Larisa DOBRYAKOVA, Łukasz LEMIESZEWSKI, Evgeny OCHIN

THE SPOOFING DETECTION OF LOCAL AREA DIFFERENTIAL GNSS IN THE ASPECT OF LAND TRANSPORT SYSTEMS

Differential Global Navigation Satellite System (DGNSS) is an enhancement to GNSS that was developed to correct errors (delays during the signals' transit to earth) and inaccuracies in the GNSS system, allowing for more accurate positioning of information. In general, access to this correction information makes differential GNSS receivers much more accurate than other receivers; with these errors removed, a GNSS receiver has the potential to achieve accuracies of up to 10 centimeters. The GNSS positioning and navigation is widely used in many industries around the world : aircrafts, ships, missiles, UAVs and vehicles rely on GNSS data. Recent studies have shown that the interference and spoofing of GNSS is a real threat to the reliability and accuracy of the GNSS system and can be used by terrorists. One of the main problems of modern navigation both manned and unmanned transport systems is a problem of transport safety. One of the main problems of modern navigation both manned and unmanned transport systems is a problem of transport safety. To improve the accuracy of transport positioning we use Differential GNSS technology, which is based on setting a fixed referent station with a known geodetic position XYZ. Unfortunately, GNSS is vulnerable to malicious intrusion. GNSS can be spoofed by false signals, but special receivers can provide defenses against such attacks. In this article are considered the principles of architecture LADGNSS – Local Area Differential GNSS.

INTRODUCTION

We introduce some definitions used in this article.

1. $\mathbf{Sat_i}, i = \overline{1, N}, N \geq 4$– the navigation Satellites as the space part of GNSS.

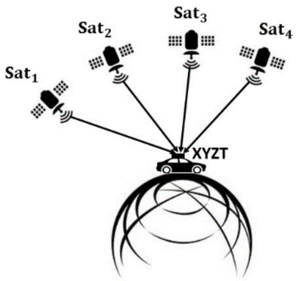

Fig. 1.*The minimum four Satellites: Sat_i – "Satellites", $i = 1,\ N,\ N \geq 4$ the visible part of GNSS satellite constellation for computing XYZT (3D space XYZ and time T)*

For land transport, as a rule, the height above sea is not calculated, therefore, the least amount of visible satellites is reduced to three (Fig. 2):

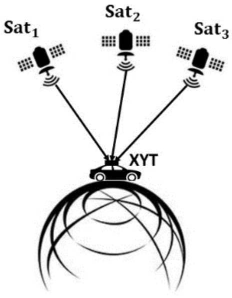

Fig. 2.*The minimum three Satellites: Sat_i – "Satellites", $i = 1,\ N,\ N \geq 3$ the visible part of GNSS satellite constellation for computing XYT (2D space XY and time T)*

2. **DS – Differential Station** – control correction station subsystem differential GNSS, including a **Reference Station (RS)** with their own coordinates $(\boldsymbol{x_{rs}}, \boldsymbol{y_{rs}})$ and the **Radio Beacon (RB)** transmitting correction information.

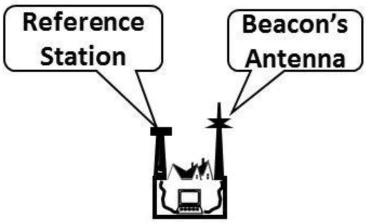

Fig. 3.*The Differential Station (DS): Reference Station (RS) + Radio Beacon Station (RB)*

3. **The Spoofing** – attack on GNSS, which is trying to deceive the GNSS receiver, transmitting the powerful false signals that imitatethe signals from GNSS and exceeding the power of true signals from GNSS.

