Scientific Journals
of the Maritime University of Szczecin

Zeszyty Naukowe
Akademii Morskiej w Szczecinie

2019, 57 (129), 29–37
ISSN 1733-8670 (Printed)
ISSN 2392-0378 (Online)
DOI: 10.17402/323

Received: 21.01.2019
Accepted: 14.02.2019
Published: 22.03.2019

Cloud-based GNSS navigation spoofing detection

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

[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] The Jacob of Paradies University, Department of Technology
25 Teatralna St., 66-400 Gorzów Wielkopolski, Poland, e-mail: llemieszewski@ajp.edu.pl
[3] 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: Cloud-based GNSS, GNSS, antiterrorism, antispoofing, transport safety, spoofer, spoofing detection algorithm

Abstract
Satellite navigation systems are commonly used to precisely determine the trajectory of transportation equipment. The widespread deployment of GNSS is pushing the current receiver technology to its limits due to the stringent demands for seamless, ubiquitous and secure/reliable positioning information. 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 risks to the implementation of even the most basic GNSS signal processing tasks. This paper has presented 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 Cloud-based infrastructure.

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 was that each person connected to ARPANET could receive not only data, but also programs. Later, this idea was called Cloud Computing (CC).

The problem of continuous position availability is one of the most important issues connected with human activity at sea. As the availability of satellite navigational systems can be limited in some cases, e.g. during military operations, additional methods of acquiring information about a ship's position must be considered.

Increasing the accuracy of positioning has acquired a particular urgency in the process of designing ships' autopilots for autonomous navigation of marine transport systems.

Analysis of computing resources has shown that the iterative GNSS process places significant demands on the performance of the user's workstation, and the widespread use of mobile computing resources (smartphones, gadgets, etc.) has made the solution of GNSS difficult to implement. One way to radically solve this problem is to transfer the GNSS software to the "cloud".

Notation and definitions

GNSS – Global Navigation Satellite System {Navstar GPS: www.navcen.uscg.gov, GLONASS:

www.glonass-iac.ru, GALILEO:www.gsc-europa.eu, BeiDou: en.beidou.gov.cn}.
ISP – Internet Service Provider.
Sat$_i$, $i=\overline{1,N}$, $N\geq 4$ – the navigation satellites as the spacefaring component of GNSS.
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 – 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).
(x_v, y_v, z_v) – the precise coordinates of the vehicle.
$(\hat{x}_v, \hat{y}_v, \hat{z}_v)$ – 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.
(x_i, y_i, z_i) – the coordinates of Sat$_i$.
T_i^v – the propagation time from Sat$_i$ to the vehicle in a vacuum.
$\hat{T}_i^v$ – the propagation time from Sat$_i$ to the vehicle in the real atmosphere.
D_i^v – the measurement result of the distance from Sat$_i$ to the vehicle (the vehicle's pseudo-ranges).
D_s^v – the distance from the spoofer to the victim.
Δt_s^v – the transit time from the spoofer to the victim.
$\Delta\rho_i$ – unknown error of the measurement result of the distance from Sat$_i$ to the vehicle.

Examples of CC 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 it possible to use dynamic information cloud resources such as state and weather forecasts, 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, and local area networks.

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

The main advantages and disadvantages of CC

Advantages:
- 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;
- the user does not have to worry about the performance of his own workstation, think about free disk space, or 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.

Disadvantages:
- confidentiality – the user agrees to the security of data on the side of the ISP;
- security – data security cannot be guaranteed;
- constant and stable Internet – access to cloud services requires a permanent connection to the Internet.

