Scientific Journals
Maritime University of Szczecin

Zeszyty Naukowe
Akademia Morska w Szczecinie

2014, 40(112) pp. 53–57
ISSN 1733-8670

On the application of GNSS signal repeater as a spoofer

Larisa Dobryakova[1], Evgeny Ochin[2]

[1] West Pomeranian University of Technology, Faculty of Computer Science and Information Technology
71-210 Szczecin, ul. Żołnierska 49, e-mail: ldobryakova@wi.zut.edu.pl
[2] Maritime University of Szczecin, Faculty of Navigation
70-500 Szczecin, ul.Wały Chrobrego 1–2, e-mail: e.ochin@am.szczecin.pl

Key words: spoofer, spoofing, GNSS, repeater

Abstract
Spoofing and antispoofing algorithms have become an important research topic within the GNSS discipline. The power of the GNSS signal on the earth's surface averages –160 dBw. While many GNSS receivers leave large space for signal dynamics, enough power space is left for the GNSS signals to be spoofed. The goal of spoofing is to provide the receiver with a misleading signal, fooling the receiver to use fake signals in space for positioning calculations. The receiver will produce a misleading position solution. The purpose of this paper is to analyze the vulnerability of the satellite signal in repeater's output from the viewpoint of GNSS spoofing attacks. The article discusses a new approach to GNSS spoofing, based on the application of GNSS signals repeating by potential terrorists. Practical spoofing that provides misleading navigation results at the receiver is difficult to conduct due to the signal infrastructure, and by applying trivial anti-spoofing algorithms in GPS receivers, spoofing attack can be easily detected. To detect spoofing attacks of this type we have a variety of methods. For example, the authors suggest the use of paired navigators and GNSS compasses as detectors of GNSS spoofing.

Introduction

Spoofing and antispoofing algorithms have become an important research topic within the GNSS discipline. There is an ever-increasing attention to safe and secure GNSS applications such as air, marine, and ground transportations, police and rescue services.

The power of the GNSS signal on the earth's surface averages –160 dBw. While, many GNSS receivers leave large space for the dynamics of the signal, enough power space is left for the GNSS signals to be spoofed. The goal of spoofing is to provide the receiver with a misleading signal, fooling the receiver to use fake signals in space for positioning calculations. The receiver will produce a misleading position solution. The purpose of this paper is to analyze the vulnerability of the satellite signal in repeater's output from the viewpoint of GNSS spoofing attacks. The article discusses a new approach to GNSS spoofing, based on the application of GNSS signals repeating by potential terrorists. Practical spoofing that provides misleading navigation results at the receiver is difficult to conduct due to the signal infrastructure, and by applying trivial anti-spoofing algorithms in GPS receivers, spoofing attack can be easily detected. There are a variety of methods to detect spoofing attacks of this type. For example, the authors suggest the use of paired navigators and GNSS compasses as detectors of GNSS spoofing.

In this paper, we are going to present a new approach to GNSS spoofing, based on the application of GNSS signals repeating by potential terrorists. For purposes of discussion, a spoof is defined as a malicious signal that overpowers the authentic signal and misleads the receiver to use a forged signal for further processing. This paper will discuss the spoof issue on a single antenna GPS receiver only.

Basic notation

$SV_i, i = \overline{0, N-1}$ Satellite Vehicles;
(x_i, y_i, z_i) – the position of SV_i at transmit time;

S – Ship, Car, Aircraft, Dron or suchlike Vehicle;
(x_s, y_s, z_s) – the receiver's position of the vehicle S at receive time;
R – repeater of GNSS signals;
$\Delta\rho$– distance from the repeater to the vehicle S;
(x_r, y_r, z_r) – the receiver's position of the repeater R at receive time;
s_i – real distance from the SV_i to the vehicle S;
S_i – assessment of the distance from the SV_i to the vehicle S (pseudorange);
t_i – real time of GNSS signal propagation from the SV_i to the vehicle S;
Δt – the receiver clock bias (error in the measurement of time aboard vehicle S);
$T_i = t_i + \Delta t$ – assessment of the GNSS signal propagation time from the SV_i to the vehicle S;
c – light velocity.