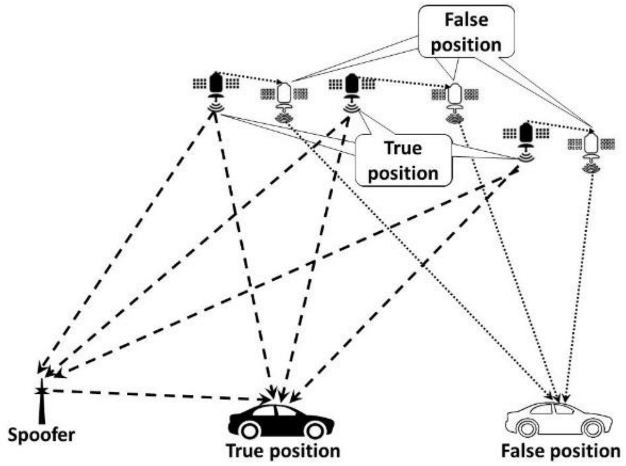

Fig. 4.*The GNSS Spoofing*

The Spoofer receives signals from GNSS satellites and change some of the parameters of these signals in the way that create the illusion of changing the position of satellites in orbits (the satellite signal distortion algorithms are not considered in this article). The spoofer cannot rely on the real GNSS signals and create a completely "fictional" constellation of satellites, but this spoofing is relatively easy to recognize.

4. **The Spoofer** – complex computer and radio equipment for the implementation of GNSS spoofing.

Fig. 5. The Spoofer – complex computer and radio equipment for the implementation of GNSS spoofing. It costs several thousand dollars. The source SPIRENT https://www.spirent.com

5. **The DGNSS –** DifferentialGNSS

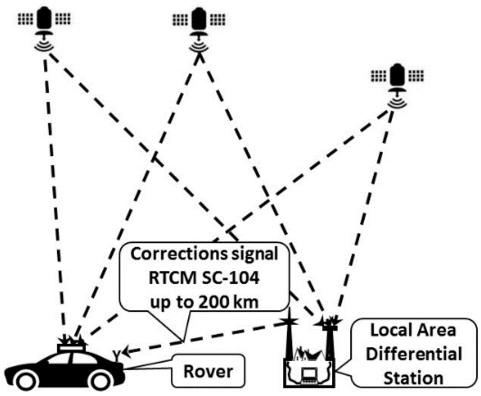

Fig. 6.The Local Area Differential GNSS: the Reference Station at a known position and a 2nd receiver on board of the Rover at an unknown position. Because the GNSS position errors for the Reference Station and for the rover are approximately the same, the difference between the known and unknown locations of the Reference Station can be used to improve the accuracy of the positioning

6. **The Rover** – any mobile GNSS receiver that is used to collect data in the field at an unknown location.
7. **LADGNSS** – Local Area Differential GNSS – Differential station transmitting correction information up to ~200 km of coastline.
8. **Pseudo-range** – distance to the satellite, resulting in the receiver based on the correlation of the received code and onboard code without correction of clock synchronization errors.
9. **Pseudo-ranges error** – uncorrected error component of each pseudo-range corrections.
10. **RTCM** – Radio Technical Commission for Maritime Services – defines a differential data link for the real-time differential correction of roving GNSS receivers.
11. $(\boldsymbol{x}, \boldsymbol{y})$ – the real coordinates of the Vehicle in the absolute coordinate (the spatial coordinates in the rectangular geocentric system of coordinates on the terrestrial ellipsoid, usually in the WGS-84).If the vehicle is 2D vehicle (ship, vessel, boat, car, etc.), the height coordinate (z) can be omitted and minimum number of navigation satellites can be reduced to three ($i = \overline{1, N}, N \geq 3$).
12. $(\boldsymbol{x_v}, \boldsymbol{y_v})$ – the calculated coordinates of the vehicle using the GNSS.
13. $(\widetilde{\boldsymbol{x}}_v, \widetilde{\boldsymbol{y}}_v)$– the calculated coordinates of the vehicle using the DGNSS.
14. (x_{rs}, y_{rs}) – the coordinates of RS.
15. $\boldsymbol{c}$ – the speed of light.
16. We also denote for $i = \overline{1, N}, N \geq 3$:
    $(\boldsymbol{x_i}, \boldsymbol{y_i}, \boldsymbol{z_i})$ – the coordinates of $\mathrm{Sat_i}$;
    $\boldsymbol{T_i^{rs}}$– the propagation time from the $\mathrm{Sat_i}$to the **RS** in vacuum;
    $\boldsymbol{\widehat{T}_i^{rs}}$ – the propagation time from the $\mathrm{Sat_i}$to the **RS** in real atmosphere;
    $\boldsymbol{\rho_i^{rs}}$– the real distance from the $\mathrm{Sat_i}$to the **RS**;
    $\boldsymbol{\widehat{\rho}_i^{rs}}$– the measurement result of the distance from the $\mathbf{Sat_i}$to the **RS** (evaluations of $\boldsymbol{D_i^{rs}}$ or pseudo-range);
    $\boldsymbol{T_i^v}$ – the propagation time from the $\mathrm{Sat_i}$to the vehicle in vacuum;
    $\boldsymbol{\widehat{T}_i^v}$ – the propagation time from the $\mathrm{Sat_i}$to the vehicle in real atmosphere;
    $\boldsymbol{\widehat{\rho}_i^v}$ – the measurement result of the distance from the $\mathrm{Sat_i}$to the vehicle (the vehicle pseudo-ranges).

