Scientific Journals
Maritime University of Szczecin

Zeszyty Naukowe
Akademia Morska w Szczecinie

2012, 30(102) pp. 93–101

2012, 30(102) s. 93–101

Antiterrorism – design and analysis of GNSS antispoofing algorithms

Antyterroryzm – projektowanie i analiza algorytmów antyspoofingu dla globalnych nawigacyjnych systemów satelitarnych

Evgeny Ochin[1], Larisa Dobryakova[2], Łukasz Lemieszewski[3]

[1] Maritime University of Szczecin, Faculty of Navigation, Institute of Marine Technologies
Akademia Morska w Szczecinie, Wydział Nawigacyjny, Instytut Technologii Morskich
70-500 Szczecin, ul. Wały Chrobrego 1–2, e-mail: e.ochin@am.szczecin.pl
[2] West Pomeranian University of Technology, Faculty of Computer Science and Information Technologies
Zachodniopomorski Uniwersytet Technologiczny, Wydział Informatyki i Technologii Informacyjnych
71-210 Szczecin, ul. Żołnierska 49, e-mail: l.dobryakova@wi.zut.edu.pl
[3] Secondary School of General Education No. 1, Zespół Szkół Zawodowych nr 1
66-400 Gorzów Wielkopolski, ul. Puszkina 31, e-mail: llemieszewski@gmail.com

Key words: GNSS, GPS, GLONASS, GALILEO, antiterrorism, antispoofing

Abstract

Many civil GNSS (Global Navigation Satellite System) applications need secure, assured information for asset tracking, fleet management and the like. But there is also a growing demand for geosecurity location-based services. Unfortunately, GNSS is vulnerable to malicious intrusion and spoofing. How can users be sure that the information they receive is authentic? Spoofing is the transmission of matched-GNSS-signal-structure interference in an attempt to commandeer the tracking loops of a victim receiver and thereby manipulate the receiver's timing or navigation solution. A spoofer can transmit its counterfeit signals from a stand-off distance of several hundred meters, or it can be co-located with its victim. Spoofing attacks can be classified as simple, intermediate, or sophisticated in terms of their effectiveness and subtlety. In an intermediate spoofing attack, a spoofer synchronizes its counterfeit signals with the authentic GNSS signals, so they are code-phase-aligned at the target receiver. In this paper, authors consider the antispoofing algorithms based on finding statistical anomalies in the basic parameters of the satellite signals. At the stage of learning, the system of antispoofing explores the statistical properties of signals and at the phase of spoofing detection, the system used thresholds characteristics of statistical anomalies. The excess of the threshold characteristics provides a basis for probabilistic decision on the presence of spoofing.

Słowa kluczowe: GNSS, GPS, GLONASS, GALILEO, antyterroryzm, antyspoofing

Abstrakt

Wiele cywilnych zastosowań GNSS (Globalnych Nawigacyjnych Systemów Satelitarnych) wymaga pewności, że informacje dotyczące śledzenia zasobów, zarządzania flotą itp. nie są sfałszowane. Na uwagę zasługuje także rosnący popyt na geobezpieczeństwo bazujące na usługach lokalizacji. Niestety GNSS jest podatny na preparowanie i modyfikowanie pakietów danych. Powstaje pytanie: jak użytkownicy mogą być pewni, że informacja, którą otrzymują jest autentyczna? Spoofing (ang. *spoof* – naciąganie, szachrajstwo) jest ingerencją w strukturę transmisji GNSS w celu modyfikacji pętli trasy odbiornika poszkodowanego, skutkiem czego jest manipulacja czasem na odbiorniku lub urządzeniem nawigacyjnym. Osoba podszywająca się może transmitować podrobiony sygnał z ukrycia w odległości do kilkuset metrów lub być współpołożona z jego ofiarą. Ataki spoofingu można zaklasyfikować jako proste, pośrednie i zaawansowane pod względem ich subtelności i efektywności. W ataku pośrednim osoba podszywająca się synchronizuje swój fałszywy sygnał z autentycznym sygnałem GNNS w taki sposób, iż następuje wyrównanie kodu–fazy dla odbiornika sygnału. W artykule przedstawiono algorytmy antyspoofingu, bazujące na znajdowaniu statystycznych anomalii w podstawowych parametrach sygnału satelitarnego. W trakcie funkcjonowania system antyspoofing bada statystyczne własności sygnałów i na etapie wykrycia spoofingu wykorzystuje charakterystyki progu anomalii. Nadmiar cech progowych stanowi podstawę do wykrycia spoofingu.

Introduction

The main requirement for a navigation system is the ability to continuously determine the coordinates of the object with the required of precision. However, during the GNSS exploitation (Global Navigation Satellite System) the situations of the refusal of communication satellites or ground-based control system may arise. The Refusals may lead to the state in which coordinates of object will determine some errors, excess of desired coordinates, therefore to assess the GNSS situation the concept of GNSS **totality** and **continuity** should be used.

