DOI 10.15826/urej.2018.2.2.003 УДК 621.396.4

Атаки на глобальные навигационные спутниковые системы и обнаружение спуфинга беспилотных кораблей, базирующееся на облачных технологиях

Л. А. Добрякова[1], *Л. С. Лемишевский*[2], *Е. Ф. Очин*[3]
[1]Западно-Поморский технологический университет,
Щецин, Республика Польша

[2]Университет имени Якова Райского,
Щецин, Республика Польша

[3]Щецинский морской университет,
Щецин, Республика Польша
e.ochin@am.szczecin.pl

Аннотация. Спутниковые навигационные системы широко используются для точного определения траектории транспортных средств. В этой статье разработаны математические модели и алгоритмы для решения проблем безопасности спутниковой навигации. Одной из проблем является спуфинг (подстановка) — ситуация, когда система (аппаратное обеспечение, программное обеспечение и т. п.) успешно маскируется как другая, фальсифицируя систему данных, и выполняет незаконные действия. В статье рассматривается алгоритм обнаружения спуфинга на основе анализа гражданского спутникового сигнала, принимаемого мобильными одноантенными или двухантенными приемниками ГНСС. Эта работа также служит для уточнения оценки угроз среди гражданского населения путем демонстрации проблем, связанных с обнаружением спуфинга.

Широкое распространение ГНСС подталкивает текущую технологию приемника к ее пределам из-за строгих требований к обеспечению бесшовного, повсеместного, безопасного и надежного позиционирования. Этот факт еще более усугубляется появлением новых приложений: миниатюрный размер, низкое энергопотребление и ограниченные вычислительные возможности пользовательских терминалов создают серьезную проблему для реализации даже самых основных задач обработки сигналов ГНСС.

Эта работа иллюстрирует преимущество спутниковой навигации с использованием облачных технологий, которая облегчает возможность разработки инновационных приложений, таких как, например, массированная обработка данных, сотрудничество между пользователями, приложения, защищенные безопасностью и т. п.

Ключевые слова. ГНСС, облачная ГНСС, ГПС, антитерроризм, антиспуфинг, безопасность транспорта, спуфинг, алгоритм обнаружения спуфинга.

Global Navigation Satellite Systems Attacks and a Cloud-based Spoofing Detection for Unmanned Ships

Larisa A. Dobryakova[1], *Łukasz S. Lemieszewski*[2], *Evgeny F. Ochin*[3]
[1] West Pomeranian University of Technology,
Szczecin, Poland

[2] The Jacob of Paradies University,
Szczecin, Poland

[3] Maritime University of Szczecin, Szczecin, Poland
e.ochin@am.szczecin.pl

Abstract. Satellite navigation systems are widely used in navigation for precise trajectory determination of transport equipment. In this article mathematical models and algorithms have been developed to solve the problems of satellite navigation safety. One of the problems is spoofing (substitution) — a situation in which a system (hardware, software, etc.) successfully masquerades as another by falsifying data system and performs illegal actions. What is considered in the paper is the spoofing detection algorithm based on the analysis of a civil satellite signal generated by the mobile GNSS-single-antenna receivers or dual-antenna. The article also serves to refine the civilian spoofing threat assessment by demonstrating the challenges involved in mounting a spoofing attack.

The widespread deployment of GNSS is pushing the current receiver technology to its limits due to the stringent demands for providing seamless, ubiquitous and secure/reliable positioning. This fact is further aggravated by the advent of new applications where the miniaturized size, low power consumption and limited computational capabilities of user terminals pose serious concerns to the implementation of even the most basic GNSS signal processing tasks.

This article presents the advantage of Cloud-Based GNSS Navigation, which facilitates the possibility of developing innovative applications where their particularities (e. g. massive processing of data, cooperation among users, security-related applications, etc.) make them suitable for implementation using a cloud-based infrastructure.

Keywords. GNSS, Cloud-Based GNSS, GPS, antiterrorism, antispoofing, transport safety, spoofer, spoofing detection algorithm.

The basic notation and definitions

GNSS — Global Navigation Satellite System: Navstar GPS, GLONASS, BeiDou and GALILEO.

Sat_i, $i = \overline{1,N}, N \geq 4$ — the navigation satellites as the spacefaring component of GNSS. *{In ideal case, when the measurements are precise and satellite time is identical with the user's equipment time the users positioning can be realized with 3 satellites. Actually satellites time differs from the time on the*

users equipment. So, for users positioning one more coordinate is necessary — time drift between users equipment and the satellite time. That's why four satellites are needed for the solving of navigation problem.}

Spoofing — an attack on a GNSS, in an attempt to deceive the GNSS receiver by transmitting powerful false signals that mimic the signals from the true GNSS, exceeding the power of these true signals.

Spoofer — complex computer and radio equipment for the implementation of GNSS spoofing.

Rover — any mobile GNSS receiver that is used to collect data in the field at an unspecified location.

Pseudo-range — the distance to the satellite, resulting in the correlation of the received code and on-board code in the receiver without correction of clock synchronization errors.

(x, y, z) — the real coordinates of a vehicle (victim). If the vehicle is a 2D vehicle (ship, vessel, boat, car, *etc.*), the height coordinate (z) can be omitted and the minimum number of required navigation satellites can be reduced to three $\left(i = \overline{1, N}, N \geq 3\right)$

(x_v, y_v, z_v) — the precise coordinates of the vehicle.

$\left(\hat{x}_v, \hat{y}_v, \hat{z}_v\right)$ — the calculated coordinates of the vehicle using the GNSS.

(x_s, y_s, z_s) — the precise coordinates of the reception antenna of the spoofer.