The security of CC

The control, monitoring and managing of the Cloud is a security issue. Physical security is based on controlling physical access to the servers and network infrastructure. Network security consists of the construction of a reliable threat model, including intrusion prevention and a 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 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 positioning

The distance from a vehicle (Figure 1) to satellites Sat$_i$, which was presented in the literature

(Specht, 2007; Januszewski, 2010; Zalewski, 2014) can be also written as:

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

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 equation (1) can be represented as (excluding time synchronization errors):

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

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

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

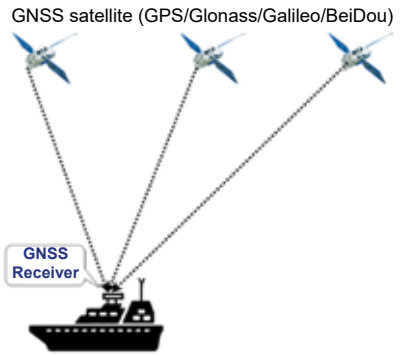

Figure 1. GNSS positioning

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 the timing errors on board, Δt, which are then used to correct the GNSS navigation clock (this article has not considered the timing errors, Δt).

$$\left\{\begin{array}{l} \sqrt{(x_1 - x_v)^2 + (y_1 - y_v)^2 + (z_1 - z_v)^2} + \Delta\rho_1 \\ \sqrt{(x_2 - x_v)^2 + (y_2 - y_v)^2 + (z_2 - z_v)^2} + \Delta\rho_2 \\ \cdots \\ \sqrt{(x_N - x_v)^2 + (y_N - y_v)^2 + (z_N - z_v)^2} + \Delta\rho_N \end{array}\right\} \rightarrow$$
$$\xrightarrow[\text{for } Sat_i,\ i=\overline{1,N}]{\text{Iteration algorithm}} (x_v, y_v, z_v) \tag{4}$$

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

$$\left\{\begin{array}{l} \sqrt{(x_1 - x_v)^2 + (y_1 - y_v)^2 + (z_1 - z_v)^2} \\ \sqrt{(x_2 - x_v)^2 + (y_2 - y_v)^2 + (z_2 - z_v)^2} \\ \cdots \\ \sqrt{(x_N - x_v)^2 + (y_N - y_v)^2 + (z_N - z_v)^2} \end{array}\right\} \rightarrow$$
$$\xrightarrow[\text{for } Sat_i,\ i=\overline{1,N}]{\text{Iteration algorithm}} (\hat{x}_v, \hat{y}_v, \hat{z}_v) \tag{5}$$

Cloud-based GNSS positioning

Currently four GNSS, including the U.S. system Navstar GPS, the Russian Glonass, the European Galileo and the Chinese Beidou, in total provide more than 40 visible GNSS satellites at a time, anywhere on Earth. This is expected to solve many of the problems currently found when using GPS in urban environments, where rarely more than two satellites are visible at a time. The problem, though, will be the huge amount of data that will need to be processed by the user's receiver (Lucas-Sabola et al., 2016) in the face of the increasing influence of interference (Jones, 2011) and abnormal propagation effects (Seco-Granados et al., 2012).

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 devices. 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.

Cloud technology provides the ability to access data without installing special applications on a device (Figure 2).

