ISSN: 1231-4005
e-ISSN: 2354-0133
ICID: 1130511
DOI: 10.5604/12314005.1130511

SUSCEPTIBILITY OF THE GPS NAVIGATION SYSTEM TO VARIOUS TYPES OF INTERFERENCES AND THREATS

Jarosław Sulkowski, Piotr Kowaleczko

C4ISR Systems Integration Division, Air Force Institute of Technology
Ksiecia Boleslawa Street 6, 01-494 Warsaw
tel.: 22 6851 304, 22 6851 620
e-mail: jaroslaw.sulkowski@itwl.plpiotr.kowaleczko@itwl.pl

Abstract

This paper is devoted to the problem of the GPS navigation system's susceptibility to various types of interferences and indicates in what way they may influence on navigation parameters. Basic principles of working of GPS receivers and possibilities of the influence on navigation parameters are discussed. Main advantages and disadvantages of using the navigation systems are indicated.

In particular, moments of reception of satellites' signals in relation to the distance of a satellite, diagram presenting the generation process of a signal emitted by a satellite, spectrum of the interfering electromagnetic wave with constant frequency and amplitude, failure to identify location in the GPS receiver, results of the studies concerning the influence of interference with the wave having constant frequency and amplitude, results of the studies concerning the influence of interference with the wave having constant frequency and changing amplitude, spectrum of the interfering signal – constant narrow-band sweeping wave, GPS receiver's application after input of a real signal with correct identification of the location, GPS receiver's application after input of the simulated signal of the satellite are presented in the paper.

Keywords: *navigation systems, interferences, threats*

1. Introduction

Nowadays Global Navigation Satellite Systems (GNSS) play a very important role in many areas of the human activity. They make the drivers' life easier, enable engineers to perform precise measurements and to locate stolen objects as well as make it easier to conduct military operations by troops. At the same time many problems arise which have to be resolved. These problems include among others:

- assessment of the influence of the mass use of GNSS on the functioning of transportation,
- indication of constraints regarding the usage of the currently applied GNSS,
- assessment of the safety of the GNSS use;

The last one is of key importance. A vast part of this paper will be devoted to this particular issue. The initial part of the paper contains a general description of the functioning of the Global Navigation Satellite System and constitutes a background for analyses concerning issues connected with GNSS resistance/susceptibility to interferences.

The paper is based on studies conducted at Air Force Institute of Technology, which concern the GPS navigation system.

2. Mechanism Of Functioning of the GPS System

2.1 Components of the GPS system

The GPS system consists of three basic components: user component – GPS receivers giving location, navigation parameters and time (PNT), space component – set of 31 satellites placed in 6 orbits and control component – monitoring and control stations. Identification of the location of a receiver is based on the measurement of the propagation time of the received signals, which are transmitted by particular satellites. It is schematically shown in Fig. 1.

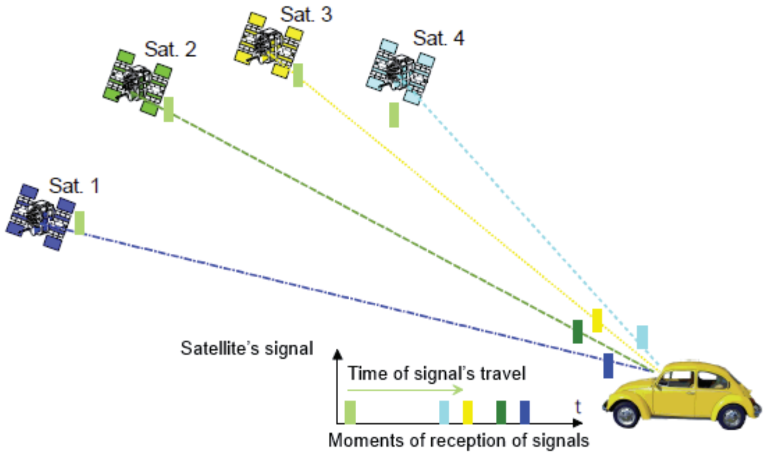


Fig. 1. Moments of reception of satellites' signals in relation to the distance of a satellite [1]

2.2 Identification of the receiver's location

Knowing the unique code of each satellite contained in the signal emitted by it and the times of reception of particular signals, we are able to determine the distances between a receiver and any particular satellite. Signal of each satellite contains a full set of navigation data regarding all satellites. The reception of these data from a single satellite takes 12.5 minute. In practice, this time is significantly shortened due to the fact that a receiver gathers data from a few satellites at the same time.