GNSS Totality – ability of the system to ensure the prejudice that the system is not able to answer accuracy of posed requirements. Therefore, one of the system tasks to maintain totality in the conditions of excessive information and in the refusal cases of communication equipment onboard one of the satellites is to recognize a damaged satellite and to exclude timely it from GNSS.

GNSS Continuity – GNSS ability to carry out its functions without interruption and deterioration of its characteristics. Therefore, deterioration of the characteristics, until the interruption in operating, is possible in conditions of partial or complete shielding of GNSS signals for any obstacles in the transmission of satellite signals in the direction of the GNSS antennas user.

GNSS signal at the input device provides a summary of the GNSS navigation signals from satellites at the L1 frequency. The signals transmitted by each satellite are composed of a sinusoidal carrier, a satellite-specific pseudorandom spreading code, and a navigation data sequence.

The L1 frequency carries both, C/A-code and P(Y)-code signals, transmitted in phase quadrature. As a result, $S_{\mathrm{L1}}(t)$ signal is available for L1 frequency of GNSS receiver. $S_{\mathrm{L1}}(t)$ signal is composed of the received RF energy $S_i(t)$ from each of N satellites in the visible constellation, plus thermal noise $\eta(t)$:

$$S(t) = \sum_{i=1}^{N} S_i(t) + \eta(t) \tag{1}$$

GNSS signal from i-th satellite can be described as follows [1]:

$$S_i(t) = Am_i(t - \tau_i)\cos\left[\left(\omega_{\mathrm{L1}} + 2\pi f_{d_i}\right)t + \varphi_i\right] \tag{2}$$

where: $S_i(t)$ – GNSS signal from i-th satellite; A – signal amplitude; t – satellite system time; $m_i(t - \tau_i)$ – function, describes the modulation and forwarding the navigation message; φ_i – random initial phase of the signal; ω_{L1} – angular frequency, corresponding to frequency L1 including Doppler shift; $2\pi f_{di}$ – initial phase shift.

GNSS Pseudolites [2] used in the development, production, support the use of satellite equipment users. With Pseudolites satellite equipment contractors are able to:

- model satellite signals and different operating conditions;
- conduct complete control over the performance of different types of test scenarios;
- simulate multiple transfers along the same route, with the same configuration of the satellite group.

This is an important advantage in comparison to conducting testing in real conditions. A real-time method for detecting GNSS spoofing in an arrow--bandwidth civilian GNSS receiver is still being developed. The ability to detect a spoofing attack is important for reliability of systems ranging from cell-phone towers, the power grid, and commercial fishing monitors. A civilian GNSS spoofer is implemented on a digital signal processor. It is used to characterize spoofing effects and to develop ways of defence against civilian spoofing.

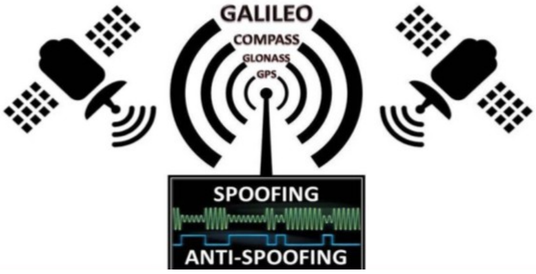

Fig. 1. Antispoofing LOGO of Maritime University of Szczecin
Rys. 1. LOGO antyspoofingu Akademii Morskiej w Szczecinie

This work is intended to equip GNSS users and receiver manufacturers with authentication methods that are effective in dealing with unsophisticated spoofing attacks. In this paper, we consider the anti-spoofing algorithms based on finding statistical anomalies in the basic parameters of the satellite signals. At the stage of functioning, the system of antispoofing explores the statistical properties of signals and at the phase of spoofing detection the system uses thresholds characteristics of statistical anomalies. The excess of the threshold characteristics provides a basis for probabilistic decision on the presence of spoofing.

Spoofing is a technology to intercept network traffic between nodes, arranged in a single wide-domain transmission. The beginnings of anti-spoofing can be seen in the patent 1942 [1], despite the fact that the main purpose of this patent was the fight of the American radio-controlled sea-based torpedoes with a radio jamming of German boats and submarines.

Spoofing is an attack, in which the offender or opponent (a bad Boy) is sending a false packages in order to persuade the victim's computer that the listening computer is the final recipient. Then the packets are sent to the actual recipient. MAC (Media Access Control) – address of the sender is replaced in such a way that the reply packets pass through the listening computer. The listening computer becomes the "gateway" for traffic victims and the offender gets a hearing traffic, for example, e-mail offerings. Breaking computers security is implemented for many decades. Currently, it can not only break the computer communication, but also GNSS.