GNSS navigation

The distance from the SV_i to the vehicle S (Fig. 1) can be written as:

$$s_i = \sqrt{(x_i - x_s)^2 + (y_i - y_s)^2 + (z_i - z_s)^2} = ct_i \quad (1)$$

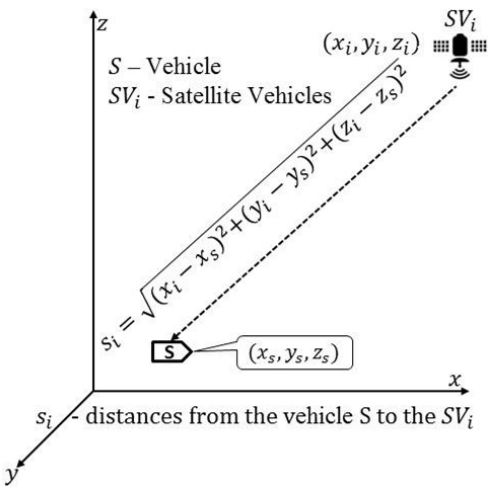

Fig. 1. GNSS navigation: $S_i = s_i + c\Delta t$ – pseudoranges from the S to the SV_i

Since the measurement of the distance from the ship to the satellites is performed by measuring the time $T_i = t_i + \Delta t$ of propagation of GNSS signals from the SV_i to the vehicle S (Fig. 2) than (1) can be represented as:

$$\sqrt{(x_i - x_s)^2 + (y_i - y_s)^2 + (z_i - z_s)^2} = c(T_i - \Delta t)$$
$$i = \overline{0, N-1}, N \geq 4 \quad (2)$$

Processor of GNSS navigator solves the system of equations (2), computes the position of the vehicle (x_s, y_s, z_s) and errors in the measurement of time aboard vehicle Δt, and it is used as a clock correction of the GNSS navigator [1, 2, 3, 4].

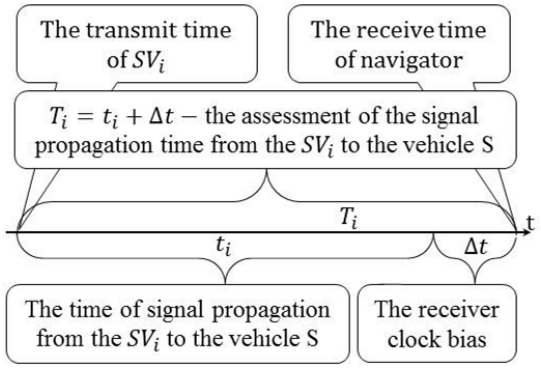

Fig. 2. The timing diagram of the GNSS navigation

GNSS navigation with repeater

The real distance of GNSS-signals propagation from the SV_i to the vehicle S (Fig. 3) can be written as:

$$\rho_i = \Delta\rho + \sqrt{(x_i - x_r)^2 + (y_i - y_r)^2 + (z_i - z_r)^2} = ct_i \quad (3)$$

where: $\Delta\rho = \Delta\rho' + \Delta\rho'' + \Delta\rho'''$.