On the basis of the known location of satellites in a given moment and measurement of distances between the satellites and the receiver, the location of the receiver on the Earth's surface is calculated. The calculation consists in solving a system of linear equations. The receiver's location is usually given in form of longitude, latitude and height above sea level.

Currently used receivers are usually equipped with digital maps, so as to deliver to the user, apart from geographical coordinates, additional information concerning some points of reference (roads, buildings etc.).

Identification of the receiver's location is possible only when signals from at least three satellites are received. In this case, it is possible to determine longitude and latitude of the receiver. If we want to know the height above sea level, then we have to receive signals from at least four satellites.

2.3 Identification of a satellite

In order to ensure the possibility to determine the identification number of a particular satellite on the basis of the received signal, the two-state modulation of phase-shift keying of carrier wave with an especially prepared PRN (Pseudo Random Noise) modulating code is used. This code is called C/A code for the standard service delivered by the GPS system. The frequency of C/A code's bit generation is 1.023 MHz with repetition period equal to 1023. Each satellite has its unique code sequence. Codes for different satellites are generated in a very similar way, but the C/A codes of particular satellites vary significantly. It results from the necessity for unambiguously identify a satellite on the basis of the received code, which is performed by correlation systems comparing the received codes with the model ones (stored in a memory or generated by a receiver). If two C/A code sequences identifying satellites were correlated, then the correlation with models of C/A codes of a receiver would reach a very high value, which would hinder unambiguous identification of a satellite. The generated satellite's code (after adding of the navigation information to it) is used for the purpose of modulation of the L1 carrier frequency (1575.42 MHz) of the GPS system. The signal prepared in this way is sent by satellite's transmitters. The way of signal's generation is depicted in Fig. 2.

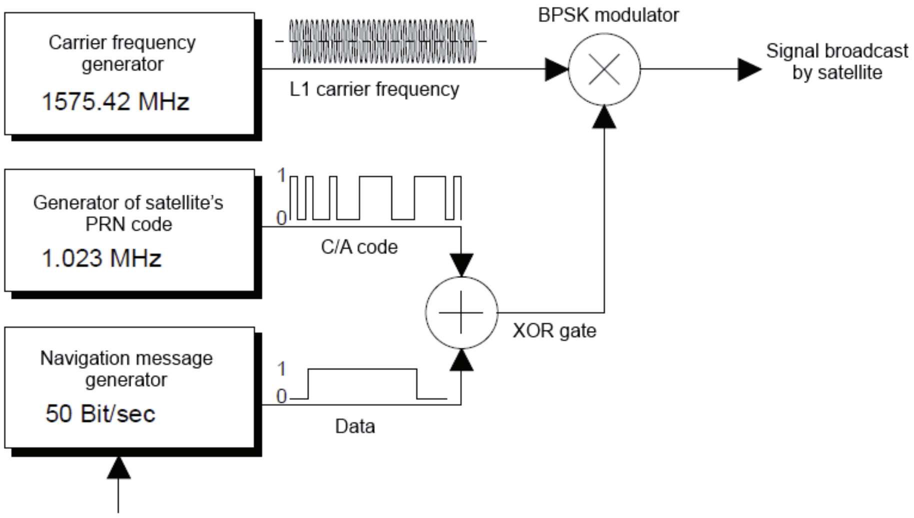

Carrier frequency generator
1575.42 MHz
L1 carrier frequency
BPSK modulator
Signal broadcast by satellite
Generator of satellite's PRN code
1.023 MHz
1
0
C/A code
XOR gate
Navigation message generator
50 Bit/sec
1
0
Data

Fig. 2. Diagram presenting the generation process of a signal emitted by a satellite [1]

From the above described principles of functioning of the GPS system potential ways of interfering of this system directly results.