$(\hat{x}_s, \hat{y}_s, \hat{z}_s)$ — the calculated coordinates of the reception antenna of the spoofer.

We also denote for $i = \overline{1, N}, N \geq 4$ (if the vehicle is a 2D vehicle (ship, vessel, boat, car, *etc.*), the height coordinate (z) can be omitted and the minimum number of navigation satellites can be reduced to three ($i = \overline{1, N}, N \geq 3$)):

(x_i, y_i, z_i) — the coordinates of Sat_i;

T_i^v — the propagation time from Sat_i to the vehicle in vacuum;

$\hat{T}_i^v$ – the propagation time from Sat_i to the vehicle in real atmosphere;

D_i^v — the measurement result of the distance from Sat_i to the vehicle (the vehicle pseudo-ranges).

D_s^v — the distance from spoofer to the victim.

Δt_s^v — the signal transit time from spoofer to the victim.

$\Delta\rho_i$ –the unknown error of the measurement result of the distance from Sat_i to the vehicle.

Introduction

Cloud technologies are data processing technologies in which computer resources are provided to the Internet user as an online service, for example, Xbox Live, Windows Live, OnLive, Google Docs, Office 365, Skype, SkyDrive, Dropbox, Google Drive and many others.

The idea of cloud technologies was first expressed by J. C. R. Licklider in 1970, when he was responsible for the development of ARPANET. The idea is that each person connected to the ARPANET receives not only data, but also programs. Later, this idea was called Cloud Computing (hereinafter CC).

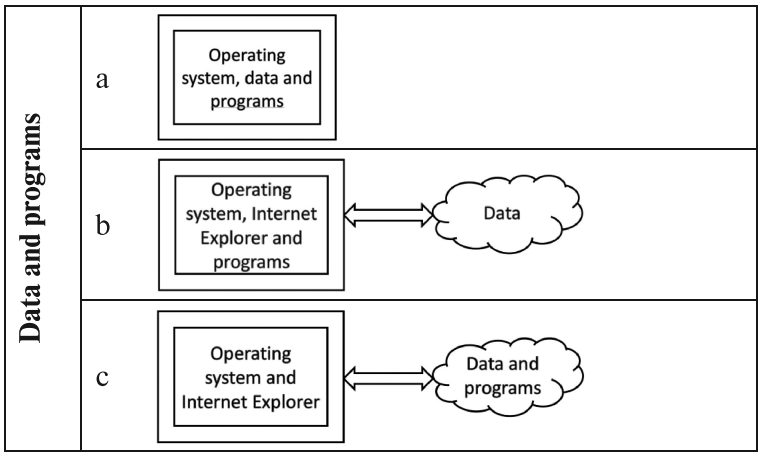

Figure 1. The main idea of cloud technologies:
a — the data and programs are on the user's workstation; b — the programs are on the user's workstation, and the data is on the network, the interface "User's workstation" ⇔ "Network" is implemented using Internet Explorer or the user's software; c — the data and programs are on the network, the interface "User Workstation" ⇔ "Network" is implemented using Internet Explorer

The wide distribution of CC begins in 2006, when Amazon introduced the WebServices infrastructure, which provides not only hosting, but also provision remote software and corresponding processing power to the client. Soon Google, Sun, IBM and Microsoft introduced similar services with its cloud-based operating system Windows Azure.

Here are just some Cloud Computing services:

Storage-as-a-Service represents cloud-based disk space as an additional logical drive or folder, for example, Google Drive. The service is the base for the remaining CC-Services.

Database-as-a-Service provides an opportunity to work with cloud databases.

Information-as-a-Service makes possible to use dynamic information cloud resources such as state and weather forecast, etc.

Application-as-a-Service or **Software-as-a-Service** provides the ability to use software deployed on cloud servers, with all software update and licensing issues regulated by the Application-as-a-Service vendor, such as for example Google Docs.

Security-as-a-Service provides secure use of web technologies, electronic correspondence, local area network.

Infrastructure-as-a-Service provides virtual platforms connected to the network that the user configures for their own tasks.

The main advantages of Cloud Computing:

- Since all computer operations are performed on servers on the network, the user can use hardware and software tools that are not available to him on his own workstation.
- You do not have to worry about the performance of your own workstation, not think about free disk space, you do not have to worry about backups and transferring information from one computer to another.
- The user does not need to monitor the release of software updates — he always has the latest version of the software.

The main disadvantages of Cloud Computing

- Confidentiality — the user agrees to the security of data on the side of the Internet Service Provider.
- Security — data security cannot be guaranteed.
- Constant and stable Internet — access to cloud services requires a permanent connection to the Internet.

The Clouds control, monitoring and managing is a security issue. Physical security is based on controlling physical access to servers and network infrastructure. Network security is the construction of a reliable threat model, including intrusion prevention and firewall. The use of a firewall implies the operation of a filter, in order to distinguish networks on subnets with different levels of trust. In the CC the most important role of the platform is performed by virtualization technology based on data encryption, data transmission security, authentication, user isolation and other technologies. In particular, work is underway to create secure data technology, in which the security mechanism is integrated.

GNSS navigation

Modern satellite navigation is based on the use of no-request range measurements between navigational satellite and the user. It means that the information about the satellite's coordinates given to the user, is included into navigation signal. The way of range measurements is based on the calculation of the receiving signal time delay compared with the signals, generated by the users equipment.

Satellite based positioning provides the world's most precise location information. It is possible to acquire positioning anywhere in the world that GNSS satellite signals are available, any time of a day, at data rates up to 100 Hz. Measurements are generated in real time or processed post-mission to achieve the highest level of accuracy.

GNSS technology is most frequently used to:

- determine the location of an object on or with respect to the Earth for navigation;
- locate an object with respect to another object for tracking purposes.

