp. 88–96. (rus)

6. **Ochieng W.Y., Sauer K.** GPS integrity and potential impact on aviation safety. *Journal of Navigation*, 2003, Vol. 56, No. 1, Pp. 51–65.

7. **Milner C., Macabiau C., Thevenon P.** Bayesian inference of GNSS failures. *Journal of Navigation*, 2016, No. 69(2), Pp. 277–294. DOI: 10.1017/S0373463315000697

8. **Heng L., Gao G.X., Walter T., Enge P.** Statistical characterization of GLONASS broadcast ephemeris errors. *Proceedings of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation* (*ION GNSS 2011*), Portland, OR, 2011, Pp. 3109–3117.

9. **Ahn J., Lee Y.J., Won D.H., Jun H.S., Yeom C., Sung S., Lee J.O.** Orbit ephemeris failure detection in a GNSS regional application. *International Journal of Aeronautical and Space Sciences*, 2015, No. 16(1), Pp. 89–101.

10. **Kulnev V., Mikhailov S.** Analiz napravleniy i sostoyaniya razrabotok funktsionalnykh dopolneniy k sputnikovym radionavigatsionnym sistemam [Analysis of state of the art of development of augmentation aids to satellite radio navigation systems]. *Besprovodnyye tekhnologii* [*Wireless Technologies*], 2006, No. 4, Pp. 61–69. (rus)

11. **Amin M.G., Closas P., Broumandan A., Volakis J.L.** Vulnerabilities, threats, and authentication in satellite-based navigation systems. *Proceedings of the IEEE*, 2016, No. 104(6), Pp. 1169–1173. DOI: 10.1109/JPROC.2016.2550638

12. **Bao L., Wu R., Wang W., Lu D.** Spoofing mitigation in Global Positioning System based on C/A code self-coherence with array signal processing. *Journal of Communications Technology and Electronics*, 2017, No. 62(1), Pp. 66–73.

13. **Broumandan A., Jafarnia-Jahromi A., Daneshmand S., Lachapelle G.** Overview of spatial processing approaches for GNSS structural interference detection and mitigation. *Proceedings of the IEEE*, 2016, No. 104(6), Pp. 1246–1257. DOI: 10.1109/JPROC.2016.2529600

14. **Wesson K.D., Gross J.N., Humphreys T.E., Evans B.L.** GNSS signal authentication via power and distortion monitoring. *IEEE Transactions on Aerospace and Electronic Systems*, 2018, No. 54(2), Pp. 739–754.

15. **Zhang Z., Zhan X.** GNSS spoofing network monitoring based on differential pseudorange. *Sensors*, 2016, Vol. 16, No. 10, 1771. DOI: 10.3390/s16101771

16. **Wang F., Li H., Lu M.** GNSS spoofing countermeasure with a single rotating antenna. *IEEE Access*, 2017, Vol. 5, Pp. 8039–8047.

17. **Ochin E.** *Detection of spoofing using differential GNSS*. Zeszyty Naukowe Akademii Morskiej w Szczecinie, 2017.

18. **Khanafseh S., Roshan N., Langel S., Chan F.C., Joerger M., Pervan B.** GPS spoofing detection using RAIM with INS coupling. *Proceedings of the Position, Location and Navigation Symposium*, 2014, Vol. 2014.

19. **Hewitson S., Wang J.** Extended receiver autonomous integrity monitoring (E-RAIM) for GNSS/INS integration. *Journal of Surveying Engineering*, 2010, Vol. 136, No. 1, Pp. 13–22.

20. **Ioannides R.T., Pany T., Gibbons G.** Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques. *Proceedings of the IEEE*, 2016, No. 104(6), Pp. 1174–1194.

21. **Van der Merwe J.R., Zubizarreta X.** Classification of spoofing attack types. *2018 European Navigation Conference* (*ENC*), IEEE, 2018, Pp. 91–99.

22. **Stubberud S.C., Kramer K.A.** Threat assessment for GPS navigation. *Proceedings of the 2014 IEEE International Symposium on Innovations in Intelligent Systems and Applications*, IEEE, 2014, Pp. 287–292. DOI: 10.1109/INISTA.2014.6873632

23. **Jovanovic A., Botteron C., Fariné P.A.** Multi-test detection and protection algorithm against spoofing attacks on GNSS receivers. *Position, Location and Navigation Symposium* (*PLANS*) *2014*, 2014 IEEE/ION, Pp. 1258–1271.

