ZESZYTY NAUKOWE AKADEMII MARYNARKI WOJENNEJ
ROK LIII NR 4 (191) 2012

Ryszard J. Katulski
Jarosław Magiera
Agnieszka Studańska
Politechnika Gdańska

DEVICE FOR SPOOFING IN GLOBAL POSITIONING SYSTEM

ABSTRACT

This article describes the device which may be used to generate false GPS signals and emit them into radio communication channel. Such attack is called GPS spoofing. Each GPS receiver which remains in the range of a spoofing device (called spoofer) indicates time and position coordinates which are predetermined by the spoofer's operator. Spoofing may be used e.g. in order to disable the terrorist group from obtaining correct navigation information. The article presents the structure of realized jamming station, which is capable of generating false GPS signals. Specific elements of this station are characterized. Moreover, the article shows the results of spoofing performance tests, which were conducted in field conditions.

Keywords:
radio communication channel, false GPS signals, jamming station, spoofing.

INTRODUCTION

Global Positioning System is the most common system used in navigation. Its satellites emit two types of signals. First, P(Y), is intended for military use, as it is multiplied with pseudorandom sequence which is known only to limited number of authorized users. Second, C/A, is generally accessible, however it gives worse accuracy of position estimation. Popular civilian GPS receivers demodulate C/A signals.

Navigation data structure, as well as pseudorandom spreading codes' sequences are widely known. There is no encryption applied to transmitted data, which makes it possible to prepare a composition of false signals in order to force the estimation of desired position, velocity or timing (PVT) information.

Such activity is called GPS spoofing. It is performed through emission of false signals towards target receiver or omnidirectionally. Signal is emitted by device called GPS spoofer. Spoofing signal, in point of reception, must be stronger than signal arriving from satellites, so that the receiver locks only on the former.

GPS spoofing may be used, for example in anti-terrorist actions in order to mislead or disable positioning service for terrorists. However, spoofer should be used with caution, as it may affect unintended targets. Sometimes even critical infrastructure takes advantage of civilian GPS signals, for example to provide precise timing in telecommunication networks. Results of failures caused by spoofing may be severe.

SPOOFING DEVICE

GPS spoofing signal generator was developed by authors of this article in Department of Radiocommunication Systems and Networks at Gdańsk University of Technology. It has a form of GPS constellation simulator [1, 2] and was built in order to investigate the influence of spoofing on GPS receivers available on the market. It consists of four main units which are: Parameter Computation Unit, Data Flow Control Unit, Signal Formation Unit and Modulation Unit. Scheme of communication between these units is shown in figure 1.

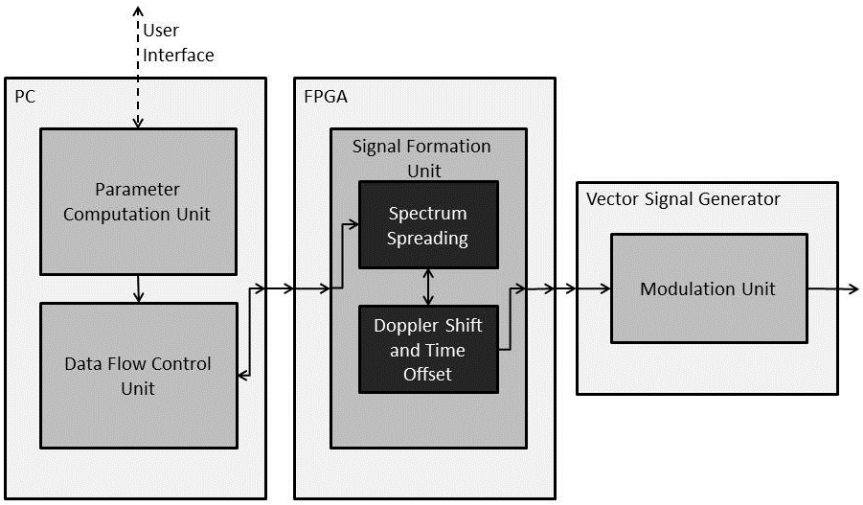

Fig. 1. Interaction between spoofer's modules

Source: own study.