The positioning information typically provided includes a horizontal domain (latitude/longitude or easting/northing) and a vertical domain (height).

The distance from a vehicle (fig. 4) to satellites Sat_i can be written as:

$$D_i^v = \sqrt{(x_i - x_v)^2 + (y_i - y_v)^2 + (z_i - z_v)^2} = cT_i^v, i = \overline{1,N}, N \geq 4. \quad (1)$$

Since the measurement of the 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 the vehicle, then (1) are represented as (excluding time synchronization errors):

$$\sqrt{(x_i - x_v)^2 + (y_i - y_v)^2 + (z_i - z_v)^2} = c\left(\hat{T}_i^v - \Delta T_i^v\right), i = \overline{1,N}, N \geq 4. \quad (2)$$

As $\Delta\rho_i = c\Delta T_i^v$, then equation (2) can be written in the form

$$\sqrt{(x_i - x_v)^2 + (y_i - y_v)^2 + (z_i - z_v)^2} - \Delta\rho_i = c\hat{T}_i^v, i = \overline{1,N}, N \geq 4. \quad (3)$$

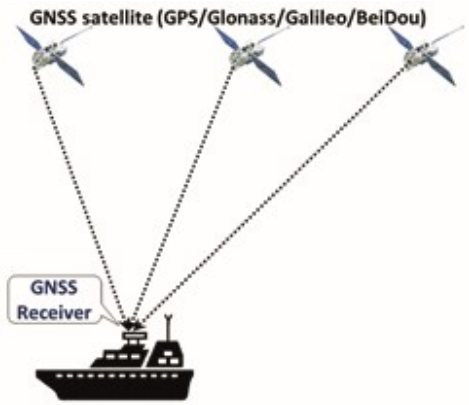

Fig. 2. GNSS Navigation

The navigation processor in the vehicle solves the system of the equations (3), calculates the position of the vehicle (x_v, y_v, z_v) and timing errors on board Δt, which are then used to correct the GNSS navigation clock (this article does not consider the timing errors, Δt).

$$\left\{\begin{array}{l} \sqrt{(x_1 - x_v)^2 + (y_1 - y_v)^2 + (z_1 - z_v)^2} - \Delta\rho_1 \\ \sqrt{(x_2 - x_v)^2 + (y_2 - y_v)^2 + (z_3 - z_v)^2} - \Delta\rho_2 \\ \sqrt{(x_3 - x_v)^2 + (y_3 - y_v)^2 + (z_3 - z_v)^2} - \Delta\rho_3 \end{array}\right\} \xrightarrow{\text{Iteration algorithm for } Sat_i,\ i=\overline{1,3}} (x_v, y_v, z_v). \quad (4)$$

Because $\Delta\rho_i$ is not an unknown value, instead of the exact value (x_v, y_v, z_v) we will get approximate results of measurements $(\hat{x}_v, \hat{y}_v, \hat{z}_v)$:

$$\left\{\begin{array}{l}\sqrt{(x_1-x_v)^2+(y_1-y_v)^2+(z_1-z_v)^2}\\ \sqrt{(x_2-x_v)^2+(y_2-y_v)^2+(z_3-z_v)^2}\\ \sqrt{(x_3-x_v)^2+(y_3-y_v)^2+(z_3-z_v)^2}\end{array}\right\} \xrightarrow[\text{for } Sat_i,\ i=\overline{1,3}]{\text{Iteration algorithm}} (\hat{x}_v, \hat{y}_v, \hat{z}_v). \quad (5)$$

Cloud-based GNSS Navigation

Currently four GNSSs, including the U. S. system Navstar GPS, the Russian Glonass, the European Galileo and the Chinese Beidou, in total will provide more than 40 visible GNSS satellites at a time, anywhere on the Earth. This is expected to solve many of the problems currently found when using GPS in urban environments, where hardly more than two satellites are visible at a time. The problem will be, though, the huge amount of data to be processed by the user receiver [1] in the face of increasing influence of interferences [2] and abnormal propagation effects [3].

All these processing tasks involve an unprecedented increase in the computational requirements of GNSS receivers, which is unfeasible with the current state of the art. User applications are gradually demanding low cost, small size and low power consumption devices, which dramatically hinder the implementation of complex processing tasks for positioning.

In this case, equation (5) takes the form

$$\left\{\begin{array}{l}\sqrt{(x_1-x_v)^2+(y_1-y_v)^2+(z_1-z_v)^2}\\ \sqrt{(x_2-x_v)^2+(y_2-y_v)^2+(z_3-z_v)^2}\\ \cdots\\ \sqrt{(x_N-x_v)^2+(y_N-y_v)^2+(z_N-z_v)^2}\end{array}\right\} \xrightarrow[\text{for } Sat_i,\ i=\overline{1,N}]{\text{Iteration algorithm}} (\hat{x}_v, \hat{y}_v, \hat{z}_v). \quad (6)$$

Analysis of computing resources shows that the iterative process (6) places significant demands on the performance of the user's workstation, and the widespread use of mobile computing resources (smartphones, gadgets, etc.) makes the solution of the system of equations (6) difficult to implement, significantly reduces the parameter N and abandons the maximum accuracy of determining the coordinates of XYZ. One way to radically solve this problem is to transfer the software for solving the system of equations (6) to the "cloud" (fig. 5).