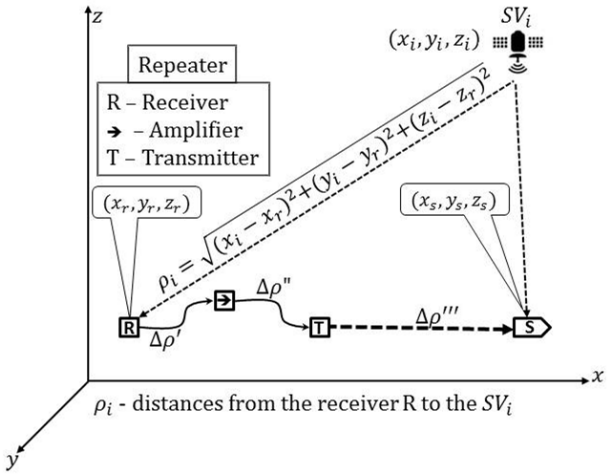

Fig. 3. GNSS navigation with repeater: $\Delta\rho'$ – cable length from the R to the amplifier; $\Delta\rho''$ – cable length from the amplifier to the T; $\Delta\rho'''$ – distance from the T to the S; $R_i = \rho_i + c\Delta t + \Delta\rho' + \Delta\rho'' + \Delta\rho'''$ – pseudoranges from the S to the SV_i

Since the measurement of the distance from the vehicle S to the satellites is performed by measuring the time propagation of GNSS signals from the SV_i to the vehicle S (Fig. 4) and taking into account the passage of GNSS signals through repeaters, we can represent the distance from the vehicle S to the satellites as:

$$R_i = \Delta\rho + \sqrt{(x_i - x_r)^2 + (y_i - y_r)^2 + (z_i - z_r)^2} = ct_i \quad (4)$$

where: $\Delta\rho = \Delta\rho' + \Delta\rho'' + \Delta\rho'''$.

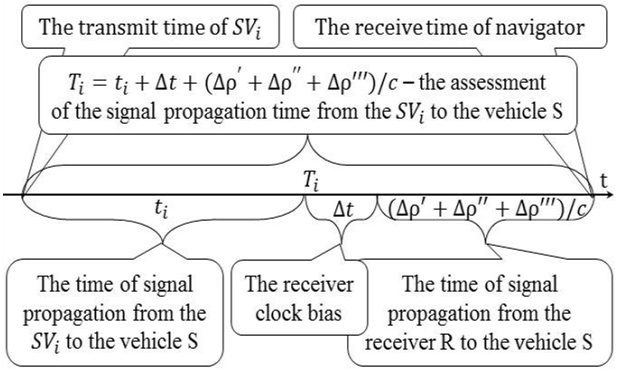

Fig. 4. The timing diagram of the GNSS navigation with repeater

Since $t_i = T_i - \Delta t$ we can represent (4) at $N = 4$ as:

$$\begin{cases} \sqrt{(x_0 - x_r)^2 + (y_0 - y_r)^2 + (z_0 - z_r)^2} = c(T_0 - \Delta t_i) \\ \sqrt{(x_1 - x_r)^2 + (y_1 - y_r)^2 + (z_1 - z_r)^2} = c(T_1 - \Delta t_i) \\ \sqrt{(x_2 - x_r)^2 + (y_2 - y_r)^2 + (z_2 - z_r)^2} = c(T_2 - \Delta t_i) \\ \sqrt{(x_3 - x_r)^2 + (y_3 - y_r)^2 + (z_3 - z_r)^2} = c(T_3 - \Delta t_i) \end{cases} \quad (5)$$

where: $\Delta t' = \Delta t + 2(\Delta\rho' + \Delta\rho'' + \Delta\rho''')/c$. It should be stressed that the system of four equations has four unknowns: (x_r, y_r, z_r) and $\Delta t' = \Delta t + 2(\Delta\rho' + \Delta\rho'' + \Delta\rho''')/c$.

Comparing (2) and (5), you will notice that both equations have a similar appearance. Processor of GNSS navigator solves the system of equations (5), computes the false position of the vehicle S as $(x_s, y_s, z_s) = (x_r, y_r, z_r)$ and computes the time $\Delta t' = \Delta t + 2(\Delta\rho' + \Delta\rho'' + \Delta\rho''')/c$ as the sum of error in the measurement of time aboard vehicle Δt and double delay GNSS signal propagation $(\Delta\rho' + \Delta\rho'' + \Delta\rho''')/c$ from the receiver R to the vehicle S and then processor use $\Delta t'$ as a clock correction of the GNSS navigator.