Main logic of the spoofer is implemented in Parameter Computation Unit (PCU). It is implemented in software as an application run on a PC computer. Navigation data sequences, as well as Doppler shifts and relative delays between signals from different satellites are computed by this unit. Operator of the spoofing device specifies the parameters such as: desired time and position coordinates, minimum elevation of satellites above the horizon, satellites' numbers. Basing on these information and proper almanac, desired data and parameters are obtained. Almanac is a set of information which is needed to estimate the positions of the satellites in certain moment of time. Operator must provide the almanac in form of a text file in one of two popular formats: YUMA or Trimble Planning. Reference time of the almanac should be close to desired time, in order to estimate the satellites' positions close to the real ones.

Navigation data sequences are generated according to message structures published in [4]. This document also specifies the equations which are used to determine the positions of satellites, basing on the parameters contained in almanac. Relative delays and Doppler shifts of signals are calculated basing on initial values and change rates of pseudoranges between satellites positions and the desired position.

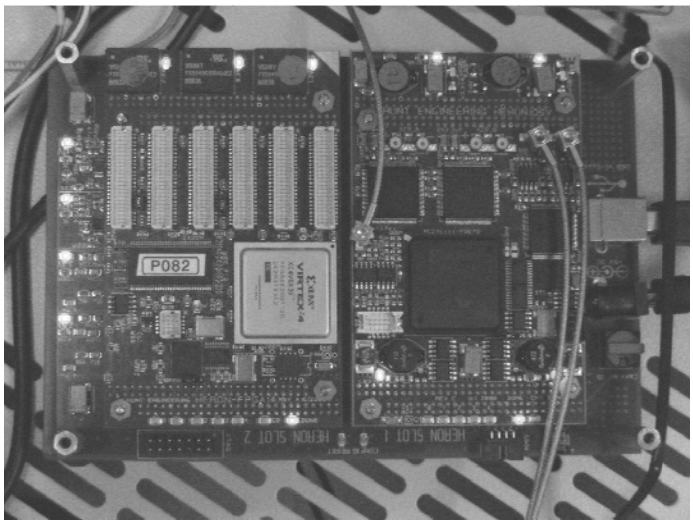

Fig. 2. FPGA modules of Signal Formation Unit

Source: own study.

Data and parameters computed in PCU are next transmitted to Signal Formation Unit (SFU). It consists of two FPGA modules by Hunt Engineering [3] which are mounted on common carrier board. SFU is presented in figure 2.

First of the modules performs spreading of the data with the pseudorandom codes, which are previously stored in the RAM memory. Spread binary sequences along with Doppler shifts and relative delays are forwarded to the second module of SFU.

FPGA chip in the second module inserts given delays and changes the bitrates of spread sequences in order to include the code Doppler shifts. Carrier Doppler shifts are included by multiplication of bipolar spread sequences with samples of cosine and sine waveforms of frequency equal to Doppler shift.

Data transfer from Parameter Computation Unit to Signal formation Unit is realized using USB interface and is maintained by Data Flow Control Unit (DFCU). Data are sent to SFU until its input buffers are almost full. In such case, SFU sets the flags which are periodically read by DFCU. If flags are set, DFCU pauses the transmission until data is read from buffers and the flags go off. Similar transmission control scheme is applied between FPGA modules.

Composite waveforms at the output of second FPGA are converted to analog form. They drive the Modulation Unit (MU) which upconverts the baseband signal to GPS L1 frequency of 1575,42 MHz. Function of analogue quadrature amplitude modulator is realized by Rohde & Schwarz SMU200A vector signal generator.

Signal power at the output of the generator is sufficient to perform spoofing when GPS receiver is a few meters away from spoofer. In order to perform spoofing on longer distance, additional power amplifier is needed. In presented configuration Amplifier Research 30S1G4 was used, which allows for emission with maximum rate of 30W.

FIELD RESEARCH

The spoofer, described previously, was tested in field conditions. During those measurements five GPS receivers were used:

— three different car GPS receiver;
— one geodetic GPS receiver;
— one USB GPS receiver.