3. Possible Ways of Interfering the GPS System

Interfering of the GPS system consists in making it impossible for a receiver to properly identify its own location. It is possible through manipulations in signals coming to a receiver.

Two basic methods of interfering receivers are widespread. These are jamming and spoofing. The purpose of this kind of actions may be to make any identification of location impossible (jamming) or to falsify information in such a way that coordinates are determined in a wrong way (spoofing). In the following part of this paper, descriptions of these two methods will be discussed.

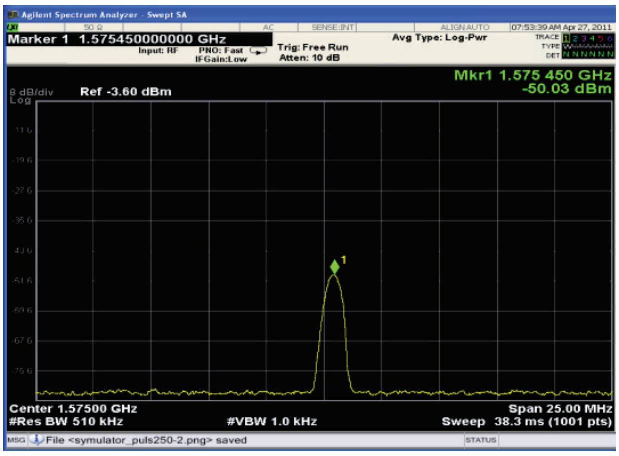
3.1. Jamming

The purpose of jamming is to interrupt the availability of a signal coming to a receiver. This type of interference may cause damage to a receiver, although its primary aim is to make decoding of any GPS signal by a receiver impossible.

The simplest method of jamming is to emit electromagnetic wave on the L1 carrier frequency (1575.42 MHz) towards a GPS receiver. The conducted studies indicate that the key factor of this method is whether the emitted interferences have constant or pulse character and whether the frequency of the interfering wave remains constant, or it slightly differs in time. The following cases were analysed.

3.1.1. Constant interferences by constant frequency

In this case, the receiver shows quite high resistance against interferences. It is consistent with both the technical specification of the system and theoretical analyses. Narrow-band interferences with constant frequency and amplitude are successfully suppressed by the receiver up to the level of 40 dB of the signal/noise ratio. The studies were conducted with the use of a signal generator (source of interfering signal) and simulator of GPS satellites' constellation (source of satellites' signals). Spectrum of the interfering signal, window of the receiver's application showing its improper work and results of the studies are presented in Fig. 3 and 4 and in Tab. 1, respectively.



Agilent Spectrum Analyzer - Swept SA
Marker 1 1.575450000000 GHz
Input: RF
PNO: Fast
IFGain:Low
Trig: Free Run
Atten: 10 dB
Avg Type: Log-Pwr
07:53:39 AM Apr 27, 2011
Mkr1 1.575 450 GHz
-50.03 dBm
8 dB/div Ref -3.60 dBm
Center 1.57500 GHz
#Res BW 510 kHz
#VBW 1.0 kHz
Span 25.00 MHz
Sweep 38.3 ms (1001 pts)
File <symulator_puls250-2.png> saved

Fig. 3. Spectrum of the interfering electromagnetic wave (constant frequency and amplitude)

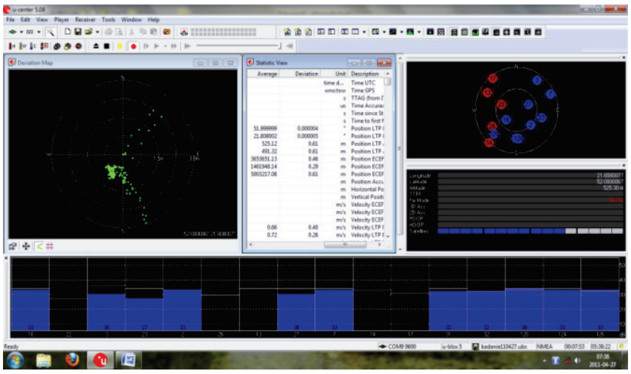


Fig. 4. Failure to identify location in the GPS receiver (blue columns – signal/noise ratio for particular satellites)