GNSS Spoofing

Civilian vehicles, such as unmanned aircraft or helicopter, the vessel, truck-type TIR etc., will be called the "navigator" or "GNSS receiver" (in the literature, such vehicle is often called a victim). Navigator moves in space with the civil GNSS procedure (mode L1) and is subjected to an spoofing attack from other vehicles, which will called "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 only GNSS system swhich can't be deceive, are GNSS military systems, that utilizie 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 figure 2. Spoofer is generally located in the immediate vicinity of the navigator and moves in space with civilian or military GNSS mode (L1 or L1/L2).

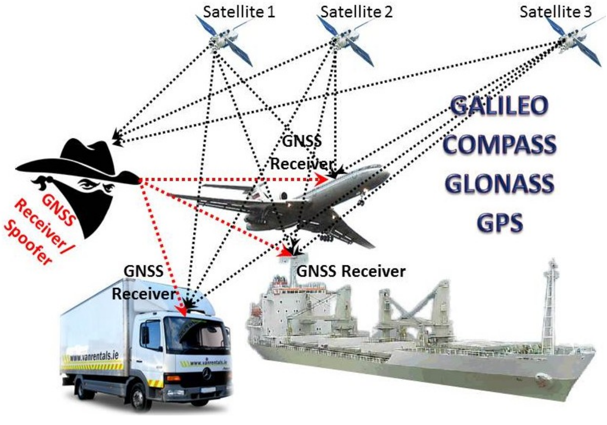

Fig. 3. GNSS Spoofing
Rys. 3. GNSS Spoofing

Spoofer performs short-term disruption of the GNSS signal L1 using GNSS jammer, which is now very widespread. For example, a device connected to the cigarette lighter (Fig. 3 – Mini Cigarette Lighter Anti-Tracker GNSS Jammer), which costs only $21.80 [3] is used on a board of TIR (Transports Internationaux Routiers) for locking devices of the vehicle's registration systems.

Fig. 2. Mini Cigarette Lighter Anti-Tracker GNSS Jammer (photo of DX)
Rys. 2. Mini zapalniczka Anty Tracker GNSS Jammer (zdjęcie DX)

A fishing vessel is able to block theself--registration system for routing and trotfishing in foreign waters.

As a result of jamming GNSS receiver „loses satellites" and starts looking for GNSS signals. At this time, spoofer includes imitator GNSS signals, which is 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.

GNSS Simulators

A GNSS simulator device is more complex compared to GNSS Jammer, it costs about € 1000 [3]. A GNSS simulator provides an effective and efficient means to test GNSS receivers and the systems that rely on them. A GNSS simulator provides control over the signals generated by the GNSS constellations and the global test environments all, in a box, so that testing can be conducted in controlled laboratory conditions. GNSS simulators generate the same kinds of signals that are transmitted by the GNSS satellites, thus GNSS receivers can process the simulated signals in exactly the same way as those from actual GNSS satellites.

Fig. 4. Multi-GNSS Spirent GSS8000 simulator (frequencies – GPS: L1, L2, L5; Galileo: E1, E5ab, E6; GLONASS: L1, L2; SBAS: L1, L5) (picture SPIRENT)
Rys. 4. Symulator Multi-GNSS Spirent GSS8000 (częstotliwości – GPS: L1, L2, L5; Galileo: E1, E5ab, E6; GLONASS: L1, L2; SBAS: L1, L5) (zdjęcie SPIRENT)

A GNSS simulator provides a superior alternative for testing, compared to using actual GNSS signals in a live environment. Unlike live testing, testing with simulators provides full control of the simulated satellite signals and the simulated environmental conditions. With a GNSS simulator, testers can easily generate and run many different test scenarios for different kinds of tests, with complete control over:

- Date, time, and location. Simulators generate GNSS constellation signals for any location and time. Scenarios for any locations around the world or in space, with different times in the past, present, or future, can all be tested without leaving the laboratory.
- Vehicle motion. Simulators model the motion of the vehicles containing GNSS receivers, such as aircraft, ships, or automobiles. Scenarios with vehicle dynamics, for different routes and trajectories anywhere in the world, can all be tested without actually moving the equipment being tested.
- Environmental conditions. Simulators model effects that impact GNSS receiver performance, such as atmospheric conditions, obscurations, multipath reflections, antenna characteristics, and interference signals. Various combinations and levels of these effects can all be tested in the same controlled laboratory environment.
- Signal errors and inaccuracies. Simulators provide control over the content and characteristics of the GNSS constellation signals. Tests can be run to determine how the equipment would perform, if various GNSS constellation signal errors occur.

