**THE ARCHIVES OF TRANSPORT** *ISSN (print):* *0866-9546*
*Volume 35, Issue 3, 2015* ***e-ISSN (online):*** *2300-8830*
***DOI:*** *10.5604/08669546.1185170*

# NEW THREAT TO GLOBAL TRANSPORT. GNSS RECEIVER SPOOFING

**Maciej Gucma**
Maritime University of Szczecin, Institute of Marine Traffic Engineering, Szczecin, Poland
e-mail: m.gucma@am.szczecin.pl

***Abstract:*** *Transport and logistics in XXI century relies on the several technical systems for assuring safe and reliable operations. One of widely used systems are satellite positioning systems, used to monitoring transport means and cargo itself. Reliability of the whole transport chain is often combined with singular reliability of satellite monitoring system. Possible threats to precise positioning of any vehicle is GNSS (Global Navigation Satellite System) deliberate interference. So called spoofing interference can mislead receiver in transport objective for reporting entirely wrong position and timing. To fight with this phenomena's antispoofing techniques are developed. This paper will provide a review of late researches in field of GNSS anti-spoofing on the side of receiver. GNSS receiver vulnerabilities for a spoofer (device) attack will be presented as well as anti-spoofing algorithms. Possible limitation, costs as well as countermeasures methods will be shown thoroughly. Some of recent trends in anti-spoofing techniques in the world will be outlined up to date.*

***Key words:*** *GNSS Receiver, signal spoofing Anti-Spoofing Technique*

## 1. Introduction

Among the great inventions in past century one is developing in high scale constantly for over 40 years. GNSS systems where GPS (Navstar Global Positioning System) administered by USA Government (not forgetting to mention Russian, EU and Chinese ones), plays significant role in almost every human activity. Economies are based now on precision timing sequences delivered from satellites moving on the Medium Earth Orbit (MEO) whilst receivers of the system are ground based tiny electronical devices. System delivers precise timing and positioning of the end user to mention transport on: large distances (air transport, waterborn transport), close areas transport (Koc and Specht, 2011) (railway, trucks), leisure transport, special means of transport etc. On the other hand electrical grids, digital communication, safety and rescue services are the most important affected by GNSS dependability users.

Signal generated by satellites with timing information is pretty low power reaching the globe ground. This situation makes it vulnerable to substituting by the other signal with unintentional information (i.e. spoofed). Whilst just high level of radiation will stop receiver to distinguish the useful signal (with enough SNR Signal To Noise ratio) so called jamming, spoofing is intentionally changing of transition to misled target user. On the other side is ease of decoding the signal and then encoding it with fake values of so called pseudoranges inside. All data are possible to be decoded because GNSS offers open standards (except Y code with is scrambled and used by military services only). Spoofing of signal is extremely dangerous for vital parts of logistic chains like large container vessel (often with over 10 thousand container on board) navigation in narrow passages, or aircrafts handlings tons of cargo and passengers in crowded airports.

Recent research conducted by UTH Texas (in 2014) was based on twin antenna spoofing detection on leisure boat (Psiaki et al. 2014a).

Paper investigates in possible ways of spoofing attack where only receiver side where especially processing layer and information layer is in interest of investigations. Primarily GNSS attack on receiver can be processed on different layers and using different methods. Scientists are defining new countermeasures i.e. detection and potentially mitigating faked GNSS signal. Researches performed in Maritime University Szczecin are concentrated in detection using twin antenna technique that offers fast and promising detection of any kind of intentional interference (Dobryakova et al., 2014). Another simple detection method presented in (Zalewski, 2014) is installation of satellite compass, where measurement of the carrier phase (on L1 frequency) is done by both receivers (GNSS compass has more than 1 built in combined receivers, usually 2 but there are systems with 3 antennas) with same oscillator correlated clock signal. Thus for Si satellite L1 carrier phase signal

$\Delta\varphi_i$ between two (or more) antennas is given as (Zalewski, 2014):

$$\Delta\varphi_i = D_{12}R_{ENU-B}L + n_i + \delta_b + \gamma_i \quad (1)$$

where:

$D_{12}$ – is a baseline between the antennas in units of L1 cycles

$R_{ENU-B}$ – is a rotation matrix of vectors from local metrics in frame coordinates East-North-Up (ENU)

L – is the unit of line of sight vector to $S_i$ in ENU frame

φ,λ – ellipsoidal coordinates for latitude and longitude

$n_i$ – integer ambiguity of wave period for Si

$\delta_b$ – line bias value

$\gamma_i$ – sum of all carrier phase errors

In such event detection of group changes in concurrent transmissions from one transmitter, thus where spoofing attack occurs, changes in $\Delta\varphi_i$ parameter might be monitored. Author (Zalewski, 2014) determines also another very simple parameter to be monitored – changes in true heading (in fact are changes in rotation matrix $R_{ENU-B}$ ) of the vessel or other transport device – such rapid transitions shall give to operator reason to become suspicious.

