Scientific Journals
of the Maritime University of Szczecin

Zeszyty Naukowe
Akademii Morskiej w Szczecinie

2016, 46 (118), 181–188
ISSN 1733-8670 (Printed)
ISSN 2392-0378 (Online)
DOI: 10.17402/135

Received: *31.08.2015*
Accepted: *25.05.2016*
Published: *27.06.2016*

The vulnerability of unmanned vehicles to terrorist attacks such as Global Navigation Satellite System spoofing

Larisa Dobryakova[1], Łukasz Lemieszewski[2], Evgeny Ochin[2]

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

Key words: GNSS, navigation, jammer, jamming, anti-jamming, spoofer, spoofing, anti-spoofing, repeater

Abstract

Spoofing, anti-spoofing, jamming, and anti-jamming algorithms have become an important research topic within the Global Navigation Satellite System (GNSS) discipline. While many GNSS receivers leave large space for signal dynamics, enough power space is left for the GNSS signals to be spoofed. GNSS signal power on the earth's surface is around 160 dBW. The goal of spoofing is to provide the receiver with a slightly more powerful misleading signal, stronger than the original GNSS signal, fooling the receiver into using fake signals for positioning calculations. The receiver will generate a misleading position of the navigator. Practical spoofing that provides misleading navigation results of the receiver is difficult to conduct due to the signal infrastructure. Using trivial anti-spoofing algorithms in GNSS receivers, spoofing attacks can be easily detected. The article discusses the vulnerability of unmanned vehicles and provides an approach to anti-spoofing based on measuring distance between two antennas.

Introduction

Navigating with a compass and map is an essential skill for many incident positions. Even with new technology, such as Global Navigation Satellite System (GNSS) receivers, map and compass skills are still needed. Confidence with navigation skills comes with practice and proficiency. This confidence level often impacts how a person performs during a crisis – which can result in life or death decisions. Unmanned vehicles (UVs) are becoming a fact of life. The need for such equipment poses a lot of problems, the most important of which are shown in Figure 1.

To understand the problems of UVs, they should be classified in terms of methods of control (Figure 2) and on their environmental context (Figure 3).

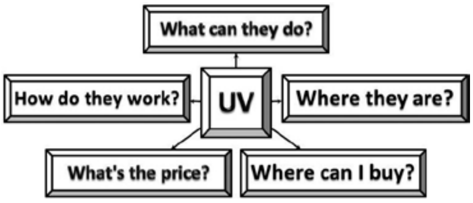

Figure 1. Equipment of UV and related issues

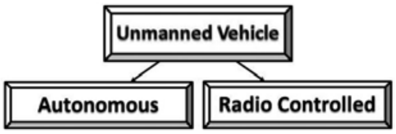

Figure 2. Classification of UV on methods of control

The term "unmanned" implies the absence of a pilot on board the UV, but admits the presence of a remote human operator (remote control). If there is no pilot and no remote human operator, such a UV is referred to as "autonomous."

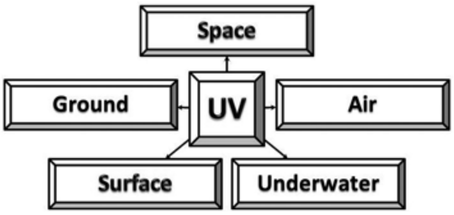

Figure 3. Classification of UV on the environment

The development of modern and advanced technologies allows the UV to successfully perform functions which in the past were not available to them, or were performed by other forces and means. In particular, UVs turn out be highly effective in carrying out the tasks of monitoring of roads, pipelines, farmland, forest fires, rivers, lakes, seas and oceans, searching for fish, and others. An unmanned vehicle prevails in those industries that are remote from humans. This is primarily warehouse logistics, mining, and others. UVs allow you to track and monitor the development of the situation in a given area or for a given route in real time.

It should be noted that the driving force of UV development is special purpose technology and above all the military (Dual-Use System). And it is not only the traditional systems of military intelligence, but also rapidly developing electronic warfare systems, including mobile systems, noise suppression radar, and radio navigation systems (*jamming*) (e-Navigation FAQ, 2015) and mobile jamming and/or *spoofing* of GNSS signals (BLN GPS, 2007).

The main advantage of UVs is that there is no person on board so that, regardless of the complexity and danger of the task performed by the UV, human life is not in danger. It does not need sophisticated life-support systems for the crew. In a crisis situation a drone can be sacrificed. Due to their advantages, UVs are taking over many of the functions of manned vehicles.

Basic notation and definitions

UV – Unmanned Vehicle (AUVSI, 2015);

BNC – On-Board Navigation and Control system, user segment (Chao, Cao & Chen, 2010; e-Navigation FAQ, 2015);

LNC– Land Navigation system and Control (BLN GPS, 2007);

INS – Inertial Navigation System (NavLab, 2015);

GNSS – Global Navigation Satellite System (GNSS, 2015);

$SV_i, i = \overline{1, N}$ – Satellite Vehicles (NS, 2015);

V – Vehicle (boat, car, plane, or drone etc.);

(x_v, y_v, z_v) – coordinates of UV;

Positioning – technology to determine the own position in space (x_v, y_v, z_v) and in time (t_v);

SPS – Standard Positioning Service: level of GNSS positioning precision, based on C/A-encoded;

C/A – encoded (Coarse/Acquisition code): Standard GNSS signal for positioning of a civil person;

R – repeater of GNSS signals (Petovello & Jee, 2009);

(x_r, y_r, z_r) – the coordinates of the repeater R;

(Δx, Δy, Δz) – coordinate error of the vehicle V, which was created by the repeater R;

c – speed of light;

EW – Electronic Warfare (EW, 2007);

Jamming – suppression of GNSS signals by a noise generator (Pullen and Gao, 2012; Scott, 2012);

Anti-jamming – counteraction of jamming;

Spoofing – falsification of GNSS signals (Scott, 2012, 2013);

Anti-spoofing – counteraction of spoofing (Jafarnia-Jahromi et al., 2012; Ochin, 2012a).