Tab. 1. Results of the studies concerning the influence of interference with the wave having constant frequency and amplitude

Interference / signal power ratio [dB]	Number of measurements	Number of identified 3D locations	Standard deviation of changes of signal/noise ratio of the received satellites [dBHz]	Percentage value of location identifications in relation to the number of measurements [%]
18	142	142	0.15	100
28	64	64	0.24	100
38	64	64	0.28	100
48	91	0	0.8	0

3.1.2. Pulse interferences by constant frequency

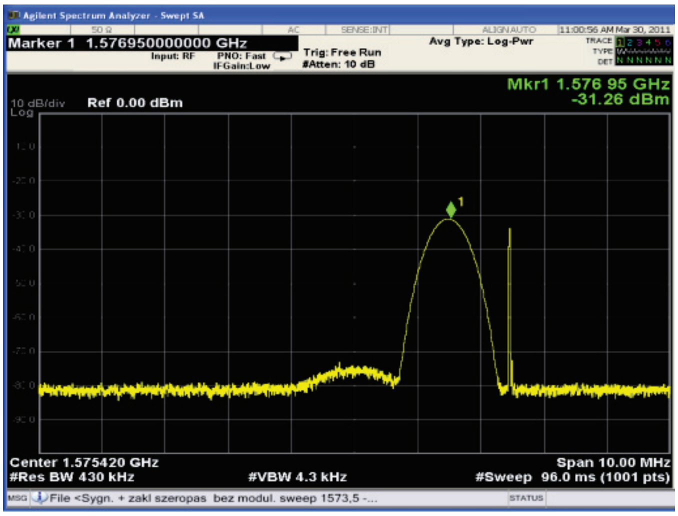
In the case that interfering signal is represented by the wave having constant frequency and amplitude changing in time (one hundred percent amplitude symmetrical impulse modulation), both the time needed for causing disturbance of its proper work and the energy needed for it are lower. The receiver's work is interrupted by the ratio of power of the interfering signal to the power of useful signal, which is higher than ca. 30 dB. It is confirmed by the results contained in Tab. 2. What's more, the device's work under interfering conditions is unstable, variable in time with the tendency to get worse (constant loosing of the possibility to identify location) as the time of exposure to the interference arises.

Tab. 2. Results of the studies concerning the influence of interference with the wave having constant frequency and changing amplitude

Duration of signal impulse [ms]	Interference / signal power ratio [dB]	Number of measurements	Number of identified 3D locations	Standard deviation of changes of signal/noise ratio of the received satellites [dBHz]	Percentage value of location identifications in relation to the number of measurements [%]
250	8	122	122	2.36	100
250	18	120	120	3.25	100
250	28	233	233	4.28	100
250	38	646	476	4.82	74
250	48	145	0	6.33	0
50	38	108	85	2.77	79
75	38	395	302	4.07	76
100	38	393	341	2.82	87
150	38	503	298	5.22	59
200	38	122	29	6.89	24
250	38	215	52	2.35	24
257	38	921	441	7.78	48
300	38	340	264	7.92	78
500	38	464	238	5.49	51

3.1.3. Pulse interferences by changing frequency

The third type of the studies conducted by the authors concerned the influence of GPS signal's interference with the use of constant narrow-band sweeping wave (with changing centre frequency). The sweeping took place in a stepping manner with sweeping time amounting to 100 ms within the range of 1573-1577 MHz. The spectrum of the interfering signal is presented in Fig. 5.



Agilent Spectrum Analyzer - Swept SA

50 Ω AC SENSE:INT ALIGN AUTO 11:00:56 AM Mar 30, 2011

Marker 1 1.576950000000 GHz

Input: RF PNO: Fast IFGain:Low Trig: Free Run #Atten: 10 dB

Avg Type: Log-Pwr

Mkr1 1.576 95 GHz -31.26 dBm

10 dB/div Log Ref 0.00 dBm

Center 1.575420 GHz

#Res BW 430 kHz

#VBW 4.3 kHz

Span 10.00 MHz

#Sweep 96.0 ms (1001 pts)

