Testing of the Interference Immunity of the GNSS Receiver for UAVs and Drones

Tomáš Morong[1] and Pavel Kovář[2]
Czech Technical University, Prague, Czech Republic, 166 27

GNSS systems are susceptible to the radio interference despite they operate in a spread spectrum. This problem becomes critical in the field of general aviation, UAV, and drones. In addition, there is a wide range of commerce of jammers of power up to 2 watts that can block the receiver function at a distance of up to 15 kilometers in free space. The paper presents two original methods developed for testing of the GNSS receiver behavior and interference immunity. The first methodology is based on a 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 methodology is based on a software GNSS simulator and a signal processing in Matlab. The signal samples from the software GNSS simulator is combined with the interference generated in Matlab and the resulting signal is replayed by a software radio. In the frame of the research, two GNSS receivers suitable for UAV and drone navigation was tested for various jamming signals and scenarios. The results are not so optimistic as the jammer signal is propagated by the line of sight in most cases. The commercial jammer can block tested receivers on to the distance from kilometers to tens of kilometers.

Nomenclature

GNSS	=	Global Navigation Satelite System
GPS	=	Global Positioning System
UAV	=	Unmanned aerial vehicle
RF	=	Radio frequency
NMEA	=	National Marine Electronic Association
SDR	=	Software-defined radio
AGC	=	Automatic Gain Control
J/S	=	Jamming-to-Signal Ratio
C/No	=	Carrier-to-Noise-Density Ratio
FM	=	Frequency Modulation
LNA	=	Low Noise Amplifier
δ_E	=	East positioning error
δ_N	=	North positioning error
δ_U	=	Up positioning error

I. Introduction

GNSS gradually becomes the primary navigation system and currently, more and more applications are dependent on that. An important sector that consequently migrates from terrestrial navigation to GNSS is aviation. The primary optimism that becomes from large precision was replaced by the reality that the GNSS has insufficient reliability, problems with certification and relatively easy way, how to jam civil GNSS signals. Everyone can buy and illegally use a GNSS jammer to make impossible to track his track or for other illegal application. That is the reason why is necessary to investigate how to protect GNSS receivers against this type of radio interference.

This paper presents original methods for measurement of the GNSS receiver interference immunity. 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 basic essence of the designed methods is to create a testing signal which can be used for a reliable test of GNSS receivers. Furthermore is important a 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.

[1] PhD. student, Faculty of Electrical Engineering: CTU, Technická 2, 166 27 Praha 6
[2] Supervisor, Faculty of Electrical Engineering: CTU, Technická 2, 166 27 Praha 6

The signal of civil GNSS jammers and jammer range were characterized in Ref. 1. The 18 jammers were investigated. The typical jammer transmits wideband chirp or FM modulated signal by a triangular wave that bandwidth is wider than the GNSS signal in most cases. The paper determines the effective range of the GPS jammer. The tased method is based o combination of the signal of GPS jammer with the GPS generator. The combined signal is imputed by coaxial cable to the input connector of the receiver. The most of the available jammers have a wider bandwidth the civil signal L1 whose carrier frequency is 1575,42 MHz and the null-to-null bandwidth of a spread spectrum is approximately 2 MHz. The example of frequency sweep of the jam signal is in Fig. 1.

The other approach of GNSS receiver testing is in Ref 2. The method is based on the software GNSS simulator, the expensive GNSS simulator is not needed. does not need expensive GNSS simulator. The samples of the test signal are then processed by the software GNSS receiver. The disadvantage of this method is that standard receiver with RF input cannot be tested based on the method discussed above we developed two original methods for GNSS receiver testing. The methods are described in the next paragraph. The third paragraph presents test results of two GNSS receivers. The next paragraph is Discussion and the last Conclusion.