Generalized operation of unmanned vehicles

One of the main areas of civilian application of UVs is supervisory functions. Using UVs we can control both the technical condition of the objects and their safety and operation, with objects able to be monitored or controlled from a long distance. For example, the fuel and energy enterprise (FEC) have in their structure hundreds of thousands of kilometers of pipelines, which are poorly protected, and in some areas are not protected at all; hence the energy companies are interested in using unmanned aircraft vehicles (UAVs).

During the assignment, UV control is carried out automatically by the BNC – on-board navigation and control system – which includes:

- satellite navigation receiver capable of receiving navigation data from the GNSS;
- INS, which provides the definition of the orientation and motion parameters of the UV;
- system of sensors capable of measuring the height and speed of the UV;
- different types of antenna and telecommunication equipment designed for flight.

The on-board navigation and control system provides:

- flight on a given route;

- change route assignments;
- return to the starting point of the team from the ground control station;
- circling a point;
- auto tracking of selected target;
- stabilization of the orientation angles UV;
- maintaining the desired altitude and airspeed;
- collection and transmission of telemetry information about the parameters of flight and the hardware;
- equipment management software.

On-board communication system:

- operates within the permitted range of radio frequencies;
- provides data transmission from on-board to the land and from the land to on-board.

Data transmitted from on-board to the land:

- telemetry options;
- streaming video and stills.

The data received on-board comprises:

- commands of the UV;
- control commands for equipment.

Information obtained from the UV, classifies the operator of LNC (Land Navigation system and Control) or directly on-board computer of UV.

Interference with unmanned vehicles

For positioning, the UV uses GNSS. GNSS corrects the work of the INS. Creation of a field of radio interference for GNSS neutralizes a UV. Monitoring information which is not accurately mapped to ground positions has no significant value. Furthermore the UV itself, without knowing its coordinates with a high probability, cannot return to the base, and will be lost. In areas where there are woods or forest, it is not possible to see an object of interest (such as a human or animal) under the trees, even in the winter when there are no leaves on the trees. Hence in each UV instruction manual, it is recommended to use it in treeless terrain with smooth relief, i.e. ideally in deserts and over water.

The importance of UVs as a means of electronic warfare should be emphasized, i.e., media jammers and/or spoofers of GNSS. In this case, the radar will observe hundreds of decoys and the GNSS receiver will switch from real GNSS signals to false ones.

Technical vulnerability of unmanned vehicles

There are many technical vulnerabilities of UVs, the main ones being:

- GNSS signals can be falsified, i.e. intercepted and replaced (GNSS spoofing) (Scott, 2012, 2013).
- If GNSS signals cannot be intercepted and replaced, it is always possible to implement the suppression of GNSS signals via radio noise generator (GNSS jamming) (Pullen and Gao, 2012; Scott, 2012).
- UV receivers can be disabled using directional microwave radiation (wireless power transmission) (Jafarnia-Jahromi et al., 2012).

In this article we consider only the first two vulnerabilities: GNSS jamming and spoofing.

Generation of radio noise to suppress GNSS signals (GNSS jamming)

The availability and usage of low-cost GNSS jamming devices has resulted in the increased threat of intentional and unintentional disruption to commercial and industrial systems that rely on precise GNSS data. The basic scheme of jamming is shown in Figure 4.

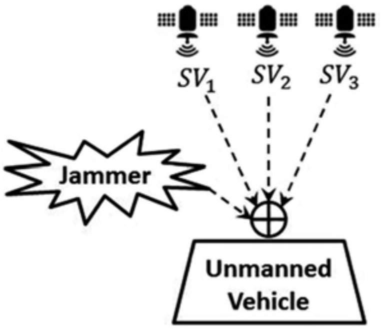

Figure 4. Suppression of GNSS signals via radio noise generator (GNSS jamming)

Falsification of GNSS signals (GNSS spoofing)

A spoofing attack on GNSS – an attack that tries to cheat the GNSS receiver, broadcasts a slightly more powerful signal, which is received from GNSS satellites, but distorted, so that the positioning system of the UV incorrectly determines its position in space and time. That is, the purpose of spoofing is a manipulation of the GNSS signal to a receiver: instead of the real UV coordinates of space and time (x_v, y_v, z_v, t_v) expected. False coordinates ($x_v + \Delta x$, $y_v + \Delta y$, $z_v + \Delta z$, $t_v + \Delta t$) are received, where Δx, Δy, Δz, Δt are the coordinate errors of the UV in space and time, by repeater R. One example of the capture of a Lockheed RQ 170 drone in Iran in 2011 was the result of such an attack (Peterson, 2011). In 2012, it proved the feasibility of hacking and interception of UV control by GNSS spoofing (BBC, 2012), and already in 2013 it was possible to prove it in practice (UT News, 2013). In 2014, a UAV MQ-5B vehicle was forced to make an emergency landing (New

Factoria, 2014). All researchers note that successful GNSS spoofing can only be performed for positioning systems that use a standard positioning service (unencrypted civil C/A code) (RT, 2012). Our research has shown that the use of simple special purpose spoofer based on a GNSS signal repeater provides loss of UV control, using Y-coding, which is an encrypted version of the P-code in anti-spoofing mode (Ochin, 2012b).