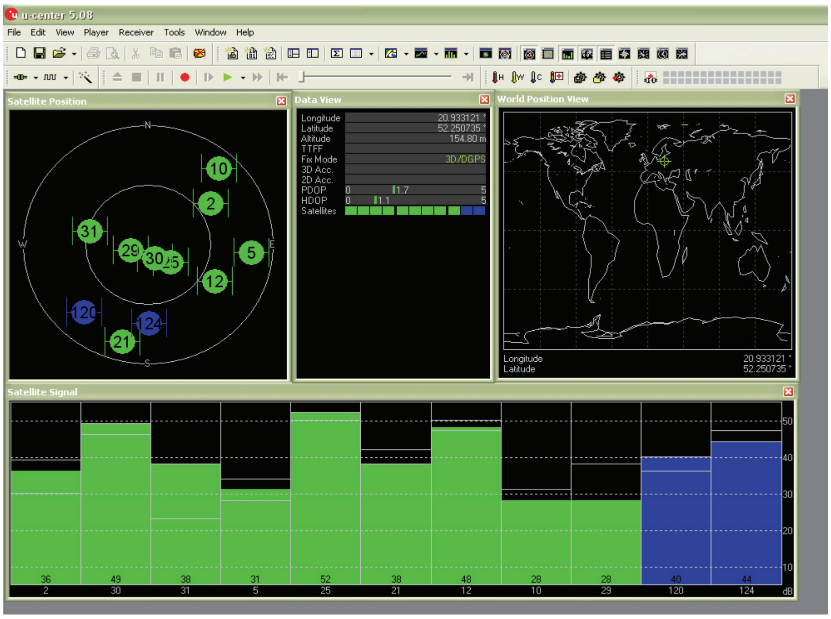
MSG File <Sygn. + zakl szeropas bez modul. sweep 1573,5 -...

STATUS

Fig. 5. Spectrum of the interfering signal – constant narrow-band sweeping wave

Switching on an external source of interferences caused rapid change of the working receiver's parameters. This change caused a stepwise change of the signal/noise ratio determined by the receiver at the beginning of working of the interferences, and subsequently the loss of the possibility to track signals from satellites, and in the end there was a lack of reception of signals from the previously tracked satellites. The information about the satellites located within the line-of-sight, as well as the last location of the receiver, were still stored by the receiver. The lack of reception of signals from the satellites made it impossible to identify the receiver's own position. The lack of reception of the satellites was constant during the work of the external source of interferences.

The studies conducted by the authors [2] revealed that there is also a quite effective method of jamming which bases on falsifying signals broadcast by satellites. It consists in generating a C/A code that is suitable for the simulated satellite. It was possible, since the whole technical documentation concerning the way of generating codes is commonly available. By the process of generating, it was decided to use the FPGA programmable structures due to their relatively simple structure (in comparison to other microcontrollers) and big capabilities in the scope of generating code sequences. Navigation information (message) is added to the generated bits of C/A code. It enables the receiver to receive data concerning ephemerides and almanacs of orbits, ionospheric corrections and exact times/corrections of clocks. The sequence of bits prepared in this way is subsequently input in the BPSK modulator, which modules the signal with it (L1 carrier frequency – 1575.42 MHz). The signal prepared in this way was input in the GPS receiver for the purpose of checking whether the device recognizes a specific satellite. Figure 6 depicts the functioning of the GPS receiver's application in the case of a real signal delivered to the receiver, and Fig. 7 presents the same situation for the simulated signal.



Longitude 20.933121 °
Latitude 52.250735 °
Altitude 154.80 m
TTFF
Fix Mode 3D/DGPS
3D Acc.
2D Acc.
PDOP 0 1.7 5
HDOP 0 1.1 5
Satellites

Longitude 20.933121 °
Latitude 52.250735 °

Fig. 6. GPS receiver's application after input of a real signal (correct identification of the location – green columns of the satellites' signals)

Each column is assigned to a particular satellite (number of the satellite under the column), its height provides us with the signal/noise power ratio, and the colour informs whether it is used for calculation of the location (green) or not (blue). It turned out that it is also possible to generate a few signals of particular satellites at the same time.