Seriousness of the problem has lead scientist from GPS Laboratory Stanford University to prepare some sort of test bed for detection of spoofer attack close to airports. This researches described in (Akos, 2012) are based on detection of AGC block monitoring of floor and noise level monitoring. Basic assumption for the level of incoming power, RF filter trigger and noise level is presented in fig. 1.

Problematics of the conducted researches is in field of transport and lies between telematics and devices of transport itself. Any attack that will lead to the disability of transport means is potentially:

- dangerous to life,
- has impact on environment,
- has large effect on economics of transport.

Methods of solving these threats are mainly the sophisticated electronics and researches conducted must lead to either understanding of spoofing process as well as potential mitigation of that kind of danger.

Methods that have been used here are mainly analytical ones for comparison of the existing and defined by all round the world scientists methods. Recently, some researches with the design of whole test bed, has been conducted in Maritime University of Szczecin. Apart from real methods simulation devices are used widely in defining the vulnerabilities.

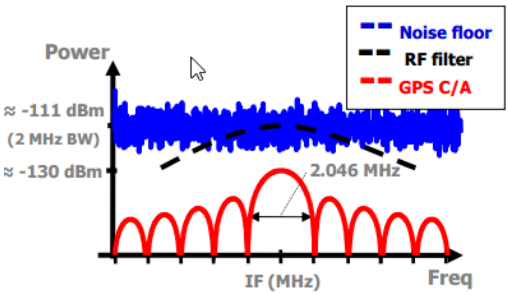


Fig. 1. Power monitoring of noise floor
*Source: Akos (2015).*

## 2. Vulnerability of GNSS against Spoofer Attack

Every GNSS receiver consist of (fig.2.):

- RF (Radio frequency) module,
- baseband signal processor,
- information processing subsystem – PVT (navigation information generation).

Purpose of the RF module is non code operation and its only amplification and converting signal (steeping down frequency and mixing it), thus it can be treated as 'dumb' module where no processing is done. Article will not cover its functionality.

For purposes of this article vulnerabilities of DSP block and PVT module will be described. Basically block of DSP is responsible for decoding PRN codes (pseudorandom noise number). In addition signal is much more complicated and comprises between others: PRN, signal bandwidth transmitter frequency, type of modulation, Doppler range and signal strength. All these values must be open kind to be able to use by different receivers. This makes GNSS signal particularly vulnerable to spoofing attack, where near located ground receiver can transmit much more powerful fake signal that will be received by target receiver.

During tracking signal by receiver, spoofer (i.e. person with device) can imply new signal laying close to the original one, and slowly start changing the original codes by ones provided for illegal operation. Thus spoofer will control the receiver and transportation device.

PVT module is also vulnerable to the external attack. This module uses extracted from signal values (like pseudorange) to determine and compute the positions in global system, velocities, altitudes, etc. PVT is working on slow changing data (in surface and airborn transport maximum velocities reach 800km/h), whilst structure of data is open and available to other receiver (in definition spoofer reads similar data as target). In the PVT module receiver proceeds RAIM (receiver autonomous integrity monitoring) that can detect abnormal events observing range residuals. Unfortunately when signal is fully faked (i.e. GNSS receiver listens only to spoofer) residual are too small to be detected as a fake signal. Spoofer usually changes residuals in PVT in constant and gradual manner not to be noticed.

Another issue is amount of data in the systems that are transmitted and then after processing can be processed. This factor is crucial for the speed of antispoofing software performance. Typical systems, their center frequencies, sample rates of transmission and bandwidths are presented in Tab. 1.