Timer error of UV and especially the use of GNSS repeater

3D navigation

The distance from SV_i to UV (V on Figure 5) can be written as:

$$s_i = \sqrt{(x_i - x_v)^2 + (y_i - y_v)^2 + (z_i - z_v)^2} = ct_i$$
$$i = \overline{0, N-1} = 0, 1, 2, ..., N-1 \qquad (1)$$

Since the measurement of the distance from the UV to satellites is performed by measuring the propagation time $T_i = t_i + \Delta t$ GNSS signal from SV_i to V, Equation (1) for $N = 4$ can be represented as:

$$\begin{cases} \sqrt{(x_1 - x_v)^2 + (y_1 - y_v)^2 + (z_1 - z_v)^2} = c\,(T_1 - \Delta t) \\ \sqrt{(x_2 - x_v)^2 + (y_2 - y_v)^2 + (z_2 - z_v)^2} = c\,(T_2 - \Delta t) \\ \sqrt{(x_3 - x_v)^2 + (y_3 - y_v)^2 + (z_3 - z_v)^2} = c\,(T_3 - \Delta t) \\ \sqrt{(x_4 - x_v)^2 + (y_4 - y_v)^2 + (z_4 - z_v)^2} = c\,(T_4 - \Delta t) \end{cases} \qquad (2)$$

The corresponding timing diagram of 3D navigation is shown in Figure 6.

The UV processor solves the system of equations (2), calculates the position UV (x_v, y_v, z_v) and measurement error of time Δt, which is used to correct the timer UV (receiver clock error as difference between UV time and GNSS system time).

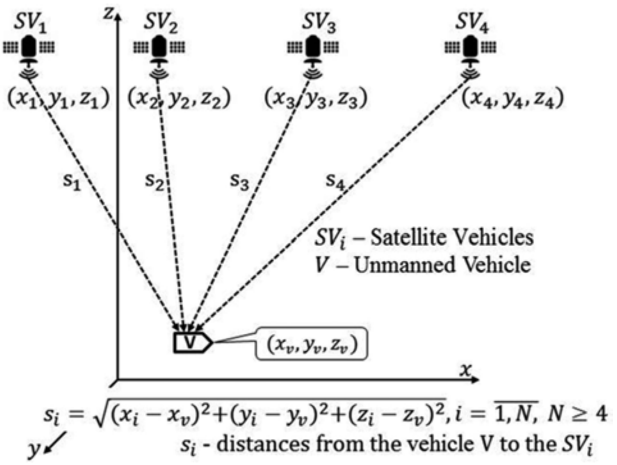
SV_1
SV_2
SV_3
SV_4
z
(x_1, y_1, z_1)
(x_2, y_2, z_2)
(x_3, y_3, z_3)
(x_4, y_4, z_4)
s_1
s_2
s_3
s_4
SV_i – Satellite Vehicles
V – Unmanned Vehicle
V
(x_v, y_v, z_v)
x
y
$s_i = \sqrt{(x_i - x_v)^2 + (y_i - y_v)^2 + (z_i - z_v)^2}, i = \overline{1, N}, N \geq 4$
s_i - distances from the vehicle V to the SV_i

Figure 5. 3D navigation

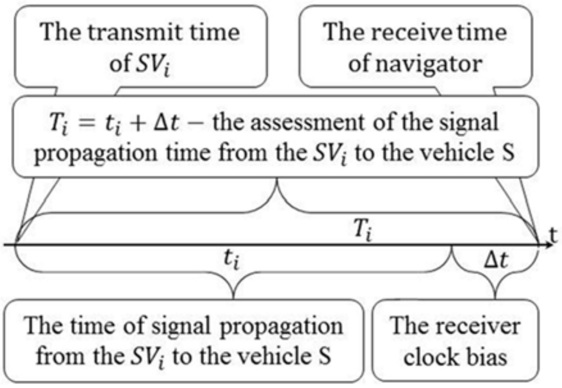
The transmit time of SV_i
The receive time of navigator
$T_i = t_i + \Delta t$ – the assessment of the signal propagation time from the SV_i to the vehicle S
T_i
t
t_i
Δt
The time of signal propagation from the SV_i to the vehicle S
The receiver clock bias

Figure 6. Timing diagram of 3D navigation

2D navigation

The navigation of ground objects such as cars, and aircraft equipped with barometric and/or radio altimeters, does not need to measure the {z} coordinate using satellites. In this case the distance from the SV_i to the vehicle V (Figure 7) can be written as:

$$s_i = \sqrt{(x_i - x_s)^2 + (y_i - y_s)^2} = ct_i$$
$$i = \overline{0, N-1}, \quad N \geq 3 \qquad (3)$$

It is important to note that the distance s_i includes the difference between the {z} coordinate of the satellite and the known {z} of the UV in the 3D case, but here in this instance in 2D.