The signal generated in this way was subsequently transmitted to a directional antenna and directed to the receiver giving the location on the basis of the real signal. It turned out that the receiver's work was disturbed by the signal/noise power ratio of the interfering signal higher than the signal/noise power ratio of the real signal and the difference amounted to only 25-30 dBm. The system was stopping identifying the right location after ca. 30 seconds from the beginning of interfering. This time was shorter when more satellites were simulated, in particular when those satellites were simulated, which were really received by the receiver. The speed of disturbing the receiver's work is also directly proportional to the power of the interfering signal.

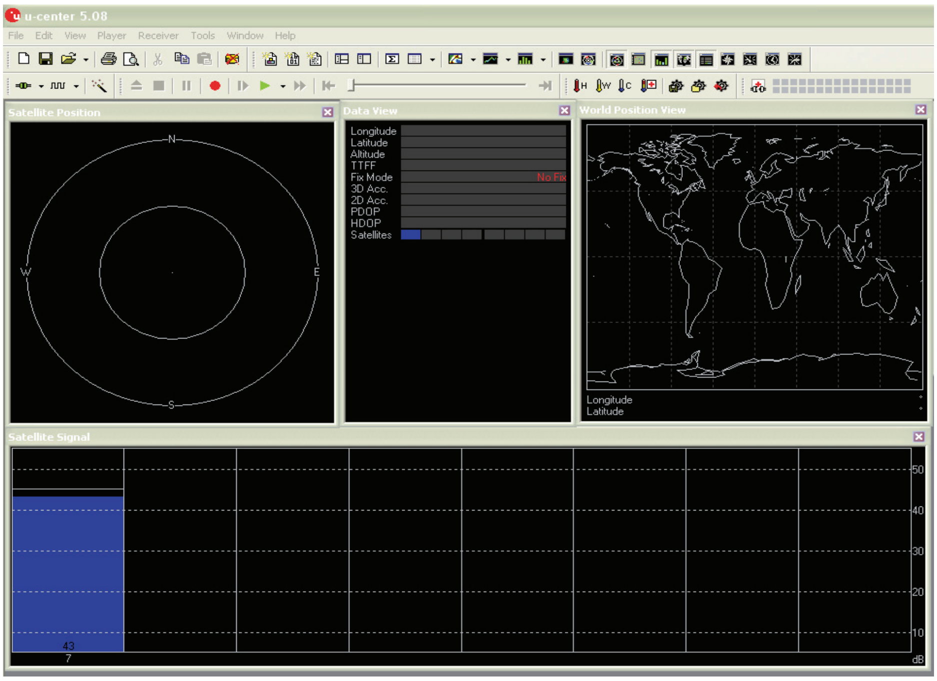


Fig. 7. GPS receiver's application after input of the simulated signal of the satellite no. 7

If signals of at least 4 satellites were generated (taking into account delays between them and changes of the carrier frequency resulting from Doppler frequencies), it would be possible to "transmit" false data to the receiver, which would cause wrong identification of location by it (spoofing), and not only a mere disturb of its work. The use of the generated C/A codes in the interfering signal enables to limit the minimum power of the interfering signal when compared to the interference using the signal of unmodulated narrow-band carrier wave with the L1 frequency.

3.2. Spoofing

In this type of interferences, the data compared in the process of GPS code replication are falsified, which causes incorrect identification of the receiver's location on their basis. We may distinguish three types of actions having the aim to diminish the precision and quality of the received location:

- program spoofing of the code – so-called malware is installed in the receiver's software, which causes incorrect identification of location. What is more, it is possible that the receiver does not show any signs of malfunction,
- differential corrections spoofing – the corrections signals sent in differential systems are spoofed. It is not particularly dangerous, since the corrections adjust the identified location from 1 to 3 meters, so possible interferences might cause distortions only in this scope,
- spoofing of signals transmitted by satellites. The receiver receives especially prepared, spoofed signals, interprets them as real and identifies incorrect location.

This type of interferences are better than jamming from the attacker's point of view, since it is possible to disturb the receiver's regular work with the use of significantly lower amount of energy. Additionally, in contrast to jamming, which is easily detectable, the receiver's user may not be able to state that the device is interfered.