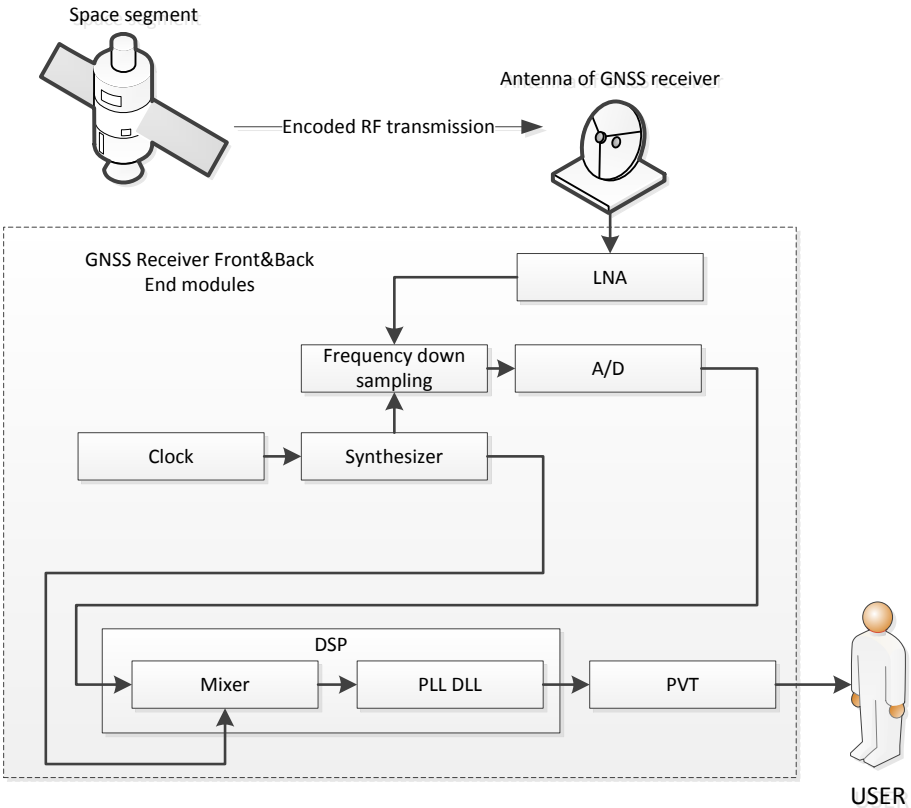


Fig. 2. Simple schematic of the GNSS Receiver (LNA- Low Noise Amplifier, DSP – digital signal processing block, PVT - information processing block, A/D Analog to digital conversion)

Table 1. Sample rates, center frequencies and bandwidths for all working GNSS constellations

| Constellation | Center frequencies (front-end number) | Sample rate/ Number of bits | Bandwidth |
|---|---|---|---|
| GPS | L1(1), L2(1),L5(1) | 20.48 MHz@2 bit | 15 MHz |
| GLONASS | G1(2), G2(2) | 20.48 MHz@2 bit | 15 MHz |
| Galileo | E1(1),E5a(1),E5b(1), E6(2) | 20.48 MHz@2 bit | 15 MHz |
| Compass | B1(2), B2(1),B3(1) | 20.48 MHz@2 bit | 15 MHz |
| SBAS | L1(1), L5(1) | 20.48 MHz@2 bit | 15 MHz |

## 3. Receiver on-board methods and techniques for detecting spoofer attack

One of the method for spoofing detection is changing the structure of GNSS itself and other is detection in real time or post processing on receiver side (on-board methods). Former cannot be implemented easily thus the latter will only be described in article. In the chapter several methods related to processing and PVT layer will be described. Post processing methods are particular useful for investigation issues and similar applications, where in transportation purposes i.e. planning and monitoring of the route this is secondary issue.

*Monitoring of CNR parameter*

Many GNSS receivers utilizesCNR (Carrier-to-noise ratio) measurement to determine signal quality. In non-attack conditions signal changes pretty smoothly (due to movement of SV and changes in environment). When spoofer starts to track signal and then transmit new, faked signal CNR will increase with non-standard manner. This shows spoofing interference (Dehghanian et al. 2012). In (Wen et al. 2005) it has been shown that there is correlation between antenna distance and CNR (with antenna separation up to 100 m CNR lowers about 22 dB). In such situation it might be spoofing situation.

*Multi antenna technique*

Using multi array antenna it is possible after some amount of time to detect if theoretical antenna is moving (thus is under attack of spoofer) (Montgomery et al. 2009). Other variant is to use only one antenna for measurement and other for detecting significant changes using variance analysis (Borio, 2013). It measures coherence between phases of spoofed PRN signal. Limitation is the noise level over 10 dB where lower values give poorer effects of detection. Last used method is to measure differential carrier (far simpler than phase coherence measurement) this method has been presented in (Psiaki et al. 2014a) and (Ochin, 2014). Another method is using synthetic array to detect phase changes.