Since the measurement of the distance from the vehicle to the satellites is performed by measuring the propagation time $T_i = t_i + \Delta t$ of GNSS signals

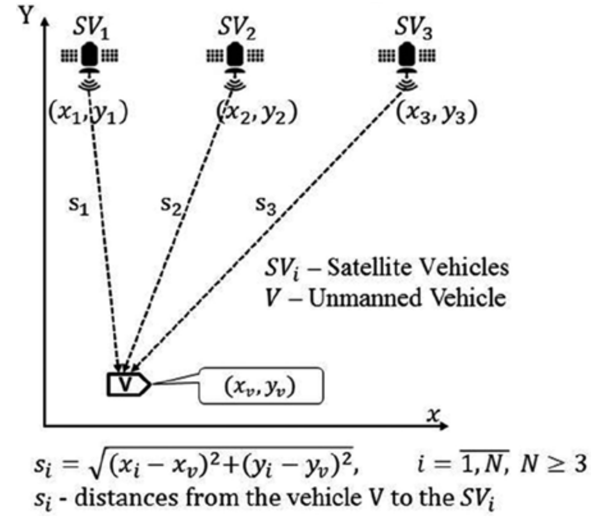
Y
SV_1
SV_2
SV_3
(x_1, y_1)
(x_2, y_2)
(x_3, y_3)
s_1
s_2
s_3
SV_i – Satellite Vehicles
V – Unmanned Vehicle
V
(x_v, y_v)
x
$s_i = \sqrt{(x_i - x_v)^2 + (y_i - y_v)^2}, \quad i = \overline{1, N}, N \geq 3$
s_i - distances from the vehicle V to the SV_i

Figure 7. 2D navigation

from the SV_i to the vehicle V (Figure 2) then (3) can be represented as:

$$\begin{cases} \sqrt{(x_1 - x_v)^2 + (y_1 - y_v)^2} = c\,(T_1 - \Delta t) \\ \sqrt{(x_2 - x_v)^2 + (y_2 - y_v)^2} = c\,(T_2 - \Delta t) \\ \sqrt{(x_3 - x_v)^2 + (y_3 - y_v)^2} = c\,(T_3 - \Delta t) \end{cases} \tag{4}$$

The processor of a UV solves the system of equations (4), computes the position of the vehicle (x_v, y_v) and time measurement errors of the vehicle Δt, and this is used as a clock correction of the UV.

1D navigation

The navigation of rail transport that moves in one direction, for example in the $\{x\}$ direction, does not need to measure the $\{y, z\}$ coordinates using satellites. In this case the distance from the SV_i to the vehicle V (Figure 8) can be written as:

$$\begin{aligned} s_i &= \sqrt{(x_i - x_v)^2} = ct_i \\ i &= \overline{0, N-1}, \quad N \geq 2 \end{aligned} \tag{5}$$

We consider only the case of rail transport navigation that moves in one direction, for example in the $\{x\}$ direction. Such a situation has no practical significance, and is here only to facilitate understanding of the theory of 2D navigation. The spatial arrangement between satellites and train is unrealistic but such situation is here only to facilitate understanding of the theory of 2D navigation.

Since the measurement of the distance from the vehicle to the satellites is performed by measuring the propagation time $T_i = t_i + \Delta t$ of GNSS signals from the SV_i to the vehicle V (Figure 2) then (5) can be represented as:

$$\begin{cases} \sqrt{(x_1 - x_v)^2} = c\,(T_1 - \Delta t) \\ \sqrt{(x_2 - x_v)^2} = c\,(T_2 - \Delta t) \end{cases} \tag{6}$$

The processor of a UV solves the system of equations (6), computes the position of the vehicle (x_v) and time measurement errors aboard the vehicle Δt, and it is used as a clock correction of the GNSS navigator.

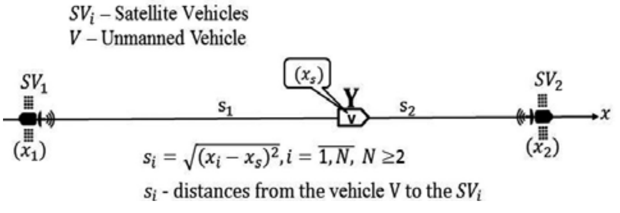
SV_i – Satellite Vehicles
V – Unmanned Vehicle
SV_1
(x_s)
Y
SV_2
s_1
V
s_2
x
(x_1)
$s_i = \sqrt{(x_i - x_s)^2}, i = \overline{1, N}, N \geq 2$
(x_2)
s_i - distances from the vehicle V to the SV_i

Figure 8. 1D navigation

Neutralization of UV timer error (1D navigation)