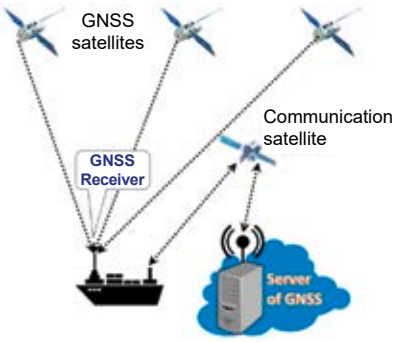

Figure 2. Cloud-based GNSS positioning

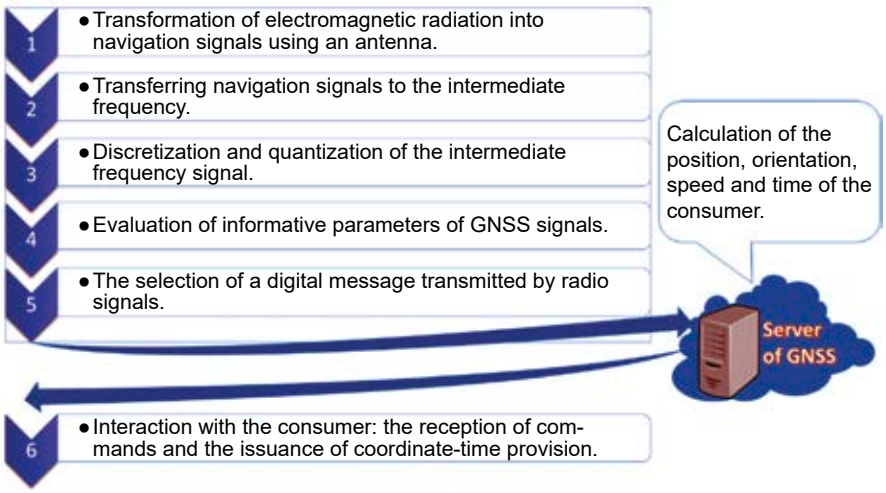

Figure 3. The separation of data processing functions between the consumer and the "cloud"

With GNSS cloud computing, users can significantly reduce the cost of building hardware and software solutions to ensure the continuity and availability of GNSS – as these costs are absorbed by the cloud service provider. The number of GNSS satellites is constantly increasing, new information channels appear, and processing algorithms are constantly being improved. This limits the ability of consumers to respond in a flexible manner to market requirements, while cloud technologies provide the ability to upgrade the software in a timely manner and increase the performance of virtual computing resources.

GNSS technologies are constantly improving: the number of satellites and the number of available signals are increasing, new systems are being put into operation, and existing ones are being expanded and modernized.

GNSS signals are detected by consistent filtering under conditions of unknown Doppler frequency shifts. The signal-to-noise ratio at the output of the matched filter determines the potential accuracy of the estimates of the parameters of the received signal.

Receiving and processing GNSS signals consists of several stages. Figure 3 shows the separation of the data processing functions between the consumer and the "cloud".

Note the main properties of Cloud-based GNSS navigation (Raia, 2011):

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

Cloud-based GNSS spoofing detection

Spoofers can be divided into two classes: one-antenna spoofers and multi-antenna spoofers. Only one-antenna spoofers have been considered in this paper, since the solution to the problem "Spoofing detection" is in the stage of scientific research.

A spoofer transmits simulated signals of several satellites in the manner that was used in the literature (Humphreys et al., 2008) in the development of a portable GPS civilian spoofer. If the level of the simulated signals exceeds the level of the signals from the real satellites, the GNSS receiver captures the false signal and calculates false coordinates.

Four different Cloud-based GNSS spoofing detection modes have been investigated in this paper:

A. A spoofer is motionless and broadcasts signals of the visible part of the GNSS satellite constellation, thus **a repeater of the GNSS signals** is used as the spoofer (Figure 4).
B. A spoofer is motionless and broadcasts signals of the visible part of the GNSS satellite constellation with the introduction of signal delays from each of the GNSS satellites, thus a repeater of the GNSS signals with the programmed signal delays from each of the GNSS satellites is used as a spoofer (Figure 4).
C. A spoofer is motionless and broadcasts a signal's record of the visible part of the GNSS satellite constellation (Figure 5), thus the GNSS recorder is used as the spoofer (Figure 6).

D. A spoofer is motionless and broadcasts simulated GNSS signals, thus a simulator of the GNSS-signals is used as a spoofer (Figure 6).

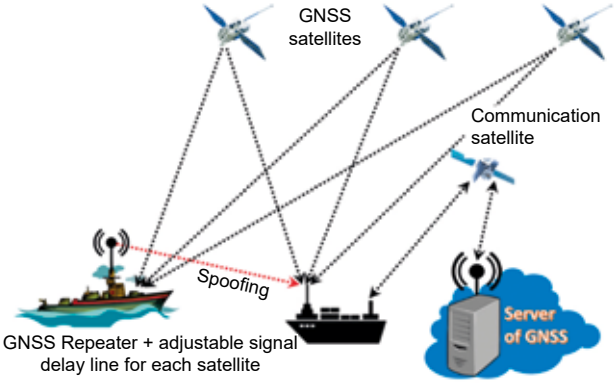

Figure 4. Spoofer broadcasts signals of the visible part of the GNSS satellite constellation without the possibility of signals delays programmed for each satellite (A) or with the possibility of signals delays programmed for each satellite (B)