This means that all the vehicles within range repeater have the same measurement results of their coordinate, i.e. instead of real coordinates obtained false coordinates (x_r, y_r, z_r). This also means that the repeater of GNSS signals can be used as a spoofer with certain disabilities.

While the devices for a GNSS interfering and jamming are becoming cheaper and more accessible, we need to protect the most important elements of the military, civil and industrial infrastructure from malicious acts. Spoofing technology or substitution of real GNSS signals has today become a real threat for unmanned navigation systems.

The Spoofing Experiments

To verify (5), we make two simple experiments in which was used navigator Holux GR-213U Smart GPS Receiver and GPS Signal Antenna Repeater Amplifier Transfer. GR-213U is a total solution of GNSS receiver. This positioning application meets strict needs such as car navigation, mapping, surveying, security, agriculture and so on. Only clear view of sky and certain power supply are necessary to the unit. With low power consumption, the GR-213U tracks up to 20 satellites at a time, reacquires satellite signals in 100 ms and updates position data every second.

To improve the accuracy of measurements the simplest algorithm is used:

$$\hat{P} = \frac{1}{600}\sum_{k=1}^{600} p_k \quad (6)$$

where: p_k – measurement results within 10 minutes at a frequency measurement 1 Hz. All measurements were carried out in an open area about 100 km from Szczecin (Poland).

Experiments 1. The measurement of the receiver's position R (Fig. 5):

$N_r = 3165.492876'$; $E_r = 916.929871'$.

Experiments 2. The measurement of the vehicle's position S: $N_s = 3165.497108'$; $E_r = 916.929652'$.

The measured distance between R and S turned:

$$D_{R-S} = \sqrt{(1852(N_r - N_s))^2 + (1112(E_r - E_s))^2} = \\ = 7.8\text{ m} \approx 7\text{ m} \quad (7)$$

Experiments 3. The measurement of the vehicle's position S under spoofing (false position):

$N_f = 3165.493234'$; $E_f = 916.929776'$.

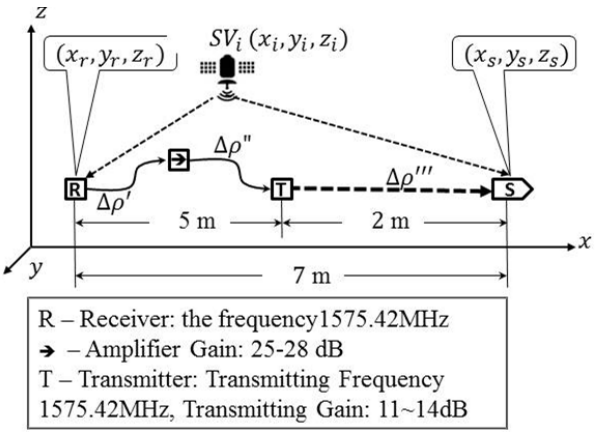

Fig. 5. The Spoofing Experiment: {R→T} – GPS Signal Antenna-Repeater-Amplifier Transfer), the actual distance between receiver R and vehicle S is equal 7 m

The measured distance between R and S turned:

$$D_{R-S} = \\ = \sqrt{\left(1852\left(N_r - N_s\right)\right)^2 + \left(\cos\frac{N_r}{3437.74677}\left(E_r - E_s\right)\right)^2} \\ = 0.7 \text{ m} \approx 0 \text{ m} \tag{8}$$

This is proof that the vehicle is in spoofing.