UV timer error can be neutralized. We show this in version 1D navigation (Figure 9). Determination of the UV position using signals from satellites SV_1 given by the equation:

$$x_1'' = x_1' + c\,(t_1'' + \Delta t - t_1') \tag{7}$$

and determination of the UV position using signals from satellites SV_2 given by the equation:

$$x_2'' = x_2' - c\,(t_2'' + \Delta t - t_2') \tag{8}$$

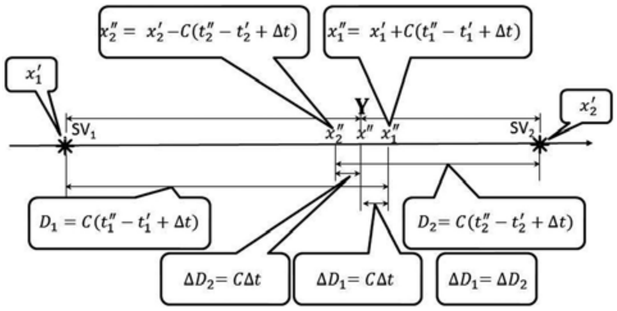
$x_2'' = x_2' - C(t_2'' - t_2' + \Delta t)$
$x_1'' = x_1' + C(t_1'' - t_1' + \Delta t)$
x_1'
Y
SV_1
x_2''
x''
x_1''
SV_2
x_2'
$D_1 = C(t_1'' - t_1' + \Delta t)$
$D_2 = C(t_2'' - t_2' + \Delta t)$
$\Delta D_2 = C\Delta t$
$\Delta D_1 = C\Delta t$
$\Delta D_1 = \Delta D_2$

Figure 9. The neutralization of UV timer error Δt

Measurement error distance ΔD from UV to the satellite, which is determined by the inaccuracy of the UV timer, leads to a situation of UV uncertainty, i.e. the UV is simultaneously at the two points in space $\{x''+\Delta D\}$ and $\{x''-\Delta D\}$, and the distance between these points is equal to $2\Delta D$. The exact UV position in space is defined as:

$$\begin{aligned} x'' &= \frac{x_1'' + x_2''}{2} = \\ &= \frac{x_1' + x_2' + c\,(t_1'' + \Delta t - t_1') - c\,(t_2'' + \Delta t - t_2')}{2} = \\ &= \frac{x_1' + x_2' + c\,((t_1'' - t_1') - (t_2'' - t_2'))}{2} \end{aligned} \tag{9}$$

where:

t'_1, t'_2 – the departure time of the broadcasts from transmitters SV_1 and SV_2;
t''_1, t''_2 – the exact time receiving a message from the transmitters SV_1 and SV_2;
x'_1, x'_2 – the position of transmitters SV_1 and SV_2;
x''_1, x''_2 – the UV position with error ΔD;
x'' – the exact UV position.

$$\left\langle \begin{aligned} x'' &= \frac{x_1' + x_2' + c\,((t_1'' - t_1') - (t_2'' - t_2'))}{2} = \\ &= \frac{\overbrace{\{x_1' + c\,(t_1'' - t_1')\}}^{= x''} + \overbrace{\{x_2' - c\,(t_2'' - t_2')\}}^{= x''}}{2} = \frac{x'' + x''}{2} \end{aligned} \right\rangle$$

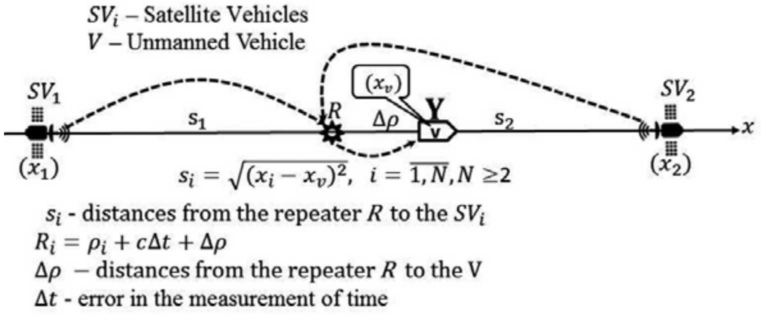
SV_i – Satellite Vehicles
V – Unmanned Vehicle
SV_1
(x_1)
s_1
R
(x_v)
$\Delta\rho$
V
s_2
SV_2
(x_2)
x
$s_i = \sqrt{(x_i - x_v)^2},\ i = \overline{1,N}, N \geq 2$
s_i - distances from the repeater R to the SV_i
$R_i = \rho_i + c\Delta t + \Delta\rho$
$\Delta\rho$ – distances from the repeater R to the V
Δt - error in the measurement of time

Figure 10. 1D navigation using GNSS repeater

Neutralization of UV timer error (2D and 3D navigation)

It can be shown that the approach of the fallback timer can neutralize the UV timer error in 2D and 3D space.

1D navigation using GNSS repeater

In the section *Neutralization of UV timer error* (*1D navigation*) it was shown how UV timer error can be neutralized. Using a similar methodological procedure, we show that, if UV receives GNSS signals from repeater GNSS signals, then the UV does not define its own position, but the repeater coordinates (Figure 10).