Figure 5. Spoofer records signals of the visible part of the GNSS satellite constellation

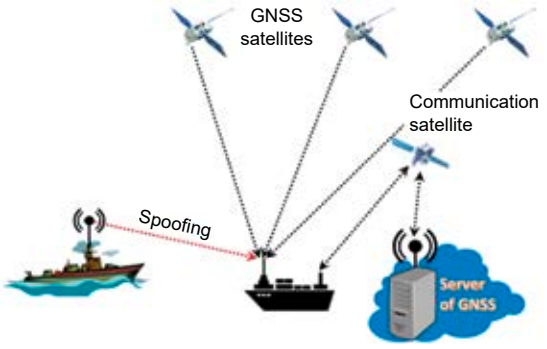

Figure 6. Spoofer broadcasts signals of the visible part of the GNSS satellite constellation (C) or broadcasts simulated GNSS signals (D)

In this article, only the modes A and B have been considered. Further information about the spoofing models can be found in the literature (Dobryakova, Lemieszewski & Ochin, 2016).

The spoofer is motionless and broadcasts signals of the visible part of the GNSS satellite constellation

In this mode the spoofer is motionless and broadcasts signals of the visible part of the GNSS satellite constellation, thus **a repeater of the GNSS signals** is used as the spoofer (Figures 4 and 5). A victim will receive the same signal as the spoofer, as can also be found in the literature (Ochin et al., 2013), but with the possibility of programmed delays for the signals for each satellite Δt_s^v (Figure 5). This means that all the receivers in the spoofing zone will calculate the same false coordinates, regardless of the distance from the spoofer to the victim:

$$\left\{\begin{array}{l}\sqrt{(x_1-x_v)^2+(y_1-y_v)^2+(z_1-z_v)^2}+D_s^v\\ \sqrt{(x_2-x_v)^2+(y_2-y_v)^2+(z_2-z_v)^2}+D_s^v\\ \cdots\\ \sqrt{(x_N-x_v)^2+(y_N-y_v)^2+(z_N-z_v)^2}+D_s^v\end{array}\right\}\rightarrow \xrightarrow[\text{for Sat}_i,\ i=\overline{1,N}]{\text{Iteration algorithm}} (\hat{x}_s,\hat{y}_s,\hat{z}_s) \quad (6)$$

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

Spoofing Detection

For the detection of GNSS spoofing, various methods have been suggested (Jafarnia-Jahromi et al., 2012):

- Detection based on the determination of the direction of the radiation source of the spoofer, then comparing the phases of the signal with several antennas.
- Detection based on the definition of Doppler frequency shift.
- Using the military GNSS signal as a reference (without needing to know the encryption key).
- Comparing the indications of the inertial navigation system and the data from the GNSS receiver.

Dual-antenna Spoofing Detector

Two antennas are installed on the Spoofing Detector (SD) (Figure 7). The distance between the antennas is denoted as D_{1-2}, a similar solution was also discussed in the literature (Psiaki et al., 2011; Dobryakova, Lemieszewski & Ochin, 2014b), but the latter used spoofing detection methods based on a dual-receiver based on correlation with the military signals.