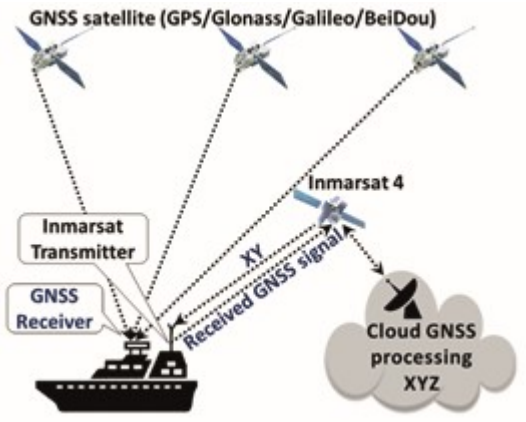

Fig. 3. Cloud-based GNSS Navigation (in general, the vehicle takes XYZ)

We note the main properties of Cloud-based GNSS navigation [4].

- Cloud-based GNSS navigation is always up-to-date — the user can be sure that all bug fixes and updates will be installed immediately after their birth.
- Access to settings at anytime, anywhere — even if the GNSS device is lost or it fails, it is easy to load settings to a new device.
- Security — Cloud-based GNSS navigation is protected by the service provider and trained personnel, so you can be sure that the data will not fall into the hands of the competitors.

Spoofing of Cloud-based GNSS Navigation

A spoofer transmits simulated signals of several satellites. If the level of the simulated signals exceeds the level of signals from real satellites, the GNSS receiver captures the false signal and calculates the false coordinates.

We will distinguish the following spoofing modes:

1. A spoofer is motionless and broadcasts signals of the visible part of GNSS satellite constellation, thus **a repeater of GNSS signals** is used as the spoofer.

2. A spoofer is motionless and broadcasts a signal's record of the visible part of GNSS satellite constellation, thus **GNSS recorder** is used as the spoofer.

3. A spoofer is motionless and broadcasts a signals of the visible part of GNSS satellite constellation with the introduction of signal delays from each of the GNSS satellites, thus **a repeater of GNSS signals with a programmer of signal delays** from each of GNSS satellites is used as a spoofer.

4. A spoofer is motionless and broadcasts a simulated GNSS signals, thuse **a simulator of GNSS-signals** is used as a spoofer.

5. A spoofer is mobile and broadcasts signals of the visible part of GNSS satellite constellation, thus **a repeater of GNSS signals** is used as the spoofer.

6. A spoofer is mobile and broadcasts a signal's record of the visible part of GNSS satellite constellation, thus **GNSS recorder** is used as the spoofer.

7. A spoofer is mobile and broadcasts signals of the visible part of GNSS satellite constellation with the introduction of delays signals from each of the satellites, thus a **repeater of GNSS signals with a programmer of signal delays** from each of GNSS satellites is used as a spoofer.

8. A spoofer is mobile and broadcasts a simulated GNSS signals, thus **a simulator of GNSS-signals** is used as a spoofer.

In this article, only the mode {1} are considered. In this mode a spoofer is motionless and broadcasts signals of the visible part of GNSS satellite constellation, thus **a repeater of GNSS signals** is used as the spoofer (fig. 6).

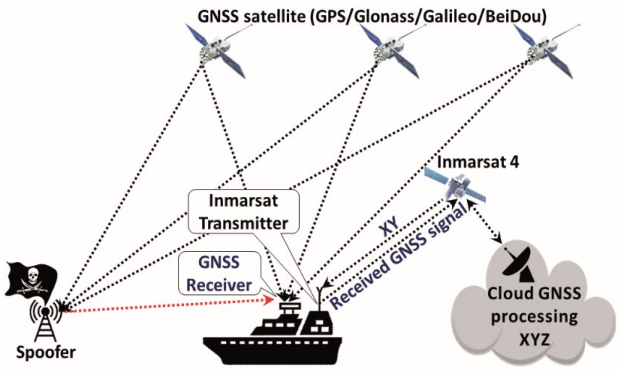

Fig. 4. Spoofing of Cloud-based GNSS Navigation

A victim receives the same signal as the spoofer, but with some delay Δt_s^v. It means that all receivers in the spoofing zone, calculate the same false coordinates, regardless of distance from spoofer to the victim:

$$\left\{\begin{array}{l}\sqrt{(x_1-x_v)^2+(y_1-y_v)^2+(z_1-z_v)^2}+D_s^v\\ \sqrt{(x_2-x_v)^2+(y_2-y_v)^2+(z_3-z_v)^2}+D_s^v\\ \ldots\\ \sqrt{(x_N-x_v)^2+(y_N-y_v)^2+(z_N-z_v)^2}+D_s^v\end{array}\right\}\xrightarrow[\text{for } Sat_i,\ i=\overline{1,N}]{\text{Iteration algorithm}}(\hat{x}_s,\hat{y}_s,\hat{z}_s),\quad(7)$$

where $D_s^v = c\Delta t_s^v$.

Detection of Spoofing

For the detection of GNSS spoofing, various methods are suggested. We list some of them.

- Detection based on the determination of the direction to the radiation source of the spoofer, comparing the phases of the signal to several antennas.

- Detection based on the definition of Doppler frequency shift.
- You can use the military GNSS signal as a reference (without the need to know the secret key).
- You can compare the indications of the inertial navigation system and the data from the GNSS receiver.

Dual-antenna Spoofing Detector

On the Spoofing Detector (SD) we install two antennas (fig. 7) and denote the distance between the antennas D_{1-2}.