GNSS Spoofing (2D training)

A GNSS Spoofing is performed in 4D $\{X,Y,Z,T\}$ space. To illustrate the principles of spoofing, we consider a virtual experiment in 2D $\{X,T\}$ space navigation. There are two transmitters S_1 and S_2, which move in unknown directions. Each of the transmitters S_1 and S_2 know the irposition x'_1, x'_2 in space. Between them is a receiver R, which also moves in an unknown direction and it does not know its position x''.

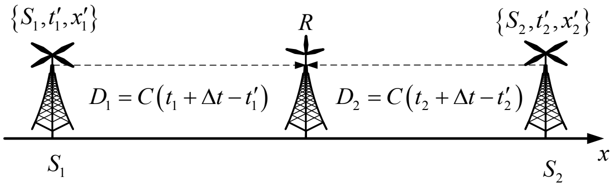
$\{S_1, t_1', x_1'\}$
R
$\{S_2, t_2', x_2'\}$
$D_1 = C(t_1 + \Delta t - t_1')$
$D_2 = C(t_2 + \Delta t - t_2')$
S_1
S_2
x

Fig. 5. Virtual navigation 2D experiment
Rys. 5. Wirtualny eksperyment nawigacyjny w 2D

On transmitters S_1 and S_2 are installed accurate clocks, such as atomic, and on the receiver R clock is in accurate, such as quartz. Transmitters S_1 and S_2 in time t_1', t_2' send messages, which contain three numbers: transmitter number (1 or 2), time of message (t_1' or t_2') and its coordinates in space (x_1' or x_2'). Receiver will receive a message at the time (t_1'' or t_2'') with error of Δt.

For the determination of accurate values of their coordinates x'' receiver can determine the approximate distance coordinates from transmitters by inaccurate determining the time distribution of radio signal from transmitter to receiver. Approximate distance from the transmitter S_1 to the receiver R is as follows:

$$x_1'' = x_1' + C\left(t_1'' + \Delta t - t_1'\right) \tag{3}$$

and the approximate distance from the transmitter S_2 to the receiver R is as follows:

$$x_2'' = x_2' - C\left(t_2'' + \Delta t - t_2'\right) \tag{4}$$

Distance error between the receiver and the transmitter is determined by the inaccuracy of a quartz clock receiver, which is equal to ΔD, leads to indeterminacy of the receiver position in space, that is receiver at the same time, "like" is in two points in space $x'' + \Delta D$ and $x'' - \Delta D$, and the distance between these points is equal to $2\Delta D$. An accurate determination of receiver position in space is determined as follows:

$$x'' = \frac{x_1'' + x_2''}{2} = \frac{x_1' + x_2' + C\left(\left(t_1'' - t_1'\right) - \left(t_2'' - t_2'\right)\right)}{2} \tag{5}$$

where: t_1', t_2' – messages return time S_1 and S_2 transmitters; x_1', x_2' – coordinates of the S_1 and S_2 transmitters; t_1'', t_2'' – exact time of a message is received by the receiver R from S_1 and S_2 transmitters; x_1'', x_2'' – approximate location of the receiver R, x'' – exact position of the receiver R.

It means that the accuracy of determining the position of the receiver does not depend on the inaccuracy of a quartz clock of its transmitter.

Let as represent our virtual experiment in space navigation, but in spoofing terms (Fig. 6). Spoofer at the same time interferes with GNSS signals by jammer and transmits to the receiver *R* amplified signals containing $\{S_1, t_1^S, x_1^S\}$ and $\{S_2, t_2^S, x_2^S\}$ information.

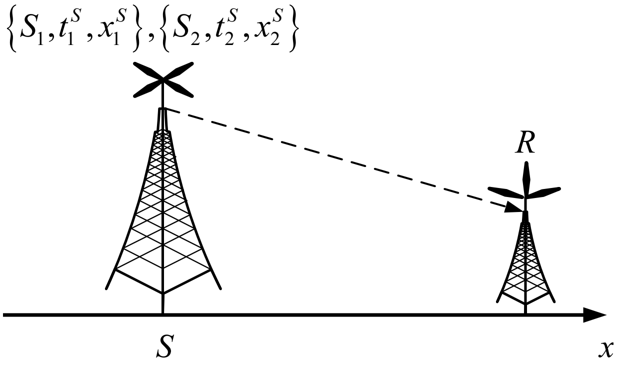

Fig. 6. Virtual 2D experiment in spoofing space navigation
Rys. 6. Wirtualny eksperyment nawigacyjny w przestrzeni 2D w warunkach spoofingu