1. GNSS POSITIONING

The distance from vehicle (Figure1) to satellites Sat_i can be written as

$$\rho_i^v = \sqrt{(x_i - x_v)^2 + (y_i - y_v)^2 + {z_i}^2} = cT_i^v, \quad i = \overline{1, N}, N \geq 3 \tag{1}$$

Since the measurement of distance from the vehicle to the satellites is carried out by measuring the propagation time $\hat{T}_i^V = T_i^V + \Delta T_i^V$ of GNSS signals from Sat_i to vehicle then (1) can be represented as (excluding time synchronization errors):

$$\sqrt{(x_i - x_v)^2 + (y_i - y_v)^2 + {z_i}^2} = c\hat{T}_i^v \tag{2}$$

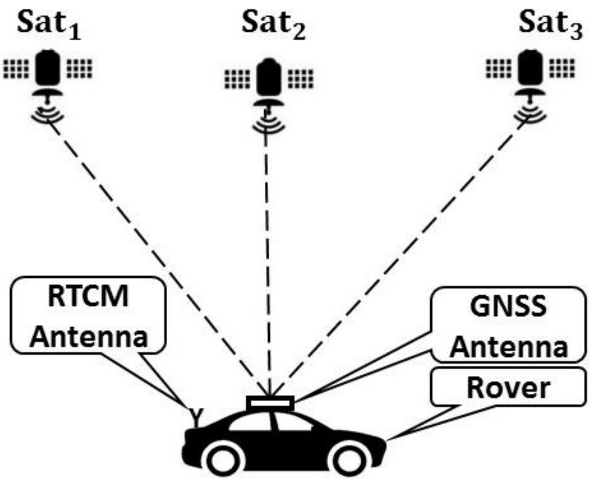

Fig. 7. GNSS and Rover: Sat_i – "Satellites", $i = \overline{1,\ N},\ N \geq 3$, the visible part of GNSS satellite constellation

The navigation processor of vehicle solves the system of the equations (2), calculates the position of the vehicle (x_v, y_v) and timing errors on board $\Delta\mathrm{t}$, which are used to correct the clock GNSS navigation (this article does not consider the timing errors $\Delta\mathrm{t}$). The calculations require the exact time, and most GNSS receivers do not contain sufficiently precise internal clock, therefore, to remove the ambiguity with respect to time, GNSS receivers need another equation that allows to obtain the exact time - this equation gives a fourth satellite. Thus, for high-precision positioning, for the receiver signals of four satellites are sufficient.Analyzing the problem of positioning accuracy (2), we note that

$$\{\hat{T}_i^v = T_i^v + \Delta T_i^v\}, i = \overline{1,N}, N \geq 3 \qquad (3)$$

that is, the accuracy is largely determined by the size of the propagation time delay from the $\mathrm{Sat_i}$ to the vehicle ΔT_i^v.

Support for GNSS Positioning technology will solve the problem of positioning in the meter range (5-10 m)

Currently, to improve the accuracy of GNSS are widely used the differential GNSS.

2. DIFFERENTIAL GNSS POSITIONING

In order to increase the accuracy of GNSS to a level that provides swimming ships in rivers and canals, was developed differential subsystem DGNSS (base station antenna is set to within a few millimeters), consisting of ground differential base stations that receive signals from satellites, counting errors for signals about its (actual) position in the system WGS84 [5-8] and transmit errors by a special radio network or by satellite. Correcting Reed-Solomon codes are used for error-correcting coding. DGNSS can refer to any type of Ground Based Augmentation System. There are many operational ground systems in use throughout the world. A similar system that transmits corrections from orbiting satellites instead of ground-based transmitters is called WAAS (Wide Area Augmentation System or Wide Area DGNSS – WADGNSS). Sometimes used synonymously, the Satellite Based Augmentation system (SBAS) can include orbiting satellite systems that have been implemented in other parts of the world such as EGNOS, MSAS, QZSS, GAGAN and others.