Effort was made to collect a set of various types of receivers due to their different software applications and functions as well as hardware solutions implemented in them.

In table 1 results of two spoofing tests are shown. In both tests all the receivers were located in the same place and the spoofer's antenna was placed 40 meters

from them in line of sight. In the first test, the position imposed by the spoofer was 1.15 km away from the real one. In the second test the distance between true and false position was 89.19 km.

Table 1. Spoofing test results

Test number	1	2
Device	Position Error [m]	Position Error [m]
Car receiver 1	8	118
Geodetic receiver	5	104
Car receiver 2	5	1381
Car receiver 3	579	369
Usb receiver	40	77
Medium error [m]	127.4	409.8

Source: own study.

Results show that the precision of fake position estimated by receiver depends on the distance between the true one and imposed by the spoofer. To achieve more accurate position in spoofed receiver the spoofer's given location should not be far from actual one of the receiver.

It must be taken into consideration that in range of spoofing station all GPS receivers will show the same position given by the spoofer.

Research conducted in laboratory implies that the power of the spoofer is also very important to attain desired effect. Locally generated GPS signal, which power was –80 dBm and SNR = –10 dB, was delivered to GPS receiver. This signal was jammed by spoofer's signal. Time needed by receiver to acquire the spoofing signal and estimate the position was measured. After 20 correct signal acquisitions the power of spoofer was decreased by 1 dB. Figure 3 shows how many seconds it takes the target receiver to fully acquire spoofer's signals and compute the fake position, velocity and time at certain spoofing power relative to genuine signal reference power equal to -80dBm. As may be seen, if the spoofing to genuine signal power ratio is more than GPS processing gain (43dB), the time of spoofer's signal acquisition is about 45 seconds. Otherwise, it is much longer than one minute.

Similar measurement with 14 different receivers was also performed:

— one geodetic GPS receiver;
— one bicycle GPS receiver;
— five USB GPS receivers;
— seven car GPS receivers.

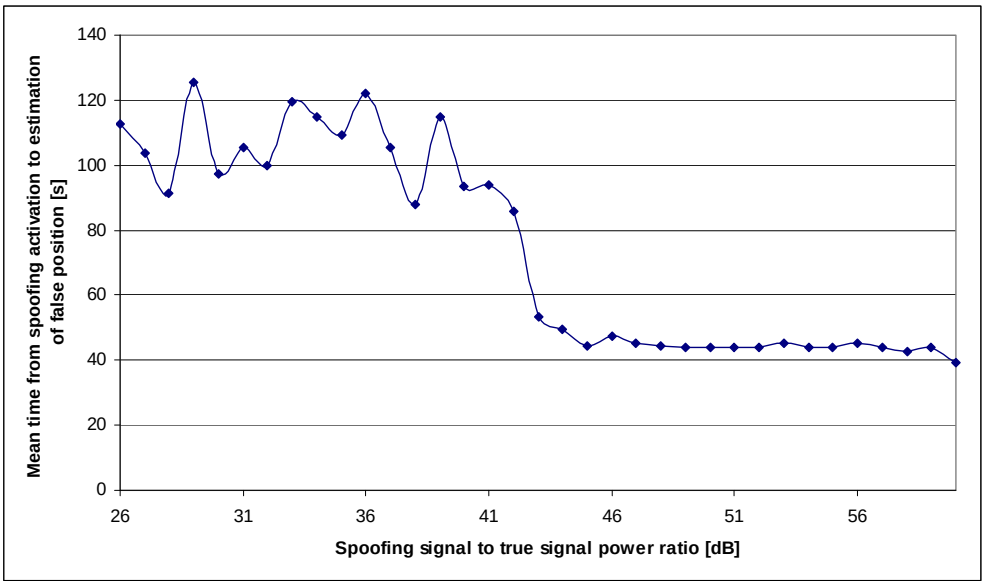

Fig. 3. Mean time of false position estimation as a function of relative spoofer's power

Source: own study.

These receivers vary in complexity, however spoofing attack is rarely aimed at specific type of receiver, thus such combination is allowed.