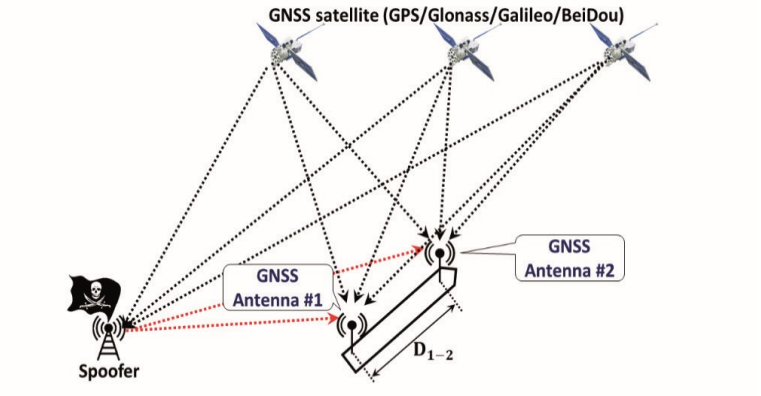

Fig. 5. Spofer and dual-antenna spoofing detector (DS), D_{1-2} — the distance between antennas of spoofing detector

Measuring the distance between antennas in normal navigation mode

The spoofing detector measures the coordinates of the antennas Y_1 and Y_2

$$\left\{\begin{array}{c}\sqrt{(x_1-x_{v1})^2+(y_1-y_{v1})^2+(z_1-z_{v1})^2}\\ \sqrt{(x_2-x_{v1})^2+(y_2-y_{v1})^2+(z_3-z_{v1})^2}\\ \ldots\\ \sqrt{(x_N-x_{v1})^2+(y_N-y_{v1})^2+(z_N-z_{v1})^2}\end{array}\right\} \xrightarrow{\text{Iteration algorithm for } Sat_i,\ i=\overline{1,N}} (\hat{x}_{v1},\hat{y}_{v1},\hat{z}_{v1}), \quad (8)$$

where (x_{v1},y_{v1},z_{v1}) — the unknown precise coordinates of the antenna Y_1, $(\hat{x}_{v1},\hat{y}_{v1},\hat{z}_{v1})$ — the calculated coordinates of the antenna Y_1.

$$\left\{\begin{array}{c}\sqrt{(x_1-x_{v2})^2+(y_1-y_{v2})^2+(z_1-z_{v2})^2}\\ \sqrt{(x_2-x_{v2})^2+(y_2-y_{v2})^2+(z_3-z_{v2})^2}\\ \cdots\\ \sqrt{(x_N-x_{v2})^2+(y_N-y_{v2})^2+(z_N-z_{v2})^2}\end{array}\right\}\xrightarrow{\text{Iteration algorithm for } Sat_i,\ i=\overline{1,N}}(\hat{x}_{v2},\hat{y}_{v2},\hat{z}_{v2}),\quad(9)$$

where (x_{v2},y_{v2},z_{v2}) — the unknown precise coordinates of the antenna Y_2, $(\hat{x}_{v2},\hat{y}_{v2},\hat{z}_{v2})$ — the calculated coordinates of the antenna Y_2.

The measurement results differ by some unknown values and, accordingly, the distance estimate $\hat{D}_{1-2}$ between the antennas will be comparable with the magnitude D_{1-2}:

$$\hat{D}_{1-2}=\sqrt{(\hat{x}_{v1}-\hat{x}_{v2})^2+(\hat{y}_{v1}-\hat{y}_{v2})^2+(\hat{z}_{v1}-\hat{z}_{v2})^2}\cong D_{1-2}.\quad(10)$$

Measurement of spacing between antennas in spoofing mode

A victim receives the same signal as the spoofer, but with some delay Δt_s^v. It means that all receivers in the spoofing zone calculate the same false coordinates, regardless of distance from spoofer to the victim:

$$\left\{\begin{array}{c}\sqrt{(x_1-x_{v1})^2+(y_1-y_{v1})^2+(z_1-z_{v1})^2}+D_s^{v1}\\ \sqrt{(x_2-x_{v1})^2+(y_2-y_{v1})^2+(z_3-z_{v1})^2}+D_s^{v1}\\ \cdots\\ \sqrt{(x_N-x_{v1})^2+(y_N-y_{v1})^2+(z_N-z_{v1})^2}+D_s^{v1}\end{array}\right\}\xrightarrow{\text{Iteration algorithm for } Sat_i,\ i=\overline{1,N}}(\hat{x}_{s'},\hat{y}_{s'},\hat{z}_{s'}),(11)$$

where $D_s^{v1}=c\Delta t_s^{v1}$ — the distance from spoofer to the antenna Y_1, $(\hat{x}_{s'},\hat{y}_{s'},\hat{z}_{s'})$ — the calculated coordinates of the spoofer using an antenna Y_1.

$$\left\{\begin{array}{c}\sqrt{(x_1-x_{v2})^2+(y_1-y_{v2})^2+(z_1-z_{v2})^2}+D_s^{v2}\\ \sqrt{(x_2-x_{v2})^2+(y_2-y_{v2})^2+(z_3-z_{v2})^2}+D_s^{v2}\\ \cdots\\ \sqrt{(x_N-x_{v2})^2+(y_N-y_{v2})^2+(z_N-z_{v2})^2}+D_s^{v2}\end{array}\right\}\xrightarrow{\text{Iteration algorithm for } Sat_i,\ i=\overline{1,N}}(\hat{x}_{s''},\hat{y}_{s''},\hat{z}_{s''}),(12)$$

where $D_s^{v2}=c\Delta t_s^{v2}$ — the distance from spoofer to the antenna Y_2, $(\hat{x}_{s''},\hat{y}_{s''},\hat{z}_{s''})$ — the calculated coordinates of the spoofer using an antenna Y_2.

In this case, the distance between the antennas Y_1 and Y_2 is defined as

$$\hat{D}_{1-2}=\sqrt{(\hat{x}_{s'}-\hat{x}_{s''})^2+(\hat{y}_{s'}-\hat{y}_{s''})^2+(\hat{z}_{s'}-\hat{z}_{s''})^2}\cong 0\,.\quad(13)$$

The final rule for detecting spoofing after comparison of (8) and (11) is

$$\boxed{if\ \widehat{D}_{1-2} \le \breve{D}\ then\ \langle Spoofing \rangle\ else\ GNSS} \tag{14}$$

where $\breve{D}$ — discriminant, determined on the basis of statistical studies at the stage of designing a real detection system.