*In-band Power Monitoring.*

Close (i.e. up to hundred meters) existence of working transmitter within band used by GNSS will imply to the level of in-band power. This factor is measured by auto gain controller (AGC) which will adjust gain level on receiver. AGC detection level requires pretty sophisticated receiver with analog output (can be A/D converted) of intermediate frequency (IF). Dedicated watch dog controls for abnormal (i.e. very high – around 2-3 dB) increase of AGC level (Akos, 2012). For receivers with digital IF output only this method will not function directly. Although work (Jafarnia-Jahromi et al. 2014) shows that initial pre – despreading of whole domain of AGC will work for it. So called Gold codes (binary sequence consisting of set of $2n-1$ sequences each one with a period of $2n-1$) are delayed and multiplied (DAM) that in result generates new Gold code. New sequence has all incidents power ranges of previous one and after next transformation (filtering low pass filter with triangle characteristic). Filter on the output detects existence of the spoofing although some other non-intentional interferences might be detected.

*Phase Rates Consistency Check*

For real, authentic SV transmitted signals, Doppler frequency along with the code rate are consistent in time domain. It happens due to the fact that both of these factor are affected by the relativity of satellite versus receiver movement. Having relation:

$$f_a = -f_{Rf}\tau_a \quad (2)$$

where:

$f_a$ – Doppler frequency

$\tau_a$ – code rate

$f_{Rf}$ – radio frequency of signal transmitted by SV

This relation can be used for spoofing detection, though such method is simple to be abused by spoofer knowing this phenomena.

*SQM Technique*

Signal Quality Monitoring (SQM) is very popular technique in GNSS quality monitoring where multipath interference can be an issue. Due to the fact that multipath is sort of the multipath (although with far higher multitude) this technique seems to be pretty suitable to detect spoofing. For detection of multipath and spoofing in SQM technique ratio and delta factors are measured to detect asymmetry of signal. This technique refers only to the ideal situation where no multipath occurs.

*Clock attack*

Clock data transmitted as pseudorange value (and then computed) must be coherent with all previously received data. This values are changing smoothly before the filter input, and in case of signal loss estimates of position are computed in PVT but values of clock signal are lost. Any rapid changes shall be detected as a spoofing. Also changes in the bias can be monitored and similarly, any fast change in these parameter will denote the attack ( Jafarnia-Jahromi et al. 2013).

*Multi receiver antispoofing technique*

One of firstly invented antispoofing devices is using several receivers in some separation from each other. Because target GNSS receiver works in the same frequency as other, they shall be receiving same position solution, that in fact should be different. Work over this simple and effective technique has been conducted in (Swaszek and Hartnett, 2013) and (Dobryakova et al. 2014).

*Ephemerid consistency check*

This technique might be processed in information layer of receiver, and is based on fact that ephemerid data validity over some short period of time. But the constellation and other ephemeris's values are not changing unexpectedly, in such case can be detected as a spoofing attack.

*Another class system comparison*

This method can be treated as an external data technique and as such can be used by comparing drift of GNSS presented position and other method computed position. Typical systems are Doppler or similar systems (Guzek, 2010) as well as inertial navigation measurements (Gucma and Montewka, 2006). Such concept is used also for multipath and total loss of signal. These devices are used in military as redundant totally non transmitting devices, independent from outer systems. Also in many applications (aircraft – Doppler system or seaborn inertial sensors) these devices gives good reference to other methods of spoofing detection like AGC monitoring or twin antenna / multireceiver detections. Basic concept is presented in fig. 3. where ellipsoidal area is for error for overall positioning. Larger values are observed in time domain for single operation on INS system due to the fact that INS systems has positive time drift and overlaid on it constant bias.

## 4. Comparison of antispoofing methods

Comparison of methods referenced in ch. 3 is shown in table 2. It has been assumed several levels of comparing anti-spoofing concepts with factors complexity of anti-spoofing solution and its performance, done in three levels i.e.