24. **Amin M.G., Closas P., Broumandan A., Volakis J.L.** Vulnerabilities, threats, and authentication in satellite-based navigation systems. *Proceedings of the IEEE*, 2016, No. 104(6), Pp. 1169–1173. DOI: 10.1109/JPROC.2016.2550638

25. **Van Trees H.L.** *Optimum array processing: Part IV of detection, estimation, and modulation theory*. John Wiley & Sons, 2004.

26. **Montgomery P.Y., Humphreys T.E., Ledvina B.M.** Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer. *Proceedings of the 2009 International Technical Meeting of the Institute of Navigation*, 2009, Pp. 124–130.

27. **Melikhova A.P., Tsikin I.A.** Optimum array processing with unknown attitude parameters for GNSS anti-spoofing integrity monitoring. *Proceedings of the 2018 41st International Conference on Telecommunications and Signal Processing* (*TSP*), IEEE, 2018, Pp. 1–4.

28. **Rachitskaya A.P., Tsikin I.A.** GNSS integrity monitoring in case of a priori uncertainty about user's coordinates. *Proceedings of the 2018 IEEE International Conference on Electrical Engineering and Photonics* (*EExPolytech*), IEEE, 2018, Pp. 83–87.

29. **Tippenhauer N.O., Pöpper C., Rasmussen K.B., Capkun S.** On the requirements for successful GPS spoofing attacks. *Proceedings of the 18th ACM Conference on Computer and Communications Security*, ACM, 2011, Pp. 75–86. DOI: 10.1145/2046707.2046719

30. **Tsikin I., Shcherbinina E.** GPS antenna array calibration for attitude determination based on reference phase difference method. *Proceedings of the 2016 39th International Conference on Telecommunications and Signal Processing* (*TSP*), IEEE, 2016, Pp. 174–177. DOI: 10.1109/TSP.2016.7760853

Received 17.05.2021.

СПИСОК ЛИТЕРАТУРЫ

1. **Teunissen P.J.G., Montenbruck O.** (eds.). Springer handbook of global navigation satellite systems. Springer, 2017.

2. **Cheng J., Wang J., Zhao L.** A direct attitude determination approach based on GPS double-difference carrier phase measurements // J. of Applied Mathematics. 2014. No. 6. Pp. 1–6. DOI: 10.1155/2014/548083

3. **Daneshmand S., Sokhandan N., Lachapelle G.** Precise GNSS attitude determination based on antenna array processing // Proc. of the 27th Internat. Technical Meeting of the Satellite Division of the Institute of Navigation. Tampa, FL, USA, 2014. Vol. 812.

4. **Niu X., Yan K., Zhang T., Zhang Q., Zhang H., Liu J.** Quality evaluation of the pulse per second (PPS) signals from commercial GNSS receivers // GPS Solutions. 2015. No. 19 (1). Pp. 141–150. DOI: 10.1007/s10291-014-0375-7

5. **Карутин С.Н., Лернер Д.В., Харисов В.Н.** Синтез алгоритмов синхронизации на основе ретрансляции навигационных сигналов с наземной станции // Радиотехника. 2016. № 9. С. 88–96.

6. **Ochieng W.Y., Sauer K.** GPS integrity and potential impact on aviation safety // J. of Navigation. 2003. Vol. 56. No. 1. Pp. 51–65.

7. **Milner C., Macabiau C., Thevenon P.** Bayesian inference of GNSS failures // J. of Navigation. 2016. No. 69 (2). Pp. 277–294. DOI: 10.1017/S0373463315000697

8. **Heng L., Gao G.X., Walter T., Enge P.** Statistical characterization of GLONASS broadcast ephemeris errors // Proc. of the 24th Internat. Technical Meeting of the Satellite Division of the Institute of Navigation. Portland, OR, 2011. Pp. 3109–3117.

9. **Ahn J., Lee Y.J., Won D.H., Jun H.S., Yeom C., Sung S., Lee J.O.** Orbit ephemeris failure detection in a GNSS regional application // Internat. J. of Aeronautical and Space Sciences. 2015. No. 16 (1). Pp. 89–101.

10. **Кульнев В., Михайлов С.** Анализ направлений и состояния разработок функциональных дополнений к спутниковым радионавигационным системам // Беспроводные технологии. 2006. № 4. С. 61–69.

11. **Amin M.G., Closas P., Broumandan A., Volakis J.L.** Vulnerabilities, threats, and authentication in satellite-based navigation systems // Proc. of the IEEE. 2016. No. 104 (6). Pp. 1169–1173. DOI: 10.1109/JPROC.2016.2550638

12. **Bao L., Wu R., Wang W., Lu D.** Spoofing mitigation in Global Positioning System based on C/A code self-coherence with array signal processing // J. of Communications Technology and Electronics. 2017. No. 62 (1). Pp. 66–73.