The Spoofing Scenarios

The general scheme of spoofing is shown in figure 6. Spoofer receives the GNSS signals, amplifies and distorts GNSS signals, according to the spoofing algorithm and directs signals towards the victim. The navigator of victim switches on the GNSS signals from the spoofer and then goes down by the wrong path. If spoofer doesn't distort the GNSS signals the victim "sees" the false coordinates spoofer $(x_s, y_s, z_s) = (x_r, y_r, z_r)$ and also goes down by the wrong path.

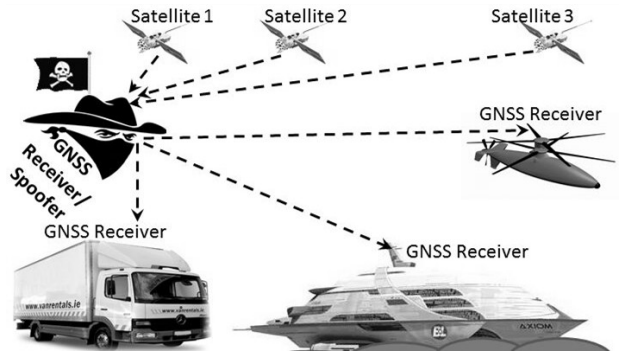

Fig. 6. The general scheme of spoofing

The Spoofing Scenarios I. Assume that the vehicle navigation (the victim) is only using the GNSS navigator and ship goes east course. Assume also that the repeater is on the longitude of the vehicle, but a little further south. From the equation (5) it can be assumed that all the vehicles within range repeater signals have the same measurement results of their coordinate. That is, instead of making real coordinates, the obtained false coordinates coincide with the coordinates of the repeater. In this case, the autopilot will provide additional vehicle maneuvering (offset) of the vehicle towards the north until it gets out of the range of the repeater signal (Fig. 6a). The real trajectory of the vessel depends on the desired course of the vehicle and from the repeater's trajectory, i.e. there are many spoofing scenarios. If the repeater coverage is limited, the actual trajectory of the vehicle changes (Fig. 6b).

a)

b)

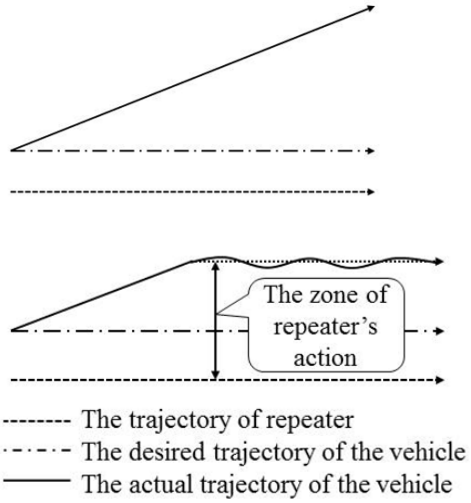

Fig. 7. The ship is heading east and repeater shifts ship in the direction "north": a) the zone of repeater's action is not limited; b) the zone of repeater's action is limited

The Spoofing Scenarios II. Assume that the navigation of unmanned aircraft (drone, Fig. 8) is carried out only with the help of GNSS navigator and drone is within the range of the signal repeater at (x_s, y_s, z_s). Assume also that the GNSS signals that the repeater at point (x_r, y_r, z_r) receives, amplifies, and transmits signals from GNSS. From the equation (5) it can concluded that the drone instead of real coordinates (x_s, y_s, z_s) receives false coordinates (x_r, y_r, z_r). In this case, additional maneuvering (offset) drone functions under the scheme:

$$(x_s, y_s, z_s) \rightarrow \{x_s - x_r, y_s - y_r, z_s - z_r\} \tag{9}$$

i.e. drone is your course and further moves in the direction $\{x_s - x_r,\ y_s - y_r,\ z_s - z_r\}$ as long as it gets out of the range of the signal repeater. The real trajectory of the drone depends on the desired course and the drone of the motion path repeater, i.e. there are many spoofing scenarios.