The receiver begins to receive imitative GNSS signals from spoofer *S*: $\{S_1, t_1^S, x_1^S\}$, $\{S_2, t_2^S, x_2^S\}$ and determines its position in space as follows:

$$x'' = \frac{x_1^S + x_2^S + C\left(\left(t_1'' - t_1^S\right) - \left(t_2'' - t_2^S\right)\right)}{2} \tag{6}$$

since $t_1'' = t_2''$, that:

$$x'' = \frac{x_1^S + x_2^S + C\left(t_1^S - t_2^S\right)}{2} \tag{7}$$

in this case, the calculated position of the receiver in space does not depend from inaccuracy quartz clock and does not depend on the receipt time of signals from the spoofing antenna, i.e. that it also does not depend on the distance between antennas S_2 and *R*. In the particular case for $t_1^S = t_2^S$:

$$x'' = \frac{x_1^S + x_2^S}{2} \tag{8}$$

and for $x_1^S = 0$ obtain the final spoofing simplification:

$$x'' = \frac{x_2^S}{2} \tag{9}$$

This virtual experiment reflects the actual spoofing presented properties, thus allows a more thorough understanding of the anti-spoofing equipment, so-called ***anti-spoofer.***

Evidence of GNSS Spoofing

Many real experiments performed have shown, that disclosure of spoofing is possible for two reasons. Firstly, the analysis of the signals which receiver gets during jamming and tuning to receive imitator signals indicates, that in these moments of time signals cannot be considered as stationary random processes. Secondly, statistical characteristics of spoofer signals significantly differ from the statistical characteristics of signals, derived from the real satellite navigation. We point out the most common differences.

- **The high level of signal.** Spoofer signal level is always higher than the level of GNSS signals.
- **The levels of signals from different GNSS satellites vary greatly.** Spoofer could imitate signals from 36 satellites. However, if the real signals differ in power, spoofing signals generally have the same power.
- **Low levels of ratio noise**. Spoofer signals are characterized by low levels of noise ratio. Receipt by the GNSS receiver undistorted signals may indicate that signal is generated by spoofer.
- **Determining unique number satellites number**. Each satellite navigation system which conducts GNSS monitoring has its own number. Some satellite signals are received only on certain sections of the earth surface. Spoofers usually do not take into account whether the GNSS receiver begins to take a signal from a satellite with extraordinary number, which practically means signals are spoofer generated.

GNSS signals as a stationary random processes

GNSS signals changing in time may be considered as a random process, looking as a continuous random fluctuation around an average value, but neither average amplitude nor character of these fluctuations don't have abrupt changes with the course of time. Such random processes are named stationary. Each stationary process can be considered as lasting indefinitely long. When studying the stationary processes beginning of the countdown, we can select any point in time. In studying the stationary process in any section we should get the same characteristics.

In contrast to stationary random processes, non-stationary random processes are characterized by having some trends developing in time. Non-stationary random processes statistical characteristics depend on the start of counting, that is depend on the time.

It should be pointed, that not all non-stationary random processes are non-stationary at all the stages of their development. There are on-stationary random processes which at certain periods of time may be interpreted as a stationary random processes. ***Spoofing can be found as a non-stationary transition from GNSS stationary random processes to spoofer stationary random processes, which imitates the GNSS signals.***

Expected value, variance and correlation function of GNSS signals

The signals of the GNSS receiver $S_i(t)$ will be considered as stationary, if all its characteristics do not depend on t. With this approach to analysis the properties of GNNS signals, the receiver will use probabilistic characteristics as expected value, variance and correlation function of GNSS signals. We shall formulate the definition of the stationary random function in the notions of those characteristics.

Because the change in stationary random function must flow uniformly in time, it is a natural requirement, the expected value for stationary random function was constant:

$$M_i(t) = M_i = \text{const} \tag{10}$$

Note, however, that this requirement is not important when it is known that it is always possible to go from random function $S_i(t)$ to centered random function $\overset{\circ}{S}_i(t)$, for which the expected value equals zero, therefore, it corresponds to the condition (2). That is, if the random process is the process of non-stationary only because of variable expected value, it can be considered as a stationary process. The second condition is a stationary random function of dispersion stability condition:

$$D_{S_i}(t) = D_{S_i} = \text{const} \tag{11}$$

Let us establish, to which condition must stationary correlation function correspond to random function [4]. Consider the random function $S_i(t)$ (Fig. 7).

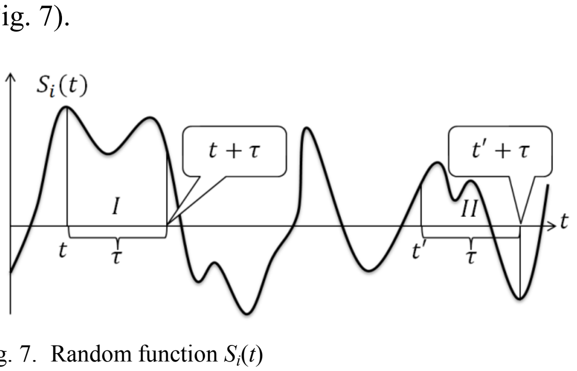

Fig. 7. Random function $S_i(t)$
Rys. 7. Funkcja losowa $S_i(t)$

Suppose $t' = t + \tau$ in the expression $K_{Si}(t, t')$, let us consider $K_{Si}(t, t + \tau)$ as the correlation moment function of two random sections, separated by time interval τ.