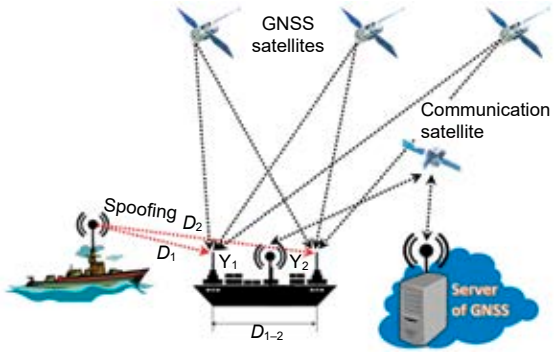

Figure 7. Spoofer and dual-antenna spoofing detector (DS): Y1 and Y2 – antennas of the DS; D_1 and D_2 – the distances from the antenna of the spoofer to the antennas of the DS, D_{1-2} – the distance between the antennas of the DS

Measuring the distance between antennas in normal navigation mode

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

$$\left\{\begin{array}{c}\sqrt{(x_1-x_{v1})^2+(y_1-y_{v1})^2+(z_1-z_{v1})^2}\\ \sqrt{(x_2-x_{v1})^2+(y_2-y_{v1})^2+(z_2-z_{v1})^2}\\ \cdots\\ \sqrt{(x_N-x_{v1})^2+(y_N-y_{v1})^2+(z_N-z_{v1})^2}\end{array}\right\}\rightarrow \xrightarrow[\text{for Sat}_i,\ i=\overline{1,N}]{\text{Iteration algorithm}} (\hat{x}_{v1},\hat{y}_{v1},\hat{z}_{v1}) \tag{7}$$

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.

$$\left\{\begin{array}{c}\sqrt{(x_1-x_{v2})^2+(y_1-y_{v2})^2+(z_1-z_{v2})^2}\\ \sqrt{(x_2-x_{v2})^2+(y_2-y_{v2})^2+(z_2-z_{v2})^2}\\ \cdots\\ \sqrt{(x_N-x_{v2})^2+(y_N-y_{v2})^2+(z_N-z_{v2})^2}\end{array}\right\}\rightarrow \xrightarrow[\text{for Sat}_i,\ i=\overline{1,N}]{\text{Iteration algorithm}} (\hat{x}_{v2},\hat{y}_{v2},\hat{z}_{v2}) \tag{8}$$

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 unknown values and, accordingly, the estimate $\hat{D}_{1-2}$ of the distance between the antennas will be comparable with the magnitude of D_{1-2}:

$$\hat{D}_{1-2}=\sqrt{(\hat{x}_{v1}-\hat{x}_{v2})^2+(\hat{y}_{v1}-\hat{y}_{v2})^2+(\hat{z}_{v1}-\hat{z}_{v2})^2}\cong \cong D_{1-2} \tag{9}$$

Measurement of the spacing between antennas in spoofing mode

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

$$\left\{\begin{array}{c}\sqrt{(x_1-x_{v1})^2+(y_1-y_{v1})^2+(z_1-z_{v1})^2}+D_s^{v1}\\ \sqrt{(x_2-x_{v1})^2+(y_2-y_{v1})^2+(z_2-z_{v1})^2}+D_s^{v1}\\ \cdots\\ \sqrt{(x_N-x_{v1})^2+(y_N-y_{v1})^2+(z_N-z_{v1})^2}+D_s^{v1}\end{array}\right\}\rightarrow \xrightarrow[\text{for Sat}_i,\ i=\overline{1,N}]{\text{Iteration algorithm}} (\hat{x}_{s'},\hat{y}_{s'},\hat{z}_{s'}) \tag{10}$$

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

$$\left\{\begin{array}{c}\sqrt{(x_1-x_{v2})^2+(y_1-y_{v2})^2+(z_1-z_{v2})^2}+D_s^{v2}\\ \sqrt{(x_2-x_{v2})^2+(y_2-y_{v2})^2+(z_2-z_{v2})^2}+D_s^{v2}\\ \cdots\\ \sqrt{(x_N-x_{v2})^2+(y_N-y_{v2})^2+(z_N-z_{v2})^2}+D_s^{v2}\end{array}\right\}\rightarrow \xrightarrow[\text{for Sat}_i,\ i=\overline{1,N}]{\text{Iteration algorithm}} (\hat{x}_{s''},\hat{y}_{s''},\hat{z}_{s''}) \tag{11}$$