A number of studies concerning the possibility of interfere a receiver with signals generated by the GPS constellation simulator were conducted [3]. It was revealed that a receiver working on a real signal, after introducing interferences from a simulator that are higher than just ca. 10 dB, stops working stably and after a while it takes over spoofed signals and gives false location to the user. The higher is the difference in the level of signals (real – interfering), the faster is the process of taking over the false data. However, the condition for successful interfering is the necessity to send signals for the satellites that are visible just before the beginning of interfering. Thus, it is not possible to spoof signals in such a way that e.g. a receiver working in Poland identifies location in e.g. Australia under the influence of an attack.

4. Threats Resulting From The Usage Of GPS Systems In Transportation

Navigation satellite systems are nowadays one of the bases of functioning of the transportation sector. They mark out the optimal route, direct drivers through it and inform them about possible traffic problems, which make drivers' work easier and more efficient. It is possible for precisely indicate where and when a given vehicle was, thus we are able to specify when we may expect a product to be delivered to an addressee. Navigation systems are of particular importance in the case of sea and air transport, in which they are the basic device to mark out the route.

Another possibility offered to the transportation sector by GPS systems is that they are able to locate a stolen vehicle or a commodity. A transmitter installed in them determines their location by the use of the GPS module, and sends it (e.g. through the GSM network) to a monitoring centre. Thus, the object may be quite quickly regained. The condition is that the device has the possibility to receive the signal and send data to the centre. If persons stealing the object are aware of the existence of the transmitter, they may secure themselves against being tracked down through physical cutting off the possibility of communication e.g. by placing the vehicle in a container that makes it impossible to receive GPS signal or simple disassembly of the device. The ways of jamming described above consist a quite serious threat by the standard use of navigation systems.

Simple jamming of a GPS signal may be caused by intentional acting (e.g. competition's activity) or accidental interferences broadcast by, for instance, mechanical devices located near power plants etc. We should bear in mind that this kind of interferences may even lead to the complete lack of possibility to determine the location (according to the results of the studies described above). This may in turn mean a necessity to change the route (which in the case of sea and air transport may even cause a disaster) or a lack of the possibility to locate a vehicle in a base. Jamming may also put a shipper at a risk of additional costs if navigation systems are used in terminals to locate objects. It may come to a situation when e.g. a crane transports wrong container onto a ship.

Spoofing is far more dangerous. While simple jamming is instantly visible for the user (lack of stable work), skilful spoofing is in practice undetectable. The receiver shows a correctly calculated location on the basis of the data delivered to it. In the case of transportation, it is thus possible to give spoofed signal to a vehicle carrying precious commodities, directing it in an arranged place and robbing it. It is also possible to significantly delay uncovering of the robbery by a monitoring centre through sending a suitably prepared signal to the receiver. While the commodities are stolen, the receiver calculates and transmits locations consistent with the established route to the monitoring centre. As a result, uncovering of the robbery will not be possible. However, the probability that criminals will use this type of solutions is rather low due to a very high cost of interfering devices and their level of complexity.

The type of the used receiver has very high influence on the possibility of causing interferences. The level of interferences that is sufficient to cause disturbance in one device may prove to be insufficient to cause disturbance in another one.

5. Conclusion

On the basis of the conducted studies, it was stated that interfering of GPS receivers might cause quite serious danger to navigation systems used in transportation. While it is difficult to use spoofing, which is far more dangerous, simple jamming methods may be used by unauthorized persons at relatively low cost and cause severe losses to shippers. The type of the used receiver plays a very important role in the resistance against interferences. It drives us to the conclusion that when we use navigation systems in transportation we should not trust them completely. They should not be the only system aiding the functioning of this industry branch.

References

[1] Joint publication: GPS Essentials of Satellite Navigation Compendium, u-box AG, 2009.

[2] Joint publication: *Opracowanie technologii zagłuszania i przeciwdziałania celowym zakłóceniom systemów nawigacji satelitarnej GNSS*, ITWL, 2011.

[3] Joint publication: *Wpływ spoofing'u na poprawność określania pozycji przez odbiornik GPS*, ITWL, 2010.