УДК 621.396.669

THE ALGORITHM'S ANALYSIS AND RESULTS OF THE GNSS CNE SPOOFING'S SELECTION AND COMPENSATION WITH MULTI-CHANNEL ANTENNA SYSTEM

SAAD H. KH.

Белорусский государственный университет информатики и радиоэлектроники (г. Минск, Беларусь)

E-mail: HusseinSaadTENG@outlook.com

Аннотация. Глобальные навигационные спутниковые системы (ГНСС) подвержены множеству помех. Спуфинг, то есть подмена навигационных сигналов, является одной из основных преднамеренных помех, влияющих на измерения положения, скорости и времени в отношении различных систем ГНСС и, в основном, пользователей системы GPS. Предложенный ранее алгоритм защиты от спуфинга GPS выбор сигналов спуфинга и их компенсации в качестве основы для получения требуемого уровня точности позиционирования. В статье приведены описание результатов анализа алгоритма, показывающие применимость и эффективность последнего.

Abstract. Global navigation satellite systems (GNSSs) are exposed to many interference incidents. Spoofing is considered one of the main intentional interference affecting the position, velocity, and time (PVT) measurements concerning the different systems of GNSS and mainly the users of the GPS one. A proposed anti-spoofing GPS/GNSS algorithm has been done before as a way for selecting the spoofing signals and compensating them as a base to get the precise accuracy level of positioning and location. Such algorithm was described previously with the main steps that should be followed to attain our mission. The article shows the analysis description and the results of the applied algorithm, showing the validity of the last.

Problem statement

Many incidents have been recorded concerning the issue of intentional and unintentional GNSS interference. GNSS (especially the GPS system) spoofing is assumed to be the main pillar of the erroneous navigation measurements. GPS spoofing is can be defined as transmitting fake navigation signals by the spoofer/s to attack the desired CNE, so that the victim will get a false position, follows a different route, faces surveying problems, etc. In our proposed anti-spoofing algorithm (applied previously), we are able to detect the spoofing signals and make compensation or suppression, the way which lead to make use as much as possible from the true navigation satellites only and that what will be shown accordingly as a result after the analysis and the discussion of this algorithm.

The anti-spoofing algorithm in brief

Before the discussion of the processing proposed algorithm and its analysis, what is shown in the figure below confines the main steps of the implemented algorithm.