The determination of the vehicle position using the UV signal from R is given by the equations:

$$\begin{cases} x_1'' = x_1' + c\left(t_1'' + \Delta t + \dfrac{\Delta\rho}{c} - t_1'\right) \\ x_2'' = x_2' - c\left(t_2'' + \Delta t + \dfrac{\Delta\rho}{c} - t_2'\right) \end{cases} \tag{10}$$

for measuring the distance error ΔD from the UV to the satellite, which is determined by the inaccuracy of the UV timer Δt, added signal delay $\Delta\rho/c$ through the dissemination of radio waves from repeater to UV. The delay $\Delta\rho/c$ can be interpreted as an additional error timer, because the delay is similar for all SV_i. This total error $\Delta t' = \Delta t + \Delta\rho/c$ leads to a situation of uncertainty in UV position, i.e. the UV is simultaneously at the two points in space $x''+\Delta D$ and $x''-\Delta D$, and the distance between these points is equal to $2\Delta D$. The exact UV position in space is defined as (11):

$$x'' = \frac{x_1'' + x_2''}{2} = \frac{x_1' + x_2' + c\left(t_1'' + \Delta t + \dfrac{\Delta\rho}{c} - t_1'\right) - c\left(t_2'' + \Delta t + \dfrac{\Delta\rho}{c} - t_2'\right)}{2} = \frac{x_1' + x_2' + c\left(\left(t_1'' - t_1'\right) - \left(t_2'' - t_2'\right)\right)}{2} \tag{11}$$

Using a similar methodological procedure we can show that, if the UV receives signals from a GNSS repeater, it does not define its own UV coordinates but the repeater's coordinates in 2D or 3D space. This property of GNSS repeater was first used by Mark Petovello and Gyu-In Jee in their article (Petovello & Jee, 2009) to solve the problem of positioning indoors, with impeded propagation of GNSS signals. Here is the quote from that paper: "Therefore, the extra path delay (through the repeater) is common to all satellites in view, and is thus indistinguishable from the receiver clock offset."

The main scenario of GNSS spoofing

The main scenario of GNSS spoofing is shown in Figure 11. The UV during normal operation carries traffic using GNSS. The terrorist, located at a distance from the UV, receives GNSS signals, distorts

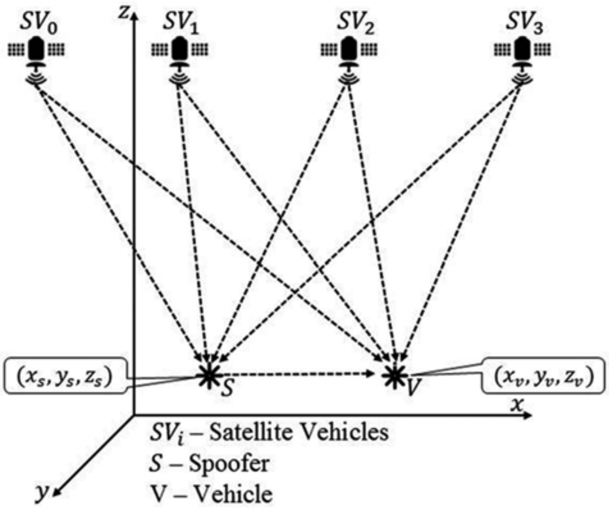

Figure 11. The main scenario of GNSS spoofing (designate)

them and broadcasts to the vehicle UV high power signal, sufficient to switch its navigation equipment from the normal mode of GNSS into GNSS spoofing.

Spoofing detection using two-antenna UV

Assume that the on-board navigation system and management of the UV has two antennas and two corresponding positioning modules N_1 and N_2. Assume also that N_1 is located at a distance D_1 from the spoofer and the processor of N_1 solves the system of equations (2), computes the false position of the vehicle (x_1^f, y_1^f, z_1^f) and the measurement error aboard the UV is Δt. Assume also that N_2 located at a distance D_2 from the spoofer and the processor of N_2 solves the system of equations (2), also computes the false position of the vehicle (x_2^f, y_2^f, z_2^f) and the measurement error aboard the UV is Δt. If we designate:

$$\Delta D = D_1 - D_2 \tag{12}$$

the system of equations (2) for N_2 can be written as:

$$\begin{cases} \sqrt{(x_1-x_s)^2+(y_1-y_s)^2+(z_1-z_s)^2} = \\ \quad = c\left(T_{\downarrow 1}^s - T_{\uparrow 1} + \Delta t + \dfrac{\Delta D}{c}\right) \\ \sqrt{(x_2-x_s)^2+(y_2-y_s)^2+(z_2-z_s)^2} = \\ \quad = c\left(T_{\downarrow 2}^s - T_{\uparrow 2} + \Delta t + \dfrac{\Delta D}{c}\right) \\ \sqrt{(x_3-x_s)^2+(y_3-y_s)^2+(z_3-z_s)^2} = \\ \quad = c\left(T_{\downarrow 3}^s - T_{\uparrow 3} + \Delta t + \dfrac{\Delta D}{c}\right) \\ \sqrt{(x_4-x_s)^2+(y_4-y_s)^2+(z_4-z_s)^2} = \\ \quad = c\left(T_{\downarrow 4}^s - T_{\uparrow 4} + \Delta t + \dfrac{\Delta D}{c}\right) \end{cases} \tag{13}$$

where:

$T_{\downarrow 1}^s, T_{\downarrow 2}^s, T_{\downarrow 3}^s, T_{\downarrow 4}^s$ – transmission times of messages from satellites 1, 2, 3, and 4;

$T_{\uparrow 1}^s, T_{\uparrow 2}^s, T_{\uparrow 3}^s, T_{\uparrow 4}^s$ – receive times of messages from satellites 1, 2, 3, and 4.