The algorithm for spoofing detecting by estimating the dispersion of the pseudorange difference of two antennas

In the normal navigation mode, the pseudoranges of the antennas Y_1 and Y_2 differ from each other in some unknown, but significantly different values

$$\widehat{\rho_i} = (\hat{\rho}_{i'} - \hat{\rho}_{i''}). \tag{15}$$

Therefore, the root-mean-square deviation (RMSD) of the differences in the pseudoranges of the antennas Y_1 and Y_2 will be significantly different from zero:

$$\sigma_{gnss} = \sqrt{\frac{\sum_{i=1}^{N}(\hat{\rho}_i' - \hat{\rho}_{i''})^2 - \frac{1}{N}(\sum_{i=1}^{N}(\hat{\rho}_{i'} - \hat{\rho}_{i''}))^2}{N-1}} >> 0. \tag{16}$$

In the spoofing mode, the pseudoranges of the antennas Y_1 and Y_2 differ from each other by a certain constant value equal to $D_1 - D_2$. In this case RMSD differences of pseudoranges of antennas Y_1 and Y_2 is practically zero, that is

$$\sigma_s \cong 0. \tag{17}$$

The final rule for spoofing detection after comparison of (16) and (17) is

$$\boxed{if \sqrt{\frac{\sum_{i=1}^{N}(\hat{\rho}_i' - \hat{\rho}_{i''})^2 - \frac{1}{N}(\sum_{i=1}^{N}(\hat{\rho}_{i'} - \hat{\rho}_{i''}))^2}{N-1}} < \frac{\sigma_{gnss} - \sigma_s}{2}\ then\ \langle Spoofing \rangle\ else\ GNSS} \tag{18}$$

If we take $\sigma_{gnss} >> \sigma_s$, then the decisive spoofing detection rule is written as

$$\boxed{if \sqrt{\frac{\sum_{i=1}^{N}(\hat{\rho}_i' - \hat{\rho}_{i''})^2 - \frac{1}{N}(\sum_{i=1}^{N}(\hat{\rho}_{i'} - \hat{\rho}_{i''}))^2}{N-1}} < \frac{\sigma_{gnss}}{2}\ then\ \langle Spoofing \rangle\ else\ GNSS} \tag{19}$$

Discussion of the decisive rules

The spoofing detector can be designed on the basis of one of the decisive rules or on the basis of any combination of decision rules. In any case, it is necessary to calculate the probabilities of the "False alarm (false positives)"and "Missing target (false negatives)" events (table 1).

Table 1

Mistakes of a decision of the first kind (False alarm) and the second kind (Missing target)

The decisive rule or combination of decision rules		Valid mode	
		GNSS	SPOOFING
Solving of Spoofing Detector	GNSS	The solution is right	**Missing target**
	SPOOFING	**False alarm**	The solution is right

The issues of optimal design and selection of boundary conditions with the aim of minimizing the probabilities of "false alarm" and "missing target" are beyond the scope of this article. The application of Bayes' theorem (or Bayesian formula) is considered as one of the widely used techniques.

Single-antenna spoofing detector

Suppose that the vehicle is moving in an arbitrary direction. The single-antenna Y is installed on the spoofing detector (fig. 8). Denote the position of the antenna at the time t as Y', the position of the antenna at the time $t'' = t' + \Delta t$ as Y'' and the distance between the two antenna positions as D_{1-2}.

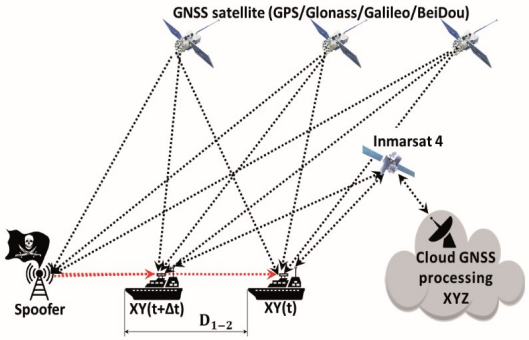

Fig. 6. Spoofer and single-antenna spoofing detector, D_{1-2} — the distance between two positions of single-antenna

Measuring the distance between two positions of single-antenna in normal navigation mode

The spoofing detector measures the coordinates of the antenna Y in two positions:

$$\left\{\begin{array}{l}\sqrt{(x_1-x_{v'})^2+(y_1-y_{v'})^2+(z_1-z_{v'})^2}\\ \sqrt{(x_2-x_{v'})^2+(y_2-y_{v'})^2+(z_3-z_{v'})^2}\\ \sqrt{(x_3-x_{v'})^2+(y_3-y_{v'})^2+(z_3-z_{v'})^2}\end{array}\right\} \xrightarrow{\text{Iteration algorithm for } Sat_i,\ i=\overline{1,3}} (\hat{x}_{v'}, \hat{y}_{v'}, \hat{z}_{v'}), \quad (20)$$

where $(x_{v'}, y_{v'}, z_{v'})$ — the unknown precise coordinates of the antenna Y at the time t, $(\hat{x}_{v'}, \hat{y}_{v'}, \hat{z}_{v'})$ — the calculated coordinates of the antenna Y at the time t.

$$\left\{\begin{array}{l}\sqrt{(x_1 - x_{v''})^2 + (y_1 - y_{v''})^2 + (z_1 - z_{v''})^2} \\ \sqrt{(x_2 - x_{v''})^2 + (y_2 - y_{v''})^2 + (z_3 - z_{v''})^2} \\ \sqrt{(x_3 - x_{v''})^2 + (y_3 - y_{v''})^2 + (z_3 - z_{v''})^2}\end{array}\right\} \xrightarrow{\text{Iteration algorithm for } Sat_i,\ i=\overline{1,3}} (\hat{x}_{v''}, \hat{y}_{v''}, \hat{z}_{v''}), \quad (21)$$

where $(x_{v''}, y_{v''}, z_{v''})$ — the unknown precise coordinates of the antenna Y at the time $t'' = t' + \Delta t$, $(\hat{x}_{v''}, \hat{y}_{v''}, \hat{z}_{v''})$ — the calculated coordinates of the antenna Y at the time $t'' = t' + \Delta t$.