1) signalization where anti-spoofing system and GNSS receiver can only show potential threat not distinguishing if it is real threat or interference,
2) alarming - system can distinguish if signal is faked, but cannot avoid it,
3) mitigating – system detects and avoids using spoofed signal,

Analysis shows that mitigation is possible only using multi antenna technique, where this assumption is based on fact that some sort of real signal must reach receiver. Threat to this kind of apriori estimation is fact that spoofers can monitor level of signal from SV and try to overlap it of few parts of dBm.

Another idea is combining multi antenna techniques with INS or similar kind of system for independent measurement. At such case complexity will be very high and cost also. In some cases where loos of automatic positioning application (like aircraft landing or vessel mooring) it is only practical way to establish potential attack threat and avoid serious losses.

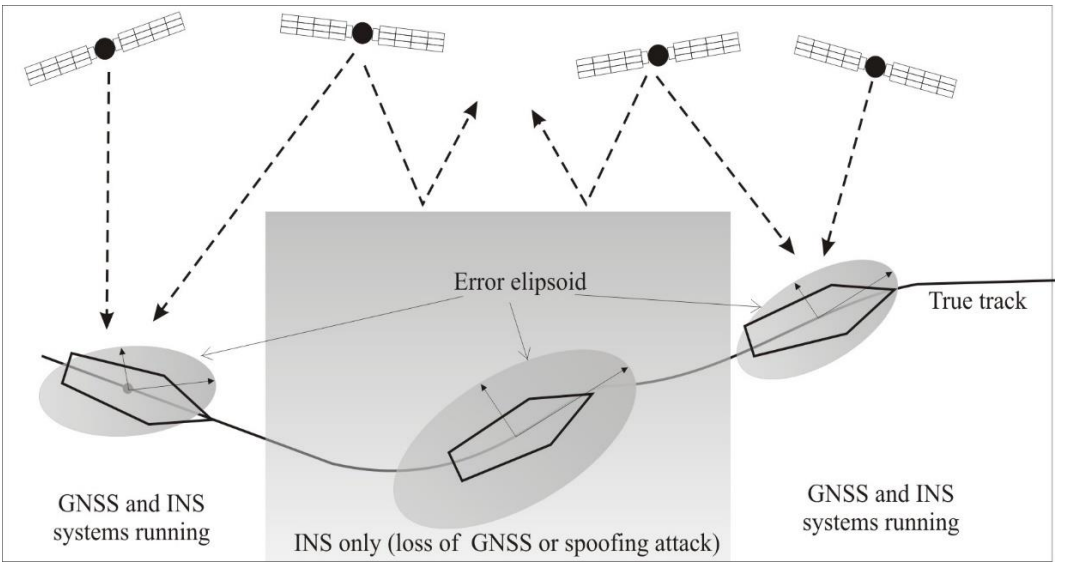


Fig 3. Loss of positioning from GNSS sensor

Table 2. Comparison of antispoofing methods complexity and performance

| Method of antispoofing | Complexity | Performance |
|---|---|---|
| Monitoring of CNR parameter | Low | Signalization |
| Multi antenna technique | High | Alarming/Mitigating |
| In-band Power Monitoring | Low | Signalization |
| Phase Rates Consistency Check | Low | Signalization/Alarming |
| SQM Technique | Low | Signalization |
| Clock attack | Low | Signalization |
| Multi receiver antispoofing technique | Medium/High | Alarming |
| Ephemerid consistency check | Low | Alarming |
| Another class system comparison | High | Alarming |

## 5. Future researches

Not every technique/method can be implemented in all situations. Some of these are stationary techniques non implementable to in other that nonmoving devices. Some requires large amount of extra receiver data. In many aspects like precise positioning of vessel in port (where required heading is 0.1deg and position accuracy less than 0.2 m) it is not enough to alarm crew members about possible threat - mitigation of fake signal is generally required.

Different combination of anti-spoofing techniques is required to mitigate real threats in high noise and high level of fake signal.

Another promising concept is connecting through filters several devices like GNSS and INS systems to obtain resistant to spoofing system. Also new methods for combination of localization through web based systems and cellular phones are very promising concepts. Also usage of multi receivers (like GPS+GLONASS) is a way to obtain robustness in positioning.

## 6. Conclusions

This paper presents current methods of loss of the security in the GNSS systems signal generated by the intentional changing of real signal to a faked signal and possible countermeasures of this phenomena. Only methods of detection available to end customer in transport has been presented. Some limitations of application as well as usefulness of methods has been prompted. It has been shown that some of the simple methods combined with each other gives pretty good results comparable to laboratory tests. Anyway still mitigations of the faked signal is desired in the transport application of GNSS and only 3rd non related to satellite ranging and positioning system can securely alarm about threat and mitigate it

## References


[1] AKOS, D.M., 2012. Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC). *Navigation*, 59(4), pp. 281-290.