In this case, the processor of N_2 solves the system of equations (10) where we have 3D situation. The two modules N_1 and N_2 receive the same signals from the spoofer (the difference is only in the signal delay) and so they calculate identically the false position of the vehicle (x_2^f, y_2^f, z_2^f) = (x_1^f, y_1^f, z_1^f)) and the measurement error aboard the vehicle $\Delta t + \Delta D/c$. Comparing equations (2), (10) and (11), we can write:

$$(x_s, y_s, z_s) = \left(x_1^f, y_1^f, z_1^f\right) = \left(x_2^f, y_2^f, z_2^f\right) \tag{14}$$

which means that all UVs under the influence of signals from the spoofer determine the same false coordinates, and therefore the measured distance between the navigators should approach zero.

$$\Delta D_{1-2} = \sqrt{\left(x_1^f - x_2^f\right)^2 + \left(y_1^f - y_2^f\right)^2 + \left(z_1^f - z_2^f\right)^2} \tag{15}$$

This property is the basis of the decision rule system for GNSS spoofing detection and the operating principle is shown in Figure 12.

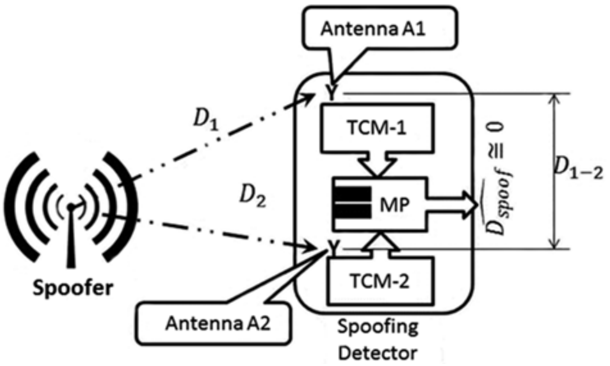

Figure 12. A single-antenna spoofer and a two-antenna Spoofing Detector (SD): Y – antenna SD; D1 and D2 – distances from the spoofer antenna to antenna of SD; MP – microprocessor that calculates the distance between the antennas and implements the decision rule; D_{1-2} – the true distance between the antennas

Conclusions

It is now known that there are a variety of approaches to the problem of spoofing detection. For example, the authors have developed several methods for spoofing detection (Ochin, 2012a; Ochin, Dobryakova & Lemieszewski, 2012; 2013). In other papers we study some of the spoofer's properties with help of a GNSS signal repeater (Dobryakova, Lemieszewski & Ochin, 2013; Ochin et al., 2013), leading us to analyze the detection and anti-spoofing of GNSS controlled drones (Ochin, 2014). We have also used the application of a satellite compass for GNSS spoofing detection (Dobryakova et al., 2014). We have also saved the application of a GNSS signal repeater as a spoofer (Dobryakova, Lemieszewski & Ochin, 2014a; Dobryakova and Ochin, 2014), and used this to increase transport safety (Dobryakova, Lemieszewski & Ochin, 2014b; 2014c). Currently we plan to present a new approach to GNSS spoofing detection and anti-spoofing on shielding of antennas.