DGNSS are divided into two main categories:

1. LADGNSS – Local Area Differential GNSS – Differential station transmitting correction information up to ~200 km of coastline.
2. WADGNSS – Wide Area Differential GNSS – formed by combining data of a few LADGNSS that located in a same region, a same state or a group of bordering states (inthis article shall not be considered).

3. LOCAL AREA DIFFERENTIAL GNSS POSITIONING

Since RS is at known location (x_{rs}, y_{rs}) we can compute the real distance from RS (Figure 2) to satellites Sat_i as

$$\rho_i^{rs} = \sqrt{(x_i - x_{rs})^2 + (y_i - y_{rs})^2 + {z_i}^2}, \quad i = \overline{1,N}, N \geq 3 \qquad (4)$$

We calculate the assessment of the distance from RS to satellites Sat_i (pseudo-range) by determining the signal propagation time from RS to the satellites $\mathrm{Sat_i}$ as

$$\hat{\rho}_i^{rs} = c\hat{T}_i^{rs}, i = \overline{1,N}, N \geq 3 \qquad (5)$$

and now we can compute the correction of a pseudo-range for all vehicles in limited scope:

$$\Delta\rho_i^{rs} = (\widehat{D}_i^{rs} - D_i^{rs}), i = \overline{1,N}, N \geq 3 \qquad (6)$$

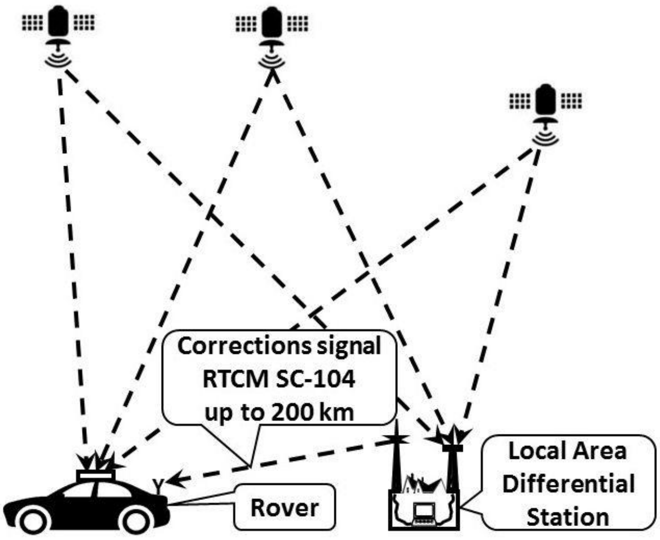

Fig.8. The Local Area Differential GNSS: this figure shows a receiver at a known position (the Reference Station) and a 2nd receiver on board of the vehicle at an unknown position (i.e. the rover or user) for relative positioning. Because the GNSS position errors for the Reference Station and for the rover are approximately the same, the difference between the known and unknown locations of the Reference Station can be used to improve the accuracy of the positioning

The Radio Beacon transmits the correction $\Delta\rho_i^{rs}$ to all vehicles, adjusting their pseudo-range as

$$\tilde{\rho}_i^v = (\hat{\rho}_i^v - \Delta\rho_i^{rs}) = \left(c\hat{T}_i^v - \Delta\rho_i^{rs}\right), i = \overline{1,N}, N \geq 3 \qquad (7)$$

In this case the system of the equations (2) assumes the form

$$\sqrt{(x_i - \tilde{x}_v)^2 + (y_i - \tilde{y}_v)^2 + {z_i}^2} = (c\hat{T}_i^v - \Delta\rho_i^{rs}) \qquad (8)$$

The navigation processor of vehicle solves the system of equations (8) and calculate the position of the vehicle $(\tilde{x}_v, \tilde{y}_v)$.