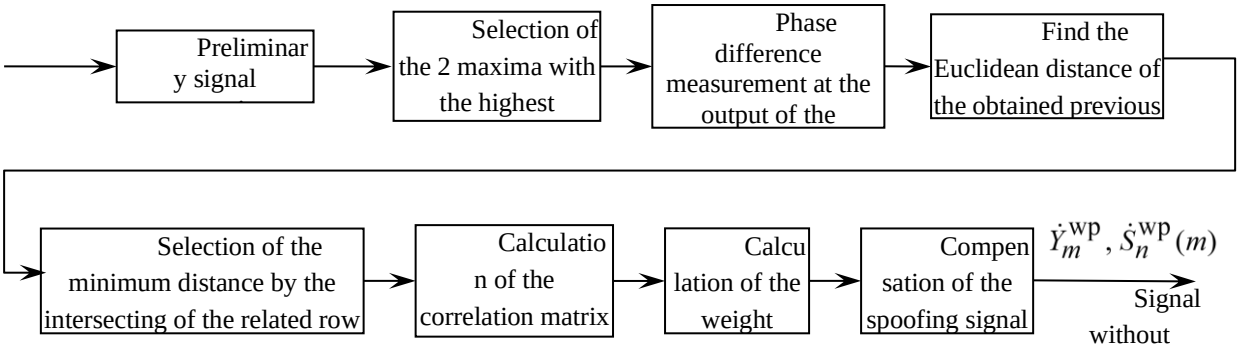


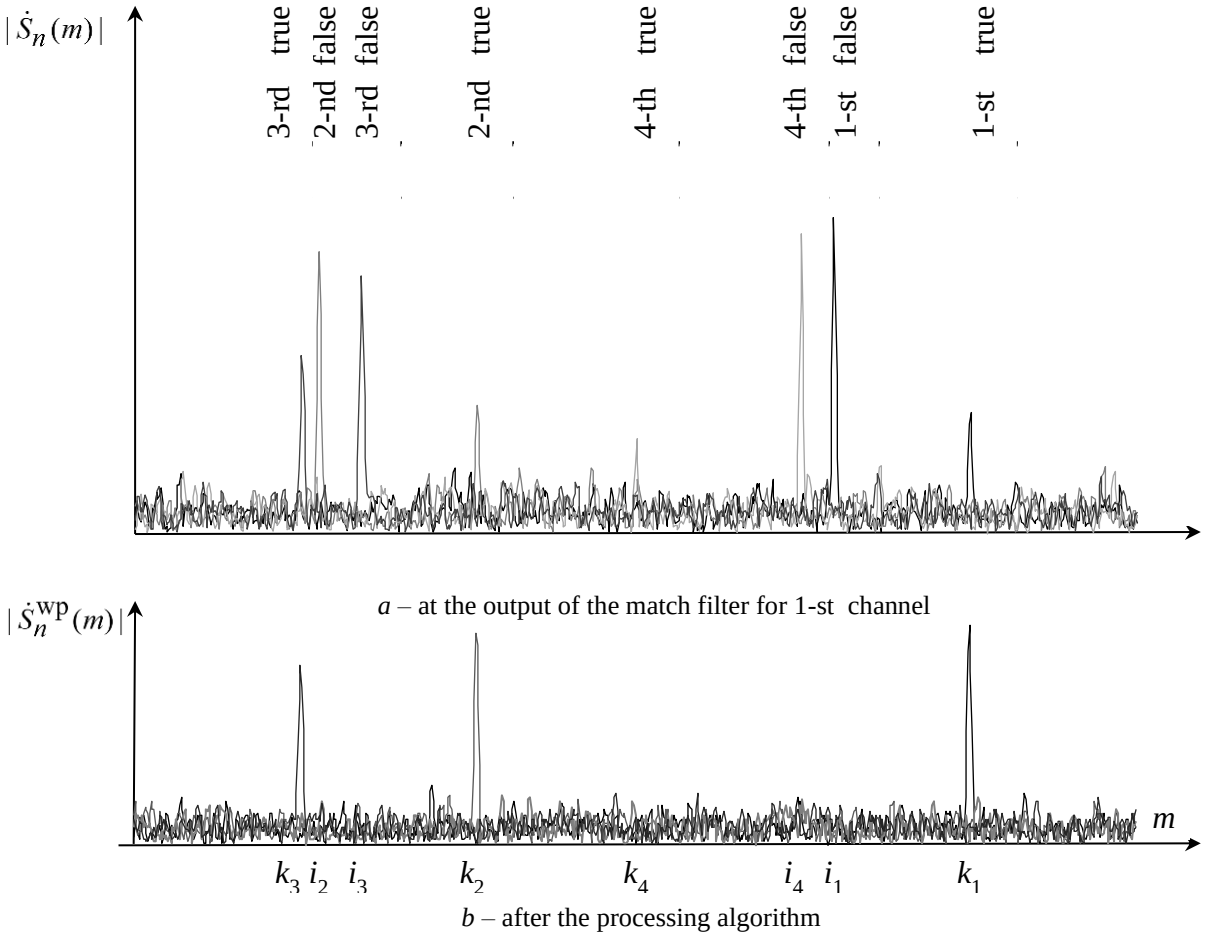
Fig. 1. The main stages of the processing algorithm for spoofing compensation

Knowing that if the radial velocity is negative, Doppler shift will be positive, they are inversely proportional to each other. Moreover, if the reflection is very high value, then the processing of spoofing suppression will decrease and the power of the output noise in the processing operation will decrease too. Also, and dealing with the power of noise, as the last at the output filter increases, then and accordingly to the time delay of the true navigation signals, the accuracy will be minimized.