If the random process $S_i(t)$ is indeed stationary, then this correlation moment does not necessarily depend on which exact location of the coordinate from with t we take the time interval τ. It must only depend on the length of the period. For example, for time periods I and II (Fig. 7) the same τ length of correlation function values $K_{Si}(t, t + \tau)$ and $K_{Si}(t_1, t_1 + \tau)$ must be the same. In summary, correlation function of stationary random process does not depend on the location of t of the first argument on the axis of abscess, but only on the interval τ between the first and second argument:

$$K_{S_i}(t, t+\tau) = K_{S_i}(\tau) \tag{12}$$

So, correlation function for stationary random process is a function of not two, but only one argument. This greatly simplifies spoofing detection. We notice, that the condition (11), which requires dispersion stability from stationary random function, is a special case of the condition (12). So if we assume in (12) $\tau = 0$, we have:

$$D_{S_i}(t) = K_{S_i}(t, t) = K_{S_i}(0) = \text{const} \tag{13}$$

Thus, such a presentation (12) is sufficient for to spoofing detect. It should be noted that $S_i(t)$ is the random correlation function which depends not on two of its arguments t and t', but only on the difference τ between them. In order not to introduce additional conditions to the expected value, we consider that $S_i(t)$ was first centered, i.e.:

$$M_i(t) = M_i = 0 \tag{14}$$

Because the correlation function of any random function is symmetric, i.e. $K_{Si}(t, t') = K_{Si}(t', t)$, is a stationary process allowing $t' - t = \tau$, we have:

$$K_{S_i}(\tau) = K_{S_i}(-\tau) \tag{15}$$

i.e. correlation function $K_{Si}(\tau)$ is an even function of its argument. Therefore, we only specify the positive value of the argument for correlation function $K_{Si}(\tau)$. In practice, instead of correlation functions $K_{Si}(\tau)$, we will use the normalized correlation function:

$$P_{S_i}(\tau) = \frac{K_{S_i}(\tau)}{D_{S_i}} = \frac{K_{S_i}(\tau)}{K_{S_i}(0)} \tag{16}$$

Function $P_{Si}(\tau)$ is coefficient correlation between the cross sections of random functions, compartment separated τ according to time, it $P_{Si}(0) = 1$.

Moving Average, MA

Moving average shows average values of GNSS signals over a period of time. There are several types of moving averages: simple (i.e. arithmetic average), exponential, smooth and weighed. Special interest presents the moving average GNSS signal value assessments (under this article does not considered).

Different types of moving averages differently assign the weights in recent measurements GNSS signals. In case of SMA (Simple Moving Average), all GNSS signals have equal importance of the considered period. Moving averages, i.e. EMA (Exponential Moving Average) and LWMA (Linear Weighted Moving Average), create larger weights for the last GNSS signals.

The most common method of interpreting a moving average GNSS signal is composed of comparing its dynamics with the dynamics of the GNSS signal.

When the value of the GNSS signal is different from the moving average and has a value greater than some threshold value, it increases the probability that the object is subjected to spoofing attack.

The discussed analysis system using a moving average can respond according to the present trend (in real time), i.e. recording spoofing shortly, after the spoofing attack on the object.

SMA (Simple Moving Average) – presents estimates of the average $S_i(t)$ for $t = n\Delta t$ in time interval $L\Delta t$:

$$\overline{M}_i(n\Delta t)=\frac{1}{L}\sum_{l=0}^{L-1}S_i\big((n-l)\Delta t\big) \tag{17}$$

where: Δt – period of the discretization process $S_i(t)$.

SMA can be obtained from the following recursive form:

$$\overline{M}_i(n\Delta t)=\overline{M}_i\big((n-1)\Delta t\big)-\frac{S_i\big((n-L)\Delta t\big)}{L}+\frac{S_i(n\Delta t)}{L} \tag{18}$$

SMA can be used to centering process $S_i(t)$:

$$S_i'(n\Delta t)=S_i(n\Delta t)-\overline{M}_i(n\Delta t) \tag{19}$$

WMA (Weighted Moving Average). One of the drawbacks of simple moving average is that in calculating its value to assign values to all GNSS signals of equal importance when averaged over the independence of whether closer or further, they stand out from the current moment of time. Those disadvantages were eliminated in the WMA. Weighted moving average is a simple modification of the simple moving average with the importance chosen in such a way, that the last GNSS signals have the greatest importance in assessing the expected value:

$$\overline{M}_i(n\Delta t)=\frac{1}{\sum\limits_{l=0}^{L-1}W_l}\sum_{l=0}^{L-1}W_l S_i\big((n-l)\Delta t\big) \tag{20}$$

where: W_l – the importance value of GNSS signals $S_i(t)$.