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

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

$$\hat{D}_{1-2}=\sqrt{(\hat{x}_{s'}-\hat{x}_{s''})^2+(\hat{y}_{s'}-\hat{y}_{s''})^2+(\hat{z}_{s'}-\hat{z}_{s''})^2}\cong 0 \tag{12}$$

The decisive rule 1

Comparing equations (9) and (12), the decisive rule for detecting spoofing can be written as (further information can be found in the literature (Dobryakova, Lemieszewski & Ochin, 2014a)):

$$\text{if } \hat{D}_{1-2}\le \check{D} \text{ then go to Spoofing} \tag{13}$$

where $\check{D}$ – discriminant, determined on the basis of statistical studies at the design stage of a real detection system.

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

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

$$\Delta\hat{\rho}_i = \left(\hat{\rho}_{i'} - \hat{\rho}_{i''}\right) \tag{14}$$

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

$$\sigma_{\text{gnss}} = \sqrt{\frac{\sum_{i=1}^{N}\left(\hat{\rho}_{i'} - \hat{\rho}_{i''}\right)^2 - \frac{1}{N}\left(\sum_{i=1}^{N}\left(\hat{\rho}_{i'} - \hat{\rho}_{i''}\right)\right)^2}{N-1}} >> 0 \tag{15}$$

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

$$\sigma_s \cong 0 \tag{16}$$

The decisive rule 2

Comparing equations (15) and (16), the decisive rule of spoofing detection as can be written as:

$$\text{if } \sqrt{\frac{\sum_{i=1}^{N}\left(\hat{\rho}_{i'} - \hat{\rho}_{i''}\right)^2 - \frac{1}{N}\left(\sum_{i=1}^{N}\left(\hat{\rho}_{i'} - \hat{\rho}_{i''}\right)\right)^2}{N-1}} < \\ < \frac{\sigma_{\text{gnss}} - \sigma_s}{2} \text{ then go to Spoofing} \tag{17}$$

If it can be assumed that $\sigma_{\text{gnss}} >> \sigma_s$, then the decisive spoofing detection rule can be written as:

$$\text{if } \sqrt{\frac{\sum_{i=1}^{N}\left(\hat{\rho}_{i'} - \hat{\rho}_{i''}\right)^2 - \frac{1}{N}\left(\sum_{i=1}^{N}\left(\hat{\rho}_{i'} - \hat{\rho}_{i''}\right)\right)^2}{N-1}} < \\ < \frac{\sigma_{\text{gnss}}}{2} \text{ then go to Spoofing} \tag{18}$$

Discussion of the decisive rules

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

Table 1. Mistakes in 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 questions of optimal design and the selection of boundary conditions with the aim of minimizing the probabilities of "false alarm" and "missing target" are beyond the scope of this article. One of the widely used techniques is the application of Bayes' theorem (or Bayesian formula).

Single-antenna spoofing detector

Supposing that the vehicle is moving in an arbitrary direction and a single-antenna Y is installed on the spoofing detector (Figure 8). Then denoting 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 $D_{1\text{–}2}$, then:

$$\left\{\begin{array}{c} \sqrt{\left(x_1 - x_{v''}\right)^2 + \left(y_1 - y_{v''}\right)^2 + \left(z_1 - z_{v''}\right)^2} \\ \sqrt{\left(x_2 - x_{v''}\right)^2 + \left(y_2 - y_{v''}\right)^2 + \left(z_2 - z_{v''}\right)^2} \\ \cdots \\ \sqrt{\left(x_N - x_{v''}\right)^2 + \left(y_N - y_{v''}\right)^2 + \left(z_N - z_{v''}\right)^2} \end{array}\right\} \rightarrow \\ \xrightarrow[\text{for Sat}_i,\ i=\overline{1,N}]{\text{Iteration algorithm}} \left(\hat{x}_{v''}, \hat{y}_{v''}, \hat{z}_{v''}\right) \tag{19}$$