References

1. AUVSI (2015). *Association for Unmanned Vehicles Systems International* [Online] Available from: http://www.auvsi.org [Accessed: August 20, 2015]
2. BBC (2012) [Online] Available from: http://www.bbc.com/russian/science/2012/06/120629_drone_spoof_hack.shtml
3. BLN GPS (2007) *Basic Land Navigation, Global Positioning System*, page 5.1. National Interagency Incident Management System, 2007. [Online] Available from: http://www.nwcg.gov/sites/default/files/products/pms475.pdf [Accessed: August 20, 2015]
4. Chao, H.Y., Cao, Y.C. & Chen, Y.Q. (2010) Autopilots for Small Unmanned Aerial Vehicles: A Survey. *International Journal of Control, Automation, and Systems* 8(1), pp. 36–44.
5. Dobryakova, L. & Ochin, E. (2014) On the application of GNSS signal repeater as a spoofer. *Scientific Journals of the Maritime University of Szczecin* 40 (112). pp. 53–57.
6. Dobryakova, L., Lemieszewski, Ł. & Ochin, E. (2013) *GNSS: povyšenie točnosti pozicionirovaniâ s ispol'zovaniem modeli WCS-84. Modelûvannâ ta informacijni tehnologij. Zbirnik naukovyh prac'*. Vypusk 68, Kijev 2013, UKD 621.396+681.511.
7. Dobryakova, L., Lemieszewski, Ł. & Ochin, E. (2014a) Design and analysis of spoofing detection algorithms for GNSS signals. *Scientific Journals of the Maritime University of Szczecin* 40 (112). pp. 47–52.
8. Dobryakova, L., Lemieszewski, Ł. & Ochin, E. (2014b) Transport safety: the GNSS spoofing detecting using two navigators. *Logistyka* 3. pp. 1328–1331.
9. Dobryakova, L., Lemieszewski, Ł. & Ochin, E. (2014c) The main scenarios of GNSS spoofing and corresponding spoofing detection algorithms. *Logistyka* 4. pp. 2751–2761.
10. Dobryakova, L., Lemieszewski, Ł., Lusznikov, E. & Ochin, E. (2014) The application of satellite compass for GNSS-spoofing detecting. *Scientific Journals of the Maritime University of Szczecin* 37 (109). pp. 28–33.
11. e-Navigation FAQ (2015) *e-Navigation Frequently Asked Questions*. [Online] Available from: http://www.iala-aism.org/about/faqs/enav.html [Accessed: August 20, 2015]
12. EW (2007) *Electronic Warfare*. Joint Publication 3-13.1. 25 January 2007. [Online] Available from: http://fas.org/irp/doddir/dod/jp3-13-1.pdf [Accessed: August 20, 2015]
13. GNSS (2015) *Global Navigation Satellite System*. [Online] Available from: https://www.princeton.edu/~alaink/Orf467F07/GNSS.pdf [Accessed: August 20, 2015]
14. Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J. & Lachapelle, G. (2012) GPS Vulnerability to Spoofing Threats and a Review of Anti-spoofing Techniques. *International Journal of Navigation and Observation* 2012, Article ID 127072, doi:10.1155/2012/127072.
15. NavLab (2015) *Introduction to inertial navigation.* [Online] Available from: http://www.navlab.net/ Publications/Introduction_to_Inertial_Navigation.pdf [Accessed: August 20, 2015]
16. New factoria (2014) *Kompleks "Avtobaza" zasek i posadil amerikanskiy BPLA MQ-5B v Krymu*. [Online] Marz 2014. Available from: http://rbase.new-factoria.ru/news/kompleks-avtobaza-zasek-i-posadil-amerikanskiy-bpla-mq-5b-v-krymu [Accessed: August 20, 2015]
17. NS (2015) *Navigation satellite*. [Online] Available from: http://www.infoplease.com/encyclopedia/science/navigation-satellite.html [Accessed: August 20, 2015]
18. Ochin, E. (2012a) *Anty-spoofingowa architektura GPS do systemów nawigacji bezzałogowej*. [Online] Available from: https://youtu.be/TLUD26xfEfQ?list=PL0C885EF8A83CA824 [Accessed: August 20, 2015]
19. Ochin, E. (2012b) *Antyterroryzm – projektowanie i analiza algorytmów antyspoofingu dla GNSS*. [Online] May. Available from: https://youtu.be/mQpY9R-pIPo [Accessed: August 20, 2015]
20. Ochin, E. (2014) *Spoofing detection and anti-spoofing for GNSS controlled drones, bombs and artillery shells* (in English and Russian languages). [Online] Available from: https://youtu.be/0PlQoAynIQo [Accessed: August 20, 2015]
21. Ochin, E., Dobryakova, L. & Lemieszewski, Ł. (2012) Antiterrorism – design and analysis of GNSS anti-spoofing algorithm. *Scientific Journals of the Maritime University of Szczecin* 30 (102). pp. 93–101.
22. Ochin, E., Dobryakova, L. & Lemieszewski, Ł. (2013) The analysis of the detecting algorithms of GNSS-spoofing. *Scientific Journals of the Maritime University of Szczecin* 36 (108) z. 2. pp. 30–36.
23. Ochin, E., Lemieszewski, Ł., Lusznikov, E. & Dobryakova, L. (2013) The study of the spoofer's some properties with help of GNSS signal repeate*r. Scientific Journals of the Maritime University of Szczecin* 36 (108) z. 2. pp. 159–165.
24. Peterson, S. (2011) *Exclusive: Iran hijacked US drone, says Iranian engineer (Video)*. [Online] December 15. Available from: http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video [Accessed: August 20, 2015]
25. Petovello, M. & Jee, G.I. (2009) *GNSS Solutions: What is GNSS repeater-based positioning and how is it different from using pseudolites?* Inside GNSS. Global Navigation Satellite Systems. Engineering, Policy and Design. pp. 18–21. [Online] July/August 2009. Available from: http://www.insidegnss.com/auto/julyaug09-GNSS-Sol.pdf [Accessed: August 20, 2015]
26. Pullen, S. & Gao, G.X. (2012) *GNSS Jamming in the Name of Privacy. Potential Threat to GPS Aviation*. Inside GNSS. Global Navigation Satellite Systems. Engineering, Policy and Design. pp. 34–43. [Online] March/April 2012. Available from: http://www.insidegnss.com/auto/marapr12-Pullen.pdf [Accessed: August 20, 2015]
27. RT (2012) *Texas college hacks drone in front of DHS*. [Online] June 2012. Available from: http://rt.com/usa/texas-1000-us-government-906 [Accessed: August 20, 2015]
28. Scott, L. (2012) *Spoofs, Proofs & Jamming. Towards a Sound National Policy for Civil Location and Time Assurance*. Inside GNSS. Global Navigation Satellite Systems. Engineering, Policy and Design. pp. 42, 44–53. [Online] September/October 2012. Available from: http://www.insidegnss.com/auto/2012-sepoct-Scott.pdf [Accessed: August 20, 2015]
29. Scott, L. (2013) *Spoofing: Upping the Anti*. Inside GNSS. Global Navigation Satellite Systems. Engineering, Policy and Design. pp. 18–19. [Online] July/August 2013. Available from: http://www.insidegnss.com/auto/IGM_TLS07_13.pdf [Accessed: August 20, 2015]
30. UT News (2013) *UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea*. [Online] July 2013. Available from: http://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea [Accessed: August 20, 2015]