4. GNSS SPOOFING

The spoofer can be built on the basis of laboratory GNSS signal generator designed for debugging GNSS receivers. Spoofing is possible to build a system based on a particular set of SDR (Software-defined radio – software-defined radio), for they have the appropriate software. Approximate cost is 1-10 thousand euro [9-13]. A victim moves in space with the civil GNSS procedure and is subjected to a spoofing attack from other vehicles on the ground or at sea, which will call a “spoofer”. GNSS spoofing is the GNSS signal conversion technology. Spoofer plans to organize an attack, so that the navigator should not know that the signal received by GNSS receiver is false. As a result of an organized attack, the navigator determines wrong time and/or location. This means that the spoofer began to administer the GNSS position in time and space.

The distortion of the signal includes a signal capture and playback at the same frequency with a slight distortion and with greater intensity, in order to deceive the electronic equipment of a victim and, respectively, co-driver, of course, if there is one on board the vehicle, ie no additional navigation equipment, for example, INS – Inertial Navigation System[1].

[1] http://clifton.mech.northwestern.edu/~me381/project/done/Gyroscope.pdf

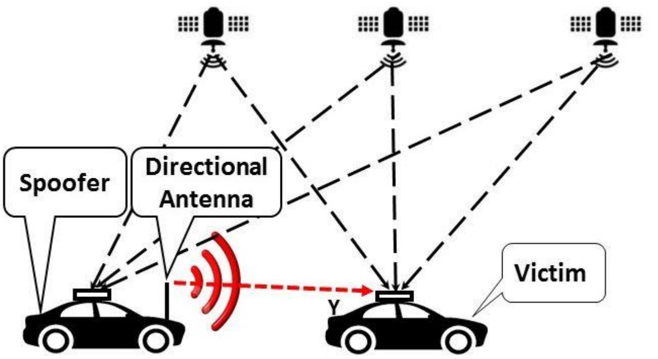

Fig. 9. *GNSS Spoofing: a vehicle called a victim. Spoofer is generally located in the immediate vicinity of the victim and moves in space with civilian or military GNSS mode (L1 or L1/L2).*

The only GNSS system switch witch can't be deceived is GNSS military system that utilizes principles of cryptography. However, for GNSS civil use such protection doesn't exist. Therefore, the research of spoofing property for anti-spoofers design must be conducted. The spoofing main idea is illustrated in Fig.9. Spoofer is generally located in the immediate vicinity of the victim and moves in space with civilian or military GNSS mode (L1 or L1/L2).

Spoofer performs short-term disruption of the GNSS signal L1 using GNSS jammer. As a result of jamming GNSS receiver „loses satellites" and starts looking for GNSS signals. At this time, spoofer includes imitator GNSS signals, which are set up to imitate the new coordinates of the GNSS receiver. Generally, GNSS signal strength exceeds the strength of imitator real GNSS signals and GNSS receiver can't determine from what time of its movement in space it is controlled by a spoofer.

5. SPOOFING OF LOCAL AREA DIFFERENTIAL GNSS POSITIONING

The LADGNSS technology provides additional opportunities of spoofing – not only GNSS signals, but also spoofing of differential correction signals. The Radio Beacon of spoofer transmits the false correction ΔD_i^f to the victim, thus "adjusting" their pseudo-range as

$$\widetilde{D}_i^v = \left(\widehat{D}_i^v - \Delta D_i^f\right) = \left(c\widehat{T}_i^v - \Delta D_i^f\right) \tag{9}$$

In this case the system of the equations (2) assumes the form

$$\left\{\sqrt{\left(\boldsymbol{x_i} - \widetilde{\boldsymbol{x}}_{\boldsymbol{f}}\right)^2 + \left(\boldsymbol{y_i} - \widetilde{\boldsymbol{y}}_{\boldsymbol{f}}\right)^2 + \boldsymbol{z_i}^2} = \left(\boldsymbol{c\widehat{T}_i^v} - \boldsymbol{\Delta D_i^f}\right)\right\} \rightarrow \rightarrow (\tilde{x}_f, \tilde{y}_f), i = \overline{1, N}, N \geq 3 \tag{10}$$

The navigation processor of vehicle solves the system of equations (10) and calculates the false position of the victim $(\tilde{x}_f, \tilde{y}_f)$.