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

The distance between antenna Y at the time t and the antenna Y at the time $t'' = t' + \Delta t$ will be comparable with the magnitude of $D_{1\text{–}2}$:

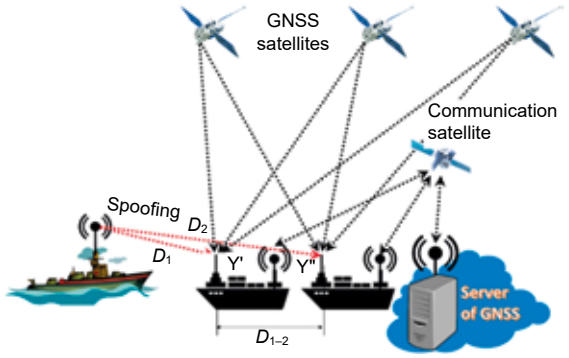

Figure 8. Spoofer and single-antenna spoofing detector (DS): Y' and Y" – the two positions of single-antenna Y; D_1 and D_2 – the distances from the antenna of the spoofer to antenna Y of the DS; D_{1-2} – the distance between the two positions of single-antenna Y

$$\hat{D}_{1-2} = \sqrt{(\hat{x}_{v'} - \hat{x}_{v''})^2 + (\hat{y}_{v'} - \hat{y}_{v''})^2 + (\hat{z}_{v'} - \hat{z}_{v''})^2} \cong \cong D_{1-2} \quad (20)$$

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

A victim will receive the same signal as the spoofer, but with delay . This means that all the receivers in the spoofing zone will calculate the same false coordinates, regardless of the distance from the spoofer to the victim:

$$\left\{ \begin{array}{l} \sqrt{(x_1 - x_{v'})^2 + (y_1 - y_{v'})^2 + (z_1 - z_{v'})^2} + D_s^{v'} \\ \sqrt{(x_2 - x_{v'})^2 + (y_2 - y_{v'})^2 + (z_2 - z_{v'})^2} + D_s^{v'} \\ \cdots \\ \sqrt{(x_N - x_{v'})^2 + (y_N - y_{v'})^2 + (z_N - z_{v'})^2} + D_s^{v'} \end{array} \right\} \rightarrow \xrightarrow{\text{Iteration algorithm for Sat}_i,\ i=\overline{1,N}} (\hat{x}_{s'}, \hat{y}_{s'}, \hat{z}_{s'}) \quad (21)$$

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

$$\left\{ \begin{array}{l} \sqrt{(x_1 - x_{v''})^2 + (y_1 - y_{v''})^2 + (z_1 - z_{v''})^2} + D_s^{v''} \\ \sqrt{(x_2 - x_{v''})^2 + (y_2 - y_{v''})^2 + (z_2 - z_{v''})^2} + D_s^{v''} \\ \cdots \\ \sqrt{(x_N - x_{v''})^2 + (y_N - y_{v''})^2 + (z_N - z_{v''})^2} + D_s^{v''} \end{array} \right\} \rightarrow \xrightarrow{\text{Iteration algorithm for Sat}_i,\ i=\overline{1,N}} (\hat{x}_{s''}, \hat{y}_{s''}, \hat{z}_{s''}) \quad (22)$$

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

In this case, the distance between antenna Y_1 at time t' and antenna Y_2 at time $t'' = t' + \Delta t$ can be defined as:

$$\hat{D}_{1-2} = \sqrt{(\hat{x}_{s'} - \hat{x}_{s''})^2 + (\hat{y}_{s'} - \hat{y}_{s''})^2 + (\hat{z}_{s'} - \hat{z}_{s''})^2} \cong 0 \quad (23)$$

The decisive rule 1

Comparing equations (20) and (23), the decisive rule for detecting spoofing can be written as:

$$\text{if } \hat{D}_{1-2} \leq \check{D} \text{ then } \langle \text{Spoofing} \rangle \text{ else } \langle \text{GNSS} \rangle \quad (24)$$

where $\check{D}$ – discriminant, determined on the basis of statistical studies at the design stage of a real detection system.