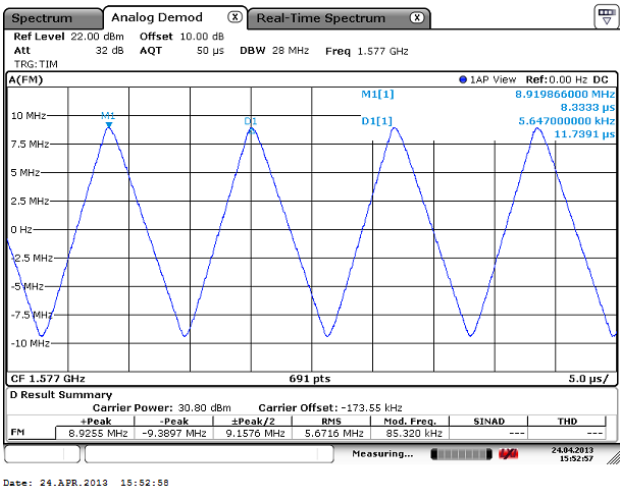

Figure 1. Signal of the jammer TG-5CA.

II. Receiver test methods

Based on Ref. 1, 2 we developed two test methods which are suitable for a quality assurance of GNSS receivers.

A. Classical method

The classical method was designed according to Ref. 1. The interference signal is generated either by the standard GNSS jammer (Fig. 3) that signal is attenuated to the required level by a step attenuator or by a vector signal generator that enables to generate any signal. For a generation of the simple jamming, the classical RF generator (Fig. 2) can be used.

Great care has to be taken to ensure that the exact power ration between the useful signal and the interference. Standard GNSS receiver is equipped with AGC circuits that adopt the gain of the receiver to the signal level from the antenna. The gain of the antennas LNA varies from 0 to 40 dB. This is why the jamming intensity must be express as a Jamming to Signal Ration J/S. The Jamming signal level without the knowledge of the level of the useful signal has no meaning.

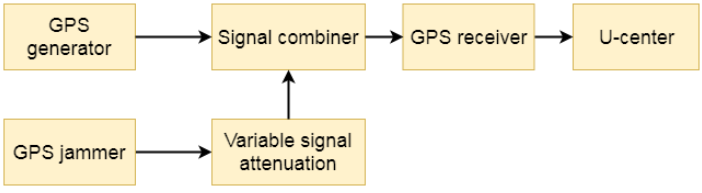

Figure 1. Block diagram of a testing procedure in the classical method

The goal of our research is to find out the threshold value of J/S for which the GPS receiver is not able to determine its position. This value is determined from the NMEA output of the receiver. We analyze the position error and 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 quality of a received signal.

Figure 3. Jammer TG-5CA

B. Software radio method

The software radio method is base on the generation of the test signal by software and replay of this signal by a software radio. This method is more effective than the classical method. The main advantages are:

1) The low cost of a software GNSS simulator
2) The repeatability of measurement
3) Usage any interfering signal

The setup of the software method is shown in Fig. 4. At first, we generated a GPS signal via a software GNSS simulator called ReGen GNSS simulator[7]. The software enables to set up the simulation parameters and trajectory of satellites. The output is in a binary file form. 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 HackRF One for replaying the test signal. The output of the SDR was directly connected to the input connector of the GPS receiver. The processing of the receiver measurement is done by the same method as in the first case.

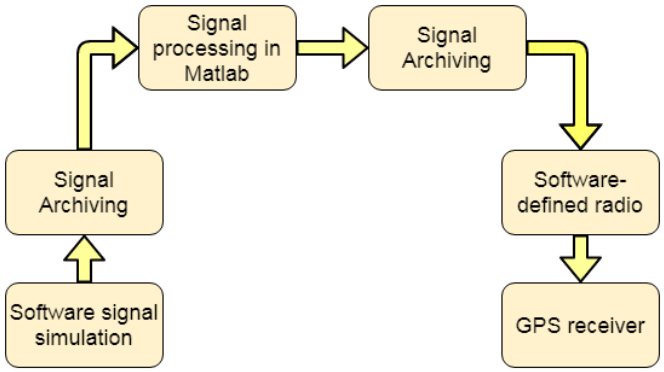

Figure 4: The setup of the software method

III. Results

This paragraph 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[6] that enables to analyze the receiver measurement and save data for further processing. The software simplifies a measurement processing and receiver performance determination.

The following paragraphs present test results for typical jamming signals. The receiver operation is investigated as an indicated signal to noise ration C/No as a function of the J/S value.