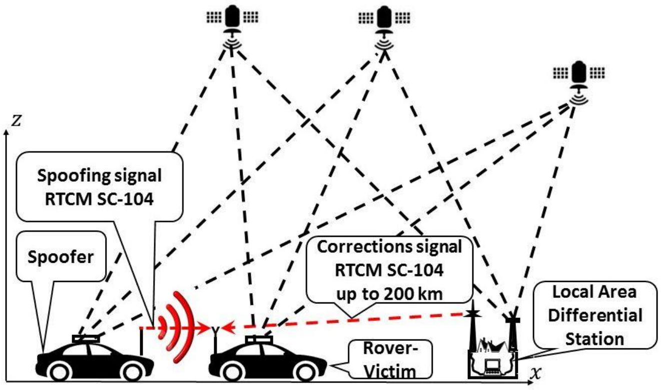
z
Spoofing signal RTCM SC-104
Spoofer
Corrections signal RTCM SC-104 up to 200 km
Local Area Differential Station
Rover-Victim
x

Fig. 10. *DGNSS Spoofing*

6. SPOOFING DETECTION OF LOCAL AREA DIFFERENTIAL GNSS POSITIONING

The navigation processor of victim solves the system of the equations (11)

$$\sqrt{(x_i - x_v)^2 + (y_i - y_v)^2 + {z_v}^2} = c\widehat{T}_i^v, \tag{11}$$

and calculates the coordinates of the victim (x_v, y_v) using the GNSS signals without any corrections. It then computes the distance between the two victim positions

$$\widetilde{\Delta D} = \sqrt{\left(x_v - \tilde{x}_f\right)^2 + \left(y_v - \tilde{y}_f\right)^2 + {z_v}^2} \tag{12}$$

If the vehicle is not exposed to the type of spoofing attack, the difference between the calculated coordinates cannot exceed a certain maximum positioning error ΔD_{max} on normal mode GNSS (DGNSS mode is not available), i.e.

$$\widetilde{\Delta D} \leq \Delta D_{max} \tag{13}$$

and the decision rule of algorithm for spoofing's determining can be written as

if $(\widetilde{\Delta D} \leq \Delta D_{max})$ then OK else goto SPOOFING (14)

7. SUMMARY AND CONCLUSIONS

The risk of losing GNSS signal is growing every day. The accessories for the manufacture of systems GNSS «Jamming and/or Spoofing» are now widely available and it can take advantage of not only military, but also terrorists. The distortion of the signal includes a signal capture and playback at the same frequency with a slight shift in time and with greater intensity, in order to deceive the electronic equipment of a victim and, respectively, co-driver, of course, if there is one on board the vehicle. The price of one chipset of such equipment is in the range of 1-10 thousand euros, depending on the dimensions and weight parameters. In this article we consider the principles of spoofing detection using Local, Regional and Wide Differential GNSS, in which correction signals of differential station is used for the detection of spoofing. This relatively simple and quite effective method has one obvious drawback – is supposed to use a fixed (stationary) differential GNSS station, the coordinates of which should be known to the geodesic (centimeters) accuracy. Our research in the field of spoofing detection [9-13] gives us confidence that this deficiency is avoidable and in the near future we expect to publish the results of our research, thanks to which,mobile differential stationcould be implemented.

REFERENCES

1. Retscher, G.: Accuracy Performance of Virtual Reference Station (VRS) Networks, Beacon DGPS Broadcasting Stations network. http://www.mx-marine.com/beacon-dgps-base-stations.html
2. Accuracy Performance of Virtual Reference Station (VRS) Networks. Journal of GPS, Vol.1, No.1:40-47, 2002 http://www.gmat.unsw.edu.au/wang/jgps/v1n1/v1n1pE.pdf
3. Beacon DGPS Base Station. http://www.mx-marine.com/downloads/BrochureBeacon2011.pdf
4. Spoofing, Detection, and Navigation Vulnerability. https://www.youtube.com/watch?v=qlX-MsYZvoM
5. World Geodetic System 1984 (WGS 84) http://gisgeography.com/wgs84-world-geodetic-system/
6. Specht C.: System GPS. Biblioteka Nawigacji nr 1. Wydawnictwo Bernardinum. Pelplin 2007.
7. Januszewski J.: Systemy satelitarne GPS, Galileo i inne. PWN 2010.
8. Dobryakova L., Lemieszewski Ł., Ochin E.: Antyterroryzm – projektowanie i analiza algorytmów antyspoofingu dla globalnych

nawigacyjnych systemów satelitarnych // ScientificJournalsMaritime University of Szczecin, 2012, 30(102), pp. 93–101. http://repository.am.szczecin.pl/handle/123456789/358