For example **LWMA** (**Linear Weighted Moving Average**) is an evaluation of the average value $S_i(t)$ for $t = n\Delta t$ in the time interval $L\Delta t$ for $W_l = L - l$, i.e.:

$$\begin{aligned}\overline{M}_i(n\Delta t)&=\frac{1}{\sum\limits_{l=0}^{L-1}(L-l)}\sum_{l=0}^{L-1}(L-l)S_i\big((n-l)\Delta t\big)=\\&=\frac{2}{L(L+1)}\sum_{l=0}^{L-1}(L-l)S_i\big((n-l)\Delta t\big)\end{aligned} \tag{21}$$

SMM (Simple Moving Median)

Under conditions of elevated noise levels as a robust assessment of the moving, SMM average can be used:

$$\overline{M}_i(n\Delta t)=\operatorname*{SMM}_{l=0}^{L-1}S_i\big((n-l)\Delta t\big) \tag{22}$$

To find the SMM, we build a string of variations L of samples $S_i((n-l)\Delta t)$ and in the form $\overline{M}_i(n\Delta t)$ it takes the average element that string.

MNCF (Moving Normalized Correlation Function)

MCNF is a standardized assessment of the correlation function $P_{Si}(\tau)$ when the time $n\Delta t$ during the period $L\Delta t$:

$$\overline{P}_{S_i}(n\Delta t,\tau)=\frac{\sum\limits_{l=0}^{L-1}\big(S_i'((n-l)\Delta t)\cdot S_i'((n-l+K)\Delta t)\big)}{\sum\limits_{l=0}^{L-1}\big(S_i'((n-l)\Delta t)\big)^2} \tag{23}$$

where: $K = \tau / \Delta t$.

Initial training of anti-spoofer in the absence of attacks on GNSS navigation device

Teaching the initial anti-spoofer, when there is no attack on the GNSS device, is performed in the laboratory, when we know with certainty that there are no attacks on GNSS navigation device. The above-discussed several statistical parameters can be used to perform an analysis of beginning and end of spoofing. In a real anti-spoofers, all these parameters and many others that have not been discussed within the article are reflect. To illustrate the technology of designing anti-spoofer, we consider one of the most important parameters. Strictly, this is not a parameter but a function. Forquite along stretch of time (several days), we estimate the cumulative distribution function (16) for some period of time $\tau_{\min} \le \tau \le \tau_{\max}$ with discretization Δt:

$$F(x,\tau) = p\left(\overline{P}_{S_i}(n\Delta t,\tau) < x\right) \tag{24}$$

where: $p(\gamma < x)$ is the probability that random variable γ is less than the argument x. Function $F(x, \tau)$ is monotonically increasing on the whole axis x, but $F(-\infty, \tau) = 0$ and $F(+\infty, \tau) = 1$. Evaluation of the density function of random variable $\overline{P}_{S_i}(n\Delta t,\tau)$ is a function:

$$f(x,\tau) = F'(x,\tau) \tag{25}$$

In general, random variable $\overline{P}_{S_i}(n\Delta t,\tau)$ has a normal distribution:

$$f(x,\tau) = \frac{1}{\sqrt{2\pi\sigma(\tau)^2}} e^{-\frac{[x-\mu(\tau)]^2}{2\sigma(\tau)^2}} \tag{26}$$

where: $\mu(\tau)$ – the average value $\overline{P}_{S_i}(n\Delta t,\tau)$ and $\sigma(\tau)$ – dispersion $\overline{P}_{S_i}(n\Delta t,\tau)$, which depend on τ. While increasing τ increases delay a decision about a possible attack on GNSS navigation device, i.e. the selection of parameter τ should be minimized.

However, for $\tau = 0$ the correlation coefficient between cross sections of random function is $P_{Si}(\tau) = 1$. It means that spoofing detection by analyzing the properties of a normalized correlation function (16) loses its meaning. For simplicity, it can be accepted, that $\tau = L\Delta t$, i.e. sections random function $P_{Si}(\tau)$ are separate and fall outside directly one after the other without delay:

$$f(x,L\Delta t) = \frac{1}{\sqrt{2\pi\sigma(L\Delta t)^2}} e^{-\frac{[x-\mu(L\Delta t)]^2}{2\sigma(L\Delta t)^2}} \tag{27}$$

As a result, in the form (23) $K = \tau/\Delta t = L$ and expression (23) can be written as:

$$\overline{P}_{S_i}(n\Delta t, L\Delta t) = \frac{\sum_{l=0}^{L-1}\left(S_i'((n-l)\Delta t)\cdot S_i'((n-l+L)\Delta t)\right)}{\sum_{l=0}^{L-1}\left(S_i'((n-l)\Delta t)\right)^2} \tag{28}$$