A. Frequency modulated sine jammer

The following two figures present the measurement results when the narrowband interference signal was used. The bandwidth of the frequency modulated sine signal was 320 kHz. Fig. 5 shows the measurement using a classical method and Fig. 6 shows the measurement using a software method. The key parameter is the critical value of J/S (Table 1) when receivers do not work accurately. The critical values determined by both methods are nearly the same.

The difference is in the rank of the measurement uncertainty. This observation confirms the credibility of the research and the correct implementation of both methods.

When we compare both receivers, we observed the EVK-MT8 is a little more immune than EVK-6H one. We also determined a position error for critical J/S (Table 2).

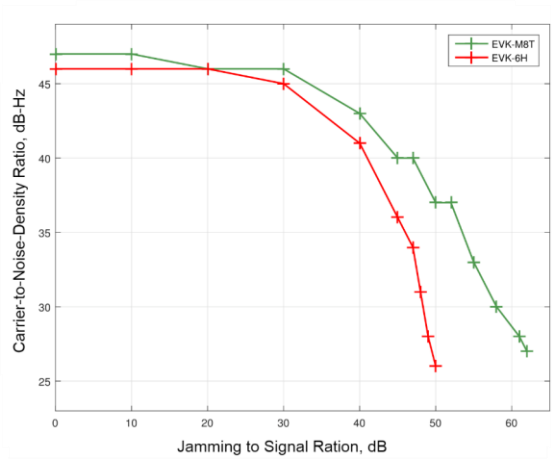

Figure 5: Classical method – frequency modulated sine jammer

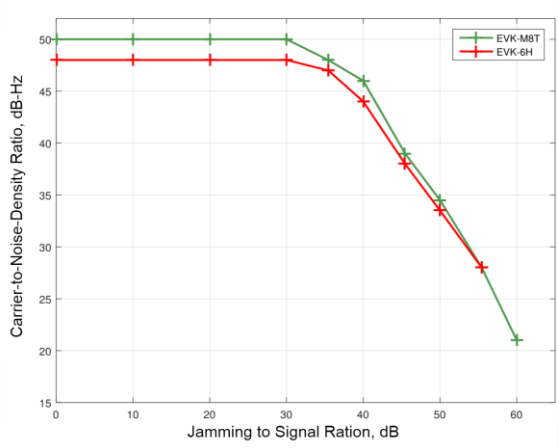

Figure 6: Software method – frequency modulated sine jammer

Table 1: Results - The narrowband interference signal and maximum positiong error

	Classical method		Software method		Maximum positiong error		
	C/No [dB-Hz]	Critical J/S [dB]	C/No [dB-Hz]	Critical J/S [dB]	δ_E [m]	δ_N [m]	δ_U [m]
EVK-6H	26	50	28	55	39.6	20.2	40.7
EVK-M8T	27	62	21	62	27.2	25.3	37.1

B. Chirp Jammer

The chirp jamming signal in a classical method was generated by a jammer TG-5CA (Fig. 3). The jamming signal power level is 32 dBm and the bandwidth of the signal is 18.5 MHz.

In software method, the chirp signal of bandwidth 6 MHz was simulated as the used SDR is featured with bandwidth is only 8 MHz. The results are shown in graphs and a Table 2. The results of the classical method are shown in Fig. 7 whereas the software method in Fig. 8.