The distance between the antenna Y at the time t' and the antenna Y at the time $t'' = t' + \Delta t$ is comparable with the magnitude D_{1-2}:

$$\hat{D}_{1-2} = \sqrt{(\hat{x}_{v'} - \hat{x}_{v''})^2 + (\hat{y}_{v'} - \hat{y}_{v''})^2 + (\hat{z}_{v'} - \hat{z}_{v''})^2} \cong D_{1-2}. \quad (22)$$

Measurement of spacing between two positions of single-antenna in spoofing mode

A victim receives the same signal as the spoofer, but with some delay $\Delta t_s^{v'}$. It means that all receivers in the spoofing zone, calculate the same false coordinates, regardless of distance from spoofer to the victim:

$$\left\{\begin{array}{l}\sqrt{(x_1 - x_{v'})^2 + (y_1 - y_{v'})^2 + (z_1 - z_{v'})^2} + D_s^{v'} \\ \sqrt{(x_2 - x_{v'})^2 + (y_2 - y_{v'})^2 + (z_3 - z_{v'})^2} + D_s^{v'} \\ \sqrt{(x_3 - x_{v'})^2 + (y_3 - y_{v'})^2 + (z_3 - z_{v'})^2} + D_s^{v'}\end{array}\right\} \xrightarrow{\text{Iteration algorithm for } Sat_i,\ i=\overline{1,3}} (\hat{x}_{s'}, \hat{y}_{s'}, \hat{z}_{s'}), \quad (23)$$

where $D_s^{v'} = c\Delta t_s^{v'}$ — the distance from spoofer to the antenna Y at the time t, $(\hat{x}_{s'}, \hat{y}_{s'}, \hat{z}_{s'})$ — the calculated coordinates of the spoofer using the antenna Y at the time t.

$$\left\{\begin{array}{l}\sqrt{(x_1 - x_{v''})^2 + (y_1 - y_{v''})^2 + (z_1 - z_{v''})^2} + D_s^{v''} \\ \sqrt{(x_2 - x_{v''})^2 + (y_2 - y_{v''})^2 + (z_3 - z_{v''})^2} + D_s^{v''} \\ \sqrt{(x_3 - x_{v''})^2 + (y_3 - y_{v''})^2 + (z_3 - z_{v''})^2} + D_s^{v''}\end{array}\right\} \xrightarrow{\text{Iteration algorithm for } Sat_i,\ i=\overline{1,3}} (\hat{x}_{s''}, \hat{y}_{s''}, \hat{z}_{s''}), \quad (24)$$

where $D_s^{y''} = c\Delta t_s^{y''}$ — the distance from spoofer to the antenna Y at the time $t'' = t' + \Delta t$; $(\hat{x}_{s''}, \hat{y}_{s''}, \hat{z}_{s''})$ — the calculated coordinates of the spoofer using the antenna Y at the time $t'' = t' + \Delta t$.

In this case, the distance between the antenna Y at the time t' and the antenna Y at the time $t'' = t' + \Delta t$ is defined as

$$\hat{D}_{1-2} = \sqrt{(\hat{x}_{s'} - \hat{x}_{s''})^2 + (\hat{y}_{s'} - \hat{y}_{s''})^2 + (\hat{z}_{s'} - \hat{z}_{s''})^2} \cong 0. \quad (25)$$

The decisive rule 1

The final rule for detecting spoofing after comparison of (20) and (23) is

$$\boxed{if\ \hat{D}_{1-2} \le \breve{D}\ then\ \langle Spoofing \rangle\ else\ GNSS}, \quad (26)$$

where $\breve{D}$ — discriminant, determined on the basis of statistical studies at the stage of designing a real detection system.

Summary and conclusions

This paper has introduced the use of Cloud-Based GNSS Navigation for developing the novel concept of antispoofing. We have presented the main features of one of the major antispoofing Cloud-Based GNSS Navigation, describing the services. Next, we have discussed the general architecture of the antispoofing Cloud-Based GNSS Navigation where GNSS raw samples can simultaneously be processed with nearly unlimited computing resources. This is of special interest for applications with computationally demanding techniques, such as indoor positioning and multi-constellation processing. It is also a very flexible scheme, since new functionalities and compatibility with future signal evolutions can easily be incorporated by updating the Cloud-Based GNSS Navigation software, regardless of the user terminals.

The risk of losing GNSS signal is growing every day. The accessories necessary for the manufacture of systems for GNSS spoofing are now widely available and this type of attack may be taken as advantage of not only by the military, but also by 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.

It is important to emphasize that GNSS is not only navigation. In the framework of the current threat model, GNSS interference is needed in order to drown out the reference signal of synchronous time that is used in a distributed network of radio electronic devices. That is, GNSS allows synchronizing with high accuracy time on stand-alone passive devices.