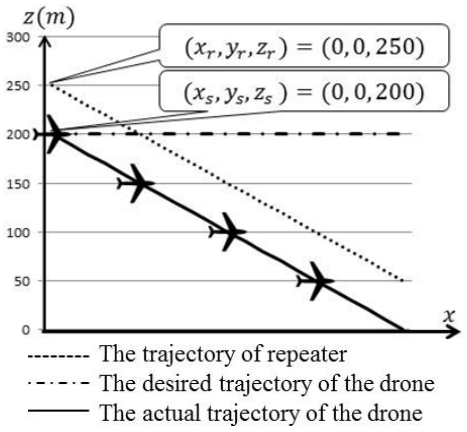

Fig. 8. Repeater shifts the drone in the direction (–z), the coverage of the repeater's signal exceeds 50 m

We assume that the repeater and the drone are parallel courses at different heights with the same speed in the direction x. Suppose that at some time the drone is (Fig. 8) at the point $(0, 0, z_s = 200\text{ m})$, and repeater is at $(0, 0, z_r = 250\text{ m})$ on a distance $\Delta z = 50$ m above the drone. Additional offset drone (scheme 7) takes the form:

$$(x_s, y_s, z_s) \rightarrow \{0, 0, z_s - z_r\} \tag{10}$$

i.e. the drone is in the x direction and further moves in a direction $(-z)$ until it leaves the repeater signal coverage or makes "emergency landing".

Conclusions

In the article it was shown that for the technical spoofer realization potential terrorists could use GNSS repeaters. The real trajectory of the vessel depends on the desired course and trajectory of the movement of the repeater, i.e. there are many spoofing scenarios. In this article, are considered only three significantly different scenarios. To detect spoofing attacks use a variety of methods. For example, the authors suggest the use of paired navigators [5] and/or GNSS compasses as detectors GNSS spoofing [6].

References

1. PARKINSON B.W., SPIKER J.J. JR.: Global Positioning System: Theory and Applications. American Institute of Aeronautics and Astronautics, Inc., 1996.
2. HOFMANN-WELLENHOF B., LICHTENEGGER H., COLLINS J.: GPS Theory and Practice. 5th edition, Springer, Wien New York 2001.
3. SPECHT C.: System GPS. Biblioteka Nawigacji 1, Wydawnictwo Bernardinum, Pelplin 2007.
4. JANUSZEWSKI J.: Systemy satelitarne GPS, Galileo i inne. PWN, 2010.
5. OCHIN E., LEMIESZEWSKI Ł., LUSZNIKOV E., DOBRYAKOVA L.: 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, 159–165.
6. DOBRYAKOVA L., LEMIESZEWSKI Ł., LUSZNIKOV E., OCHIN E.: Применение спутникового компаса для обнаружения ГНСС-спуфинга. Scientific Journals Maritime University of Szczecin 37(109), 2014, 28–33.

Others

7. GPS Standard Positioning Service (SPS) Performance Standard. 4th Edition (now in effect), September 2008.
8. MONTGOMERY P.Y., HUMPHREYS T.E., LEDVINA B.M.: Receiver-Autonomous Spoofing Detection: Experimental Results of a Multi-antenna Receiver Defense against a Portable Civil. GPS Spoofer ION 2009 International Technical Meeting, 2009.
9. TIPPENHAUER N.O., PÖPPER CH., RASMUSSEN K.B., CAPKUN S.: On the Requirements for Successful GPS Spoofing Attacks. http://www.syssec.ethz.ch/research/ccs139-tippenhauer.pdf
10. DOBRYAKOVA L., LEMIESZEWSKI Ł., OCHIN E.: Antyterroryzm – projektowanie i analiza algorytmów antyspoofingu dla globalnych nawigacyjnych systemów satelitarnych. Scientific Journals Maritime University of Szczecin 30(102), 2012, 93–101.
11. University NAVSTAR Consortium (UNAVCO) http://www.colorado.edu/geography/gcraft/notes/gps/gps_f.html