Simulation results and discussion

The simulation of the model is done using Matlab software. In our model, we set the positions of the array antenna elements, the directivity of these elements, the coordinates of the GPS navigation satellites, coordinates of the spoofer, jammer, false positioning coordinates; add to that all the parameters related to the GPS NSs, power transmitted by the GPS NS, power of the spoofer, jammer, azimuths and elevations for all the NSs, spoofer, jammer, etc…In our model, we calculate the signal at the input of the receiving channels and processing procedure is done according to the formulas (1)-(18). Then we detect the navigation signal, estimate the time delay, and measure the coordinates of the CNE. In the simulation process, we set the following parameters: the carrier frequency f_0 = 1575,42 MHz, $\lambda = c / f_0$, bandwidth of the receiving channels is 4 MHz, T_0 = 1ms, F_s = 4 MHz, L =4, N_{T_0} =4, the distance between the elements of the array antenna system is $\lambda / 2$, the spectral power density of the noise power is $N_0 = 10^{-20} W / \mathrm{H}z$. Note that the power of the spoofer is 0,01 W. Moreover, the parameters of the GPS NS are standard [1,2]. We assume that the coordinates of the spoofer and the false position are respectively the following: (-1500, -5000,20) and (7000,8000,0). Furthermore, the coordinates of the array antenna elements are (0,0,0). The gain in zenith for the array's elements is 3 dBi for each; the directivity of the array elements is represented as the cosine of the angle between the zenith and the source's direction (spoofer, NS, jammer,etc.).

The results of the simulation are shown in figure 2. In the first part of the figure, we can notice obviously that at the output of the filter the indices of maximum for the four true signals and the four spoofing signals, and after the operation of the processing algorithm, the compensation and the suppression of the spoofing signals while receiving only the navigation satellites' signals (true signals) with increasing in the amplitudes dealing mainly with the first and the second true signals.



a – at the output of the match filter for 1-st channel

b – after the processing algorithm

Fig. 2. The true and the spoofing signals at the output of the match filter for the 1-st channel and after the processing algorithm

Table 1 shows the gain values for the adapted directional pattern towards the directions of the spoofer and the NSs in decible unit with reference to the isotropic antenna (dBi) for 10 iterations. Add to that, there are also the values for the NSs' signal to noise ratio (SNR) and the resulting error in estimating the coordinates of the navigation receiver. Note that the values of the signal-to-noise ratio exceeding 5...6 are not random.

Table 1 – The adaptive beamforming towards the spoofer and the NSs in addition to the NSs' SNR

№ of Processing	Gain, dBi, to spoofer	Gain, dB/ SNR, to NSs								Error, m
		1	2	3	4	5	6	7	8	
1	< –40	1,6 / 41	2,1 / 58	0,6 / 27	0,1 / 6	1,2 / 1,1	0,01 / 0,3	1,2 / 0,3	0,01 / 1,1	52
2	< –40	1,1 / 32	1,1 / 31	0,4 / 20	0,1 / 8	1,9 / 42	0,03 / 1,6	0,6 / 10	0,02 / 4,8	37
3	< –40	1 / 35	1,4 / 54	0,5 / 14	0,1 / 1	1,9 / 68	0,04 / 1,0	1,0 / 27	0,01 / 0,5	66
4	< –40	1,3 / 47	1,1 / 34	0,6 / 29	0,1 / 6	1,5 / 54	0,04 / 7,0	0,4 / 0,9	0,01 / 1,4	129
5	< –40	0,8 / 32	1,3 / 47,4	0,4 / 25	0,07 / 4	1,9 / 1,9	0,03 / 0,7	1,3 / 31	0,01 / 1,6	10
6	< –40	1,5 / 60	1,4/ 34,8	0,6 / 8	0,04 / 4	1,2 / 0,2	0,03 / 1,7	1,2 / 3,1	0,01 / 1,8	36
7	< –40	1,6 / 46	1,9/ 58,9	0,7 / 21	0,1 / 8	1,2 / 2,4	0,02 / 1,2	0,8 / 0,1	0,01 / 0,9	54
8	< –40	1,4 / 47	1,6/ 40,1	0,8 / 35	0,07 / 4	1,3 / 23	0,04 / 1,9	0,1 / 0,3	0,01 / 1,5	84
9	< –40	1,2 / 29	1,3/ 48,9	0,6 / 21	0,09 / 1	1,6 / 2,6	0,03 / 1,8	0,8 / 0,3	0,01 / 1,3	22
10	< –40	1,5 / 42	1,3/ 42	0,5 / 15	0,1 / 9	1,4 / 0,2	0,03 / 0,7	0,7 / 1.4	0,01 / 0,7	80