Area of permissible values (28) in the absence of attacks on GNSS navigation device is defined by introducing the function threshold:

$$\overline{\sigma} = r\sigma(L\Delta t) \tag{29}$$

where: $r > 0$ – threshold value for deciding rules:

$$\begin{aligned} &\text{if} \quad \{\mu(L\Delta t) - r\sigma(L\Delta t)\} \le \overline{P}_{S_i}(n\Delta t, L\Delta t) \le \\ &\quad \le \{\mu(L\Delta t) + r\sigma(L\Delta t)\} \\ &\text{then}\,\mathrm{ATTACK}=0 \quad \text{else} \quad \mathrm{ATTACK}=1 \end{aligned} \tag{30}$$

Central moment of anti-spoofer learning is the choice of the parameter r. In an initial phase of learning you can choose $r = 3$ (Fig. 8) and start under attack on GNSS navigation device anti-spoofer learning process.

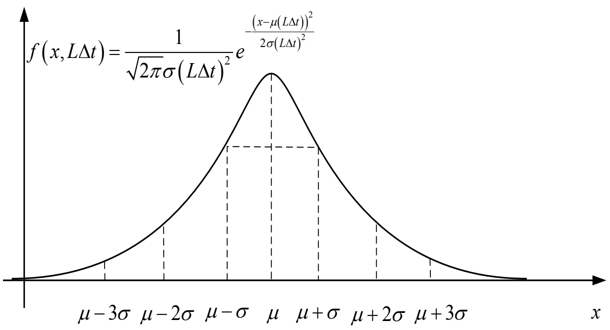

Fig. 8. The choice of the threshold value *r* for the decision rule (30)

Rys. 8. Wybór wartości progowej *r* dla reguły decyzyjnej (30)

Initial training of anti-spoofer in the conditions of the attacks on GNSS navigation device

Initial training of anti-spoofer in the conditions of the attacks on GNSS navigation device is performed in the laboratory. Spoofer work in a learning mode – the attack on GNSS navigation device, i.e. spoofer with a well-known periodicity generate false GNSS signals of satellites during a certain specified time. For quite a long stretch of time (several days), we estimate determined validation spoofing detection (28). Threshold correction r is possible only in the moment learning of attack, i.e. at $t = n\Delta t$, as follows:

$$\begin{aligned} &\text{if} \quad \{\mu(L\Delta t) - r\sigma(L\Delta t)\} \le \overline{P}_{S_i}(n\Delta t, L\Delta t) \le \\ &\quad \le \{\mu(L\Delta t) + r\sigma(L\Delta t)\} \\ &\text{then}\, r := r + \Delta r \quad \text{else} \quad r := r - \Delta r \end{aligned} \tag{31}$$

where: Δr – correction value threshold for a rule decisive (30–31).

Conclusions

The first part of the article describes a general approach to anti-spoofer design. Design results are markedly different and depending on the means of communication (ships, aircraft or surface transportation), the presence of the crew on board, means of communication (drone anti-spoofing is more complicated), the limit price and other parameters. This approach to design has been repeatedly tested and the performance was demonstrated in [5]. The second part shows the results of designing anti-spoofer to apply it to the fishing ships.

References

1. Markey H.K. at al.: Secret Communication System. US Patent 2,292,387 11.08.1942.
2. Badea V., Eriksson R.: Pseudolite INDOOR real time precise positioning, Norrkopping 2005.
3. Mini Cigarette Lighter Anti-Tracker GNSS Jammer, http://www.dealextreme.com/p/mini-cigarette-lighter-anti-tracker-gps-jammer-blocker-max-10m-coverage-35827
4. Ventcel' E.S.: Teoriâ veroâtnostej: Učeb. dlâ vuzov. 6-e izd. ster. M.: Vysš. šk., 1999.
5. Očin E.F.: Principy postroeniâ obučaûŝihsâ avtomatov dlâ obnaruženiâ poverhnostnyh defektov tel vraŝeniâ, Akademiâ nauk SSSR, Defektoskopiâ, 1985, 7, 83–87.

Others

6. Âcenkov V.S.: Osnovy sputnikovoj navigacii. Sistemy GPSNAVSTAR i GLONASS. M.: Gorâčaâ liniâ–Telekom, 2005.
7. Authenticating GNSS: Proofs against Spoofs, Part 1, http://www.insidegnss.com/auto/IGM%20Jul_Aug_07%20Working%20Papers.pdf
8. Authenticating GNSS: Proofs against Spoofs, Part 2, http://www.insidegnss.com/auto/SepOct07-wkngpapers-proof-spoof.pdf
9. GNSS Simulators http://www.spirent.com/positioning-and-navigation.aspx
10. GNSS vulnerability: present dangers and future threats, https://connect.innovateuk.org/web/6517437