9. Dobryakova L., Lemieszewski Ł., Ochin E.: The analysis of the detecting algorithms of GNSS-spoofing. Scientific Journals Maritime University of Szczecin, 2013, 36(108) z. 2, pp. 30–36 http://repository.am.szczecin.pl/handle/123456789/561
10. Dobryakova L., Lemieszewski Ł., Lusznikov E., Ochin E.: The study of the spoofer's some properties with help of GNSS signal repeater// Scientific Journals Maritime University of Szczecin, 36(108) z. 2 2013, pp. 159–165 http://repository.am.szczecin.pl/handle/123456789/581
11. Dobryakova L., Lemieszewski Ł., Ochin E.: Design and Analysis of Spoofing Detection Algorithms for GNSS Signals // Scientific Journals Maritime University of Szczecin, 40(112), 2014, pp. 47-52 http://repository.am.szczecin.pl/handle/123456789
12. Dobryakova L., Ochin E.: On the application of GNSS signal repeater as a spoofer /Scientific Journals Maritime University of Szczecin, 40(112), str. 53-57, ISSN 1733-8670, 2014 http://repository.am.szczecin.pl/handle/123456789

Wykrycie spoofingu w lokalnych różnicowych GNSS w aspekcie lądowych systemów transportowych

Różnicowe Globalne Satelitarne Systemy Nawigacyjne (DGNSS) są rozszerzeniem GNSS. Zostałyone opracowane w celu skorygowania błędów (opóźnienia sygnałów podczas transmisji do ziemi) i nieścisłości w systemie GNSS, co pozwala na przesłanie bardziej dokładnych informacji pozycjonowania. Dostęp do informacji dotyczących poprawek różnicowych dla odbiorników GNSS pozwala na znacznie bardziej dokładne pozycjonowanie niż w przypadku innych odbiorników. Poprzez usunięcie tych błędów odbiornik GNSS ma potencjał, aby osiągnąć dokładność do 10 centymetrów. Pozycjonowanie GNSS i nawigacja są szeroko stosowane w wielu gałęziach przemysłu na całym świecie: w samolotach, na statkach, w rakietach, bezzałogowych statkach powietrznych(UAV) i pojazdach, opierających swoją pozycję na danych GNSS. Najnowsze badania wykazały, że ingerencja i fałszowanie GNSS jest realnym zagrożeniem dla wiarygodności i dokładności systemu GNSS, podatność ta może być wykorzystana przez terrorystów. Jednym z głównych problemów współczesnych załogowych i bezzałogowych systemów nawigacyjnych jest zagrożenie bezpieczeństwa transportu. Aby zwiększyć dokładność pozycjonowania transportu, wykorzystuje się różne technologie mechanizmu różnicowego GNSS opartego na ustawieniu stacji referencyjnej ze znanym geodezyjnym położeniem w przestrzeni XYZ. Niestety, GNSS jest w dużym stopniu narażone na ataki. Sygnał GNSS może być podrobiony przez nadawanie fałszywych sygnałów, ale specjalne odbiorniki mogą zapewnić przed nimi obronę. W artykule przyjęto zasady architektury LADGNSS – LocalAreaDifferential GNSS.

Authors:

Dr inż. **Larisa Dobryakova**–West Pomeranian University of Technology, Faculty of Computer Science and Information Technologies, 71-210 Szczecin, ul. Żołnierska 49, e-mail: ldobryakova@wi.zut.edu.pl

Dr inż. **Łukasz Lemieszewski** –The Jacob of Paradies University, Department of Technology, ul. Teatralna 25, 66-400 Gorzów Wielkopolski, e-mail: llemieszewski@ajp.edu.pl

Prof. dr hab. inż. **Evgeny Ochin**–Maritime University of Szczecin, Faculty of Navigation, 70-500 Szczecin, ul. WałyChrobrego 1–2, phone +48 608 437 562, e-mail: e.ochin@am.szczecin.pl