[2] AKOS, D.M., 2015. *GNSS RFI/Spoofing: Detection, Localization, & Mitigation.* Presentation. Stanford: Stanford's 2012 PNT Challenges and Opportunities Symposium.

[3] BORIO, D., 2013. PANOVA Tests and their Application to GNSS Spoofing Detection. *Aerospace and Electronic Systems, IEEE Transactions on*, 49(1), pp. 381-394.

[4] DEHGHANIAN, V., NIELSEN, J. and LACHAPELLE, G., 2012. GNSS spoofing detection based on receiver C/No estimates, *Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2012), Nashville, TN* 2012, pp. 2878-2884.

[5] DOBRYAKOVA, L., LEMIESZEWSKI, Ł. and OCHIN, E., 2014. Design and analysis of spoofing detection algorithms for GNSS signals. *Zeszyty Naukowe / Akademia Morska w Szczecinie*, 40(112), pp. 47-52.

[6] GUCMA, M. and MONTEWKA, J., 2006. *Podstawy morskiej nawigacji inercyjnej*. Szczecin: Akademia Morska w Szczecinie.

[7] GUZEK, M., 2010. Car ADR/EDR recorders-uncertainty of vehicle's speed and trajectory determination. *Archives of Transport*, 22(2), pp. 163-174.

[8] JAFARNIA-JAHROMI, A., BROUMANDAN, A., NIELSEN, J. and LACHAPELLE, G., 2014. Pre-Despreading Authenticity Verification for GPS L1 C/A Signals. *Navigation*, 61(1), pp. 1-11.

[9] JAFARNIA-JAHROMI, A., DANESHMAND, S., BROUMANDAN, A., NIELSEN, J. and LACHAPELLE, G., 2013. *PVT Solution Authentication Based on Monitoring the Clock State for a Moving GNSS Receiver*. Vienna, Austria: Presented at the European Navigation Conference (ENC2013).

[10] KOC, W. and SPECHT, C., 2011. Selected problems of determining the course of railway routes by use of GPS network solution. *Archives of Transport*, 23(3), pp. 303-320.

[11] MONTGOMERY, P.Y., HUMPHREYS, T.E. and LEDVINA, B.M., 2009. Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer, *Proceedings of the ION International Technical Meeting*, January 26-28 2009, Anaheim, CA, pp. 124-130.

[12] OCHIN, E., GUCMA, L., PETLIN, S., VIDMAR, P., GUCMA, M., PUSZCZ, A., PERKOVIC, M., HARSH, R. and LEMIESZEWSKI, Ł., 2014. Problems of telecommunication networks for the safety of maritime transport, *Proceedings of World Maritime Technology Conference* 2014, Saint-Petersburg.

[13] PSIAKI, M., O'HANLON, B., POWELL, S., BHATTI, J., WESSON, K., HUMPHREYS, T. and SCHOFIELD, A., 2014b. GNSS Spoofing Detection using Two-Antenna Differential Carrier Phase, *Proc. of the 27th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS ),(Tampa, Florida)* 2014b, pp. 2776-2800.

[14] PSIAKI, M.L., HANLON, B.W.O., POWELL, S.P., BHATTI, J.A., HUMPHREYS, T.E., SCHOFIELD, A. and WESSON, K.D., 2014a. *GNSS Spoofing Detection using Two-Antenna Differential Carrier Phase.* Presented at the ION/GNSS+ 2014.

[15] SWASZEK, P.F. and HARTNETT, R.J., 2013. Spoof detection using multiple COTS receivers in safety critical applications, *Proc. ION*

*GNSS+ 2013, Nashville TN, Sept. 2013* 2013, pp. 2921-2930.

[16] WEN, H., HUANG, P.Y., DYER, J., ARCHINAL, A. and FAGAN, J., 2005. Countermeasures for GPS signal spoofing, *ION GNSS 2005. Long Beach, CA (2005)* 2005, pp. 13-16.

[17] ZALEWSKI, P., 2014. Real-time GNSS spoofing detection in maritime code receivers. *Zeszyty Naukowe / Akademia Morska w Szczecinie*, 38(110), pp. 118-124.