This time the jammed signal was the real one — obtained from satellites, amplified and repeated in laboratory. Spoofing station was not turned on until all the receivers acquired GPS signal and showed true position. During measurement only spoofers power was changed. In figure 4 measurement results are shown. Receivers reacted differently on the spoofers signal. Most of them showed the position imposed by the spoofer (blue colour). Some showed random position — neither the true one nor spoofer's (red colour). There were receivers which acted like only jammed ones, which means that they did not acquire spoofer's signal (violet colour). There were also receivers which seemed not to receive the spoofer signal at all (green colour) as they showed the true position all the time, however when power of spoofer was stronger than –26 dBm, the shown position did not fluctuate which means that those units did not work properly — were plugged.

As it might be seen in figure 4 if the spoofers power is lower than –26 dBm there was a number of receivers which managed to obtain the true position. If the power of spoofer was stronger than –26 dBm many receivers got plugged. It means that if the range of spoofer station will be vast, receivers in contiguity of this station will be plugged or only jammed.

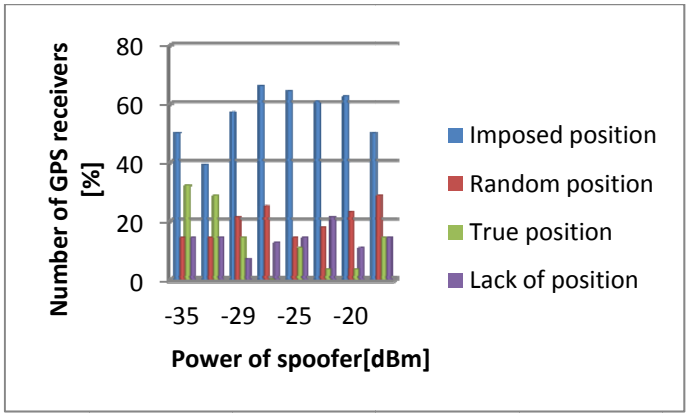

Fig. 4. Spoofing effectiveness in spoofer's power function

Source: own study.

CONCLUSION

GPS spoofing might be a useful instrument against terrorism. In presented article authors described operating spoofing station developed by them with employment of FPGA modules. Research made by authors shows that various GPS receivers act differently in presence of spoofing signal. Nevertheless, the estimation of true position is impossible if the strength of spoofer's signal is selected properly. Accuracy of imposed position may be increased by application of measurements made by local reference GPS receiver.

REFERENCES

[1] Abart C., *Simulating GNSS Constellations — GPS, Galileo and SBAS*, ELMAR, 50th International Symposium, 2008.

[2] Wang Y. et al., *Design and implementation of programmable multi-mode GNSS signal simulator*, Communication Technology (ICCT), 12th IEEE International Conference, 2010.

[3] http://hunteng.co.uk/info/fpga-dsp.htm.

[4] ICD-GPS-2000, Global Positioning System Interface Control Document, 2000.

URZĄDZENIE DO SPOOFINGU W SYSTEMIE GLOBALNEGO POZYCJONOWANIA

STRESZCZENIE

Artykuł poświęcono opisowi układu umożliwiającego wytwarzanie i wprowadzanie do kanału radiokomunikacyjnego fałszywych sygnałów systemu GPS. Atak tego typu jest nazywany spoofingiem GPS. Odbiornik GPS znajdujący się w zasięgu urządzenia emitującego takie sygnały (tzw. spoofera) wskazuje czas i współrzędne położenia odbiornika zadane przez operatora spoofera. Spoofing może zostać użyty na przykład w celu uniemożliwienia grupie terrorystycznej uzyskania poprawnej informacji nawigacyjnej. W artykule przedstawiono budowę zrealizowanej stacji zakłócającej umożliwiającej wytwarzanie fałszywych sygnałów nawigacyjnych GPS. Scharakteryzowane zostały poszczególne elementy tej stacji. Ponadto zaprezentowano wyniki wykonanych w warunkach terenowych testów efektywności spoofingu z użyciem opracowanego urządzenia.

Słowa kluczowe:

kanał radiokomunikacyjny, fałszywe sygnały system GPS, stacja zakłócająca, spoofing.