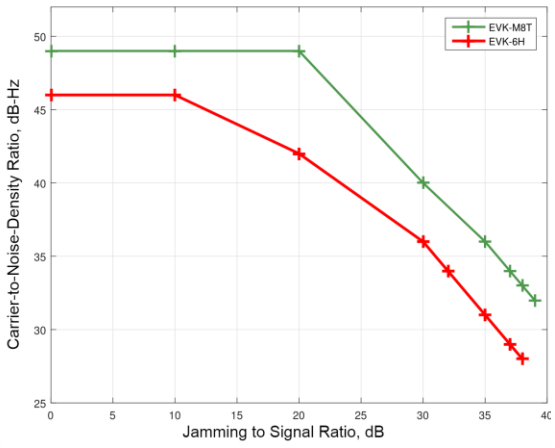

Figure 7: Classical method – Jamming: chirp signal from the jammer TG-5CA

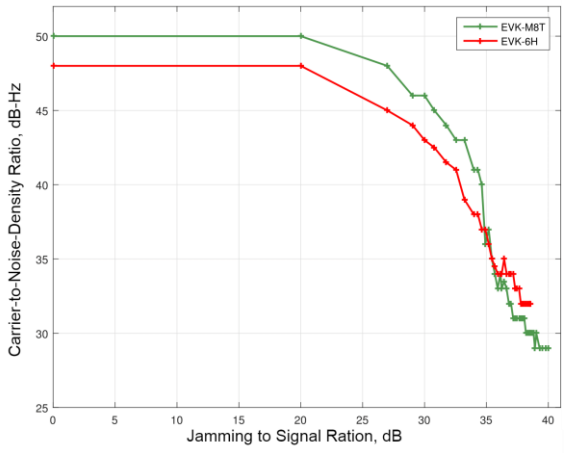

Figure 8: : Software method – Jamming: chirp signal

Table 2: Results - The wideband interference signal and maximum positiong error

	Classical method		Software method		Maximum positiong error		
	C/No [dB-Hz]	Critical J/S [dB]	C/No [dB-Hz]	Critical J/S [dB]	δ_E [m]	δ_N [m]	δ_U [m]
EVK-6H	28	38	32	37	7.1	6.8	9.1
EVK-M8T	32	39	30	39	2.9	5.3	3.6

C. Effective range of Jammer

The key parameter of the jammer or GNSS receiver user 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 free space propagation 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. The jammer effective range for interference signal power 32 dBm is in Table 3. The details can be found in Ref. 3.

Table 3: Results - Effective range of Jammer

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

IV. Discussion

In case of narrowband jamming, the critical values of J/S are between 50 dB and 62 dB. For the ideal chirp signal, the critical values of J/S have been considerably weaker and vary between 37 dB and 39 dB.

It is obvious that a narrowband interference signal must be transmitted with several times higher power than the wideband chirp jamming to jam the GNSS receiver. Respectively, if such signals were transmitted by a real jammer, its effective range would not be too large. This is the reason why the jammer manufactures use the wideband signals.

Although the signal jammer has to more powerful than GNSS signal the power of the interference signal can be low because the power of the useful signal is extremely weak. In a case, the jamming signal is propagated near the ground

it is complicated to jam GNSS signal because the jamming signal is attenuated due to buildings etc. On the other hand, an aircraft that usually flies high above the Earth, the jammer signal is effective by the free space loss only.

V. 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 21 dB-Hz to 28 dB-Hz for frequency modulated sine jammer. The maximal positioning errors have been in tens of meters.

The minimal values of C/No have been from 28 dB-Hz to 32 dB-Hz for chirp jammer. The maximal positioning errors have been in units of meters.

The future work will be focused on the investigation of the jammer signal in different outdoor, indoor environments including the aeronautical.

Acknowledgments

This research is supported by the grant Strategic infrastructure protective system detecting illegal acts intentionally affecting GNSS signals No. VI2VS/439 of Ministry of Interior of the Czech Republic

References

Electronic Publications

[1]Ryan, H, et al., "Innovation: Know Your Enemy: Signal Characteristics of Civil GPS Jammers". *GPS WORLD* [online],URL http://gpsworld.com/gnss-systeminnovation-know-your-enemy-12475/ [cited 10 March 2018].

[2]Alison Brown, Jarrett Redd, and Mark-Anthony Hutton, "Innovation: Simulating GPS Signals: It Doesn't Have to Be Expensive". *GPS WORLD* [online],URL http://gpsworld.com/simulating-gps-signals/ [cited 10 March 2018].

Books

[3] E. D. Kaplan and C. Hegarty, *Understanding GPS: principles and applications*, Artech House, Boston, 2006.

[4] B. R. Rao, *GPS/GNSS antennas*, Artech House, Norwood, 2012.

[5] P. Kovář, *Družicová navigace: od teorie k aplikacím v softwarovém přijímači, :* Česká technika - nakladatelství ČVUT, Prague, 2016.

Computer Software

[6]U-center, Ver. 8.21, U-blox, Thalwil, 2017.

[7]ReGen™ software for GNSS RF simulator, Ver. academic, iP-solutions, Tokyo, 2015.