13. **Broumandan A., Jafarnia-Jahromi A., Daneshmand S., Lachapelle G.** Overview of spatial processing approaches for GNSS structural interference detection and mitigation // Proc. of the IEEE. 2016. No. 104 (6). Pp. 1246–1257. DOI: 10.1109/JPROC.2016.2529600

14. **Wesson K.D., Gross J.N., Humphreys T.E., Evans B.L.** GNSS signal authentication via power and distortion monitoring // IEEE Transactions on Aerospace and Electronic Systems. 2018. No. 54 (2). Pp. 739–754.

15. **Zhang Z., Zhan X.** GNSS spoofing network monitoring based on differential pseudorange // Sensors. 2016. Vol. 16. No. 10. 1771. DOI: 10.3390/s16101771

16. **Wang F., Li H., Lu M.** GNSS spoofing countermeasure with a single rotating antenna // IEEE Access. 2017. Vol. 5. Pp. 8039–8047.

17. **Ochin E.** Detection of spoofing using differential GNSS. Zeszyty Naukowe Akademii Morskiej w Szczecinie, 2017.

18. **Khanafseh S., Roshan N., Langel S., Chan F.C., Joerger M., Pervan B.** GPS spoofing detection using RAIM with INS coupling // Proc. of the Position, Location and Navigation Symp. 2014. Vol. 2014.

19. **Hewitson S., Wang J.** Extended receiver autonomous integrity monitoring (E-RAIM) for GNSS/INS integration // J. of Surveying Engineering. 2010. Vol. 136. No. 1. Pp. 13–22.

20. **Ioannides R.T., Pany T., Gibbons G.** Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques // Proc. of the IEEE. 2016. No. 104 (6). Pp. 1174–1194.

21. **Van der Merwe J.R., Zubizarreta X.** Classification of spoofing attack types // Proc. of the 2018 European Navigation Conf. IEEE, 2018. Pp. 91–99.

22. **Stubberud S.C., Kramer K.A.** Threat assessment for GPS navigation // Proc. of the 2014 IEEE Internat. Symp. on Innovations in Intelligent Systems and Applications. IEEE, 2014. Pp. 287–292. DOI: 10.1109/INISTA.2014.6873632

23. **Jovanovic A., Botteron C., Fariné P.A.** Multi-test detection and protection algorithm against spoofing attacks on GNSS receivers // Position, Location and Navigation Symp. 2014. IEEE/ION, 2014. Pp. 1258–1271.

24. **Amin M.G., Closas P., Broumandan A., Volakis J.L.** Vulnerabilities, threats, and authentication in satellite-based navigation systems // Proc. of the IEEE. 2016. No. 104 (6). Pp. 1169–1173. DOI: 10.1109/JPROC.2016.2550638

25. **Van Trees H.L.** Optimum array processing: Part IV of detection, estimation, and modulation theory. John Wiley & Sons, 2004.

26. **Montgomery P.Y., Humphreys T.E., Ledvina B.M.** Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer // Proc. of the 2009 Internat. Technical Meeting of the Institute of Navigation. 2009. Pp. 124–130.

27. **Melikhova A.P., Tsikin I.A.** Optimum array processing with unknown attitude parameters for GNSS anti-spoofing integrity monitoring // Proc. of the 2018 41st Internat. Conf. on Telecommunications and Signal Processing. IEEE, 2018. Pp. 1–4.

28. **Rachitskaya A.P., Tsikin I.A.** GNSS integrity monitoring in case of a priori uncertainty about user's coordinates // Proc. of the 2018 IEEE Internat. Conf. on Electrical Engineering and Photonics (EExPolytech). IEEE, 2018. Pp. 83–87.

29. **Tippenhauer N.O., Pöpper C., Rasmussen K.B., Capkun S.** On the requirements for successful GPS spoofing attacks // Proc. of the 18th ACM Conf. on Computer and Communications Security. ACM, 2011. Pp. 75–86. DOI: 10.1145/2046707.2046719

30. **Tsikin I., Shcherbinina E.** GPS antenna array calibration for attitude determination based on reference phase difference method // Proc. of the 2016 39th Internat. Conf. on Telecommunications and Signal Processing. IEEE, 2016. Pp. 174–177. DOI: 10.1109/TSP.2016.7760853

Статья поступила в редакцию 17.05.2021.

THE AUTHOR / СВЕДЕНИЯ ОБ АВТОРЕ

Rachitskaya Antonina P.
Рачицкая Антонина Павловна
E-mail: antonina_92@list.ru