References

1. Dobryakova L., Lemeszewski Ł., Ochin E. Design and Analysis of Spoofing Detection Algorithms for GNSS Signals. *Scientific Journals of the Maritime University of Szczecin*, 2014, no. 40 (112), p. 47–52.

2. Dobryakova L., Lemeszewski Ł., Ochin E. Transport safety: the GNSS spoofing detecting using two navigators [Bezpieczeństwo w transporcie: wykrycie ataku GNSS spoofing za pomocą dwóch nawigatorów]. *Logistyka*, 2014, nr 3/2014, pp. 1328–1331.

3. Dobryakova L., Lemeszewski Ł., Ochin E. The vulnerability of unmanned vehicles to terrorist attacks such as GNSS-spoofing. *Scientific Journals of the Maritime University of Szczecin*, 2016, no. 46 (118), pp. 181–188.

4. Dobryakova L., Lemeszewski Ł., Ochin E. Protecting vehicles vulnerable to terrorist attacks, such as GNSS jamming, by electromagnetic interference shielding of antenna. *Scientific Journals of the Maritime University of Szczecin*, 2017, no. 50 (122), pp. 77–83.

5. GPS World (2015) Spoofing, Detection, and Navigation Vulnerability. Available at: https://www.youtube.com/watch?v=qlX–MsYZvoM (accessed 13.04.2018).

6. Humphreys T. E., Ledvina B. M., Psiaki M. L., O'Hanlon B. W., Kintner Jr. P. M. Assessing the Spoofng Threat: Development of a Portable GPS Civilian Spoofer. *Preprint of the 2008 ION GNSS Conference Savanna*. GA, 2008, September 16–19.

7. Jafarnia-Jahromi A., Broumandan A., Nielsen J., Lachapelle G. GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. *Hindawi Publishing Corporation International Journal of Navigation and Observation,* 2012, Article ID127072. doi: 10.1155/2012/127072

8. Januszewski J. *Systemy satelitarne GPS, Galileo i inne*. PWN. 2010.

9. Jones M. The civilian battlefield. Protecting GNSS receivers from interference and jamming. *Inside GNSS*, 2011, vol. Mar./Apr., pp. 40–49.

10. Lucas-Sabola V., Seco-Granados G., López-Salcedo J. A., García-Molina J. A., Crisci M. Cloud GNSS receivers: New advanced applications made possible. *International Conference on Localization and GNSS (ICL-GNSS)*. Barcelona, 2016, pp. 1–6.

11. 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*, 2013, 36 (108) z. 2, pp. 159–165.

12. Psiaki M. L., O'Hanlon B. W., Bhatti J. A., Shepard D. P., Humphreys T. E. Civilian GPS Spoofing Detection based on Dual-Receiver Correlation of Military Signals. *Proceedings of ION GNSS*. Portland, Oregon, 2011.

13. Raia M. The Benefits of Choosing a Cloud-Based GPS Tracking System. *CloudExpo Journal*, 2011, August 18. Available at: http://cloudcomputing.sys-con.com/node/1950571 (accessed 13.04.2018)

14. Seco-Granados G., López-Salcedo J. A., Jimenez-Banos D., López-Risueno G. Challenges in Indoor Global Navigation Satellite Systems. *IEEE Signal Proc. Mag.*, 2012, vol. 29, no. 2, pp. 108–131.

15. Specht C. System GPS. *Biblioteka Nawigacji*, 2007, nr 1. Wydawnictwo Bernardinum. Pelplin.

Information about the author

Larisa A. Dobryakova received the M. S. degrees in Baltic State Technical University "Voenmeh" D. F. Ustinov in Russia in 1998 and the Ph. D. degree at West Pomeranian University of Technology in Poland, scientific discipline CS&IT in 2007.

From 2007 she is an associate professor at West Pomeranian University of Technology in Poland, Faculty of CS&IT, Department of Methods of Artificial Intelligence and Applied Mathematics.

Larisa A. Dobryakova is the co-author of 3 books and more than 40 articles. Her research interests focus on the problems of antiterrorism, including GNSS anti-spoofing.

Łukasz S. Lemieszewski received the M. S. degrees in computer and telecommunications networks from West Pomeranian University of Technology Szczecin in 2002, and the Ph. D. degree in Maritime University of Szczecin, scientific discipline transport in 2016.

From 2016 he is an assistant professor at The Jacob of Paradies University, Department of Technology, in Gorzów Wielkopolski, Poland.

Łukasz S. Lemieszewski is the co-author of 2 books and more than 20 articles. His research interests focus on spoofing and jamming detection methods using different types of receivers, and microelectromechanical system equipment. The scope of his interests comprises also network communication protocols and the security of their transmissions.

Evgeny F. Ochin received the M. S. degree in 1969, the Ph. D. degree in 1974 and the Ph. D.-hubil. degree in 1997 in ITMO University (Saint Petersburg National Research University of Information Technologies, Mechanics and Optics, Russia).

From 1974 to 2004, he was an assisted professor and professor in the department of computer technology and vice-rector on scientific work in ITMO University. From 1996 to 2001, he was vice-rector on informatization of Baltic State Technical University "Voenmeh" D. F. Ustinov. From 2002 to 2008, he was director of the Institute "Architecture of Computers and Telecommunications" and head of the department "Computer networks" of Szczecin Technological University, Poland. From 2008 to 2018 he is a professor of Maritime University of Szczecin (Poland), Navigation Faculty, Department of Marine Information Technology.

Evgeny F. Ochin is the author of 4 books, more than 160 articles, and more than 20 inventions. His research interests include CS&IT, safety of satellite navigation on land, sea and air, including anti-jamming and GNSS anti-spoofing, based on inertial navigation system.

Поступила / Receiver: 11.06.2018
Принята в печать / Accepted: 17.07.2018