The results in table 1 show that for all gain values of the adapted directivity towards the spoofer < -40 dBi; for 5-6 navigation satellites, the gain of the adapted antenna system is 1...1.5 with a typical SNR, but there are 2 NSs in the direction of which the gain is close to zero. This may be due to their close location to the direction of the source of spoofing, or may be a random result in digital diagram formation. The error is typical for 1 repetition for the NS signal.

The variable parameters of the algorithm for a given geometry of a multichannel receiving system are: the threshold value h_D for the selection of measurements of the phases of signals related to one direction and the number N_{T_0} of repetition periods of the navigation signal used in the selection. The threshold value h_D can be determined based on the assumption that the matrix elements D representing the differences in the signals' phases estimation will have a normal distribution with zero mathematical expectation and variance determined by the formula of potential measurement accuracy. Therefore, the threshold can be determined based on the probability of a random variable falling into a given interval, or, in a particular case, according to the "three sigma" rule.

With an increase in the number N_{T_0} of the navigation signal's repetition periods, the accuracy of the estimation of the correlation matrix by spoofing signals increases. This leads to an increase in the degree of suppression of spoofing signals and an increase in the signal-to-noise ratio due to a decrease in the norm of the vector of weighting coefficients [3] and a decrease in the power of internal noise after weight processing.

The total number of independent samples used in the evaluation of the interference correlation matrix is $N_{T_0} N_{ns}$, where N_{ns} is the number of navigation satellites for which spoofing signals are present. If the condition $N_{T_0} N_{ns} \geq 2N_{ar}$ is met, where N_{ar} is the number of elements in the array antenna system, the signal-to-noise loss will be less than 3 dB [4]. With a further increase in the number of counts used, losses are reduced. Therefore, at N_{ns} =5...6, it is enough to choose N_{T_0} =2...4. With the specified parameters, the detection of the spoofing signal and the adjustment of the weighting coefficients in the multichannel receiving system can be carried out periodically with an interval of 50 ... 100 ms. This will ensure timely detection of spoofing signals, including with the initial coincidence of true and false navigation signals by the delay time and a "smooth" change in the delay time and the Doppler shift of the false signal frequency [4,5].

Conclusion

To sum up, the concept of GNSS spoofing was highlighted shedding light on the problems that may be caused by such attack. After the progress and the implementation of the proposed anti-spoofing algorithm, the analysis is discussed and the results obtained revealing the validity of such algorithm in detecting and compensating the spoofing false signals with the receiving of only the navigation satellite ones. At the end, and may be in future work, such algorithm can be taken as a base from which we can launch towards an applicable anti-spoofing CNE hardware.

References

1. Parkinson B.W., Spilker Jr.J. Global Positioning System: Theory and Application. V.1 – Washington: American Institute of Aeronautics and Astronautics, 1996. – 793 p.
2. Interface Specification. Navstar GPS Space Segment. Navigation User Interfaces (IS-GPS-200) // Navstar GPS, 2004. – 207 p.
3. Reed I.S., Mallett J.D, Brennan L.E. Rapid convergence rate in adaptive arrays. IEEE Trans. Aerospace and Electronic Systems, Vol.10, № 6, 1974. – Pp. 853-863.
4. Ali Jafarnia-Jahromi, Ali Broumandan, John Nielsen, and Gérard Lachapelle. GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques // International Journal of Navigation and Observation, Volume 2012, Article ID 12707, 16p. doi:10.1155/2012/127072.
5. Yang Gao, Hong Li, Mingquan Lu, and Zhenming Feng. Intermediate Spoofing Strategies and Countermeasures // Tsinghua science ajnd technology, Volume 18, №6, 2013. – Pp. 599-605.