Summary and conclusions

This paper has introduced the use of Cloud-based GNSS Navigation to develop the novel concept of antispoofing. The main features of one of the major antispoofing Cloud-based GNSS Navigation have been presented, and the services have been described. Next, the general architecture of an antispoofing Cloud-based GNSS Navigation was discussed where GNSS raw samples could be simultaneously 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 into the system by updating the Cloud-based GNSS Navigation software, regardless of the user's terminals.

The risk of losing the 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 cannot only be instigated by the military, but also by terrorists. The distortion of the signal includes signal capture and playback at the same frequency with a slight time shift and greater intensity, in order to deceive the electronic equipment of the victim.

It is important to emphasize that GNSS is not only used for 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 the time on stand-alone passive devices to be synchronized with high accuracy.

References

1. Dobryakova, L., Lemieszewski, Ł. & Ochin, E. (2014a) Design and Analysis of Spoofing Detection Algorithms for GNSS Signals, *Scientific Journals Maritime University of Szczecin, Zeszyty Naukowe Akademia Morska w Szczecinie* 40 (112), pp. 47–52.
2. Dobryakova, L., Lemieszewski, Ł. & Ochin, E. (2014b) Transport safety: the GNSS spoofing detecting using two navigators/Bezpieczeństwo w transporcie: wykrycie ataku GNSS spoofing za pomocą dwóch nawigatorów. *Logistyka* 3, pp. 1328–1331.
3. Dobryakova, L., Lemieszewski, Ł. & Ochin, E. (2016) The vulnerability of unmanned vehicles to terrorist attacks such as GNSS-spoofing. *Scientific Journals Maritime University of Szczecin, Zeszyty Naukowe Akademia Morska w Szczecinie* 46 (118), pp. 181–188.
4. Humphreys, T.E., Ledvina, B.M., Psiaki, M.L., O'Hanlon, B.W. & Kintner Jr., P.M. (2008) *Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer*. Preprint of the 2008 ION GNSS Conference Savanna, GA, September 16–19.
5. Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J. & Lachapelle, G. (2012) GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. *Hindawi Publishing Corporation International Journal of Navigation and Observation*, Article ID127072, doi: 10.1155/2012/127072.
6. Januszewski, J. (2010) *Systemy satelitarne GPS, Galileo i inne*. PWN.
7. Jones, M. (2011) The civilian battlefield. Protecting GNSS receivers from interference and jamming. *Inside GNSS*, Mar./Apr., pp. 40–49.
8. Lucas-Sabola, V., Seco-Granados, G., López-Salcedo, J.A., García-Molina, J.A. & Crisci, M. (2016) *Cloud GNSS receivers: New advanced applications made possible*. 2016 International Conference on Localization and GNSS (ICL-GNSS), Barcelona, pp. 1–6.
9. Ochin, E., Lemieszewski, Ł., Lusznikov, E. & Dobryakova, L. (2013) The study of the spoofer's some properties with help of GNSS signal repeater. *Scientific Journals Maritime University of Szczecin, Zeszyty Naukowe Akademia Morska w Szczecinie* 36 (108) z. 2, pp. 159–165.
10. Psiaki, M.L., O'Hanlon, B.W., Bhatti, J.A., Shepard, D.P. & Humphreys, T.E. (2011) *Civilian GPS Spoofing Detection based on Dual-Receiver Correlation of Military Signals*. Preprint from ION GNSS, Proceedings of ION GNSS, Portland, Oregon, 2011.
11. Raia, M. (2011) The Benefits of Choosing a Cloud-Based GPS Tracking System. *CloudExpo Journal*, August 18, http://cloudcomputing.sys-con.com/node/1950571 [Accessed: April 13, 2018].
12. Seco-Granados, G., López-Salcedo, J.A., Jimenez-Banos, D. & López-Risueno, G. (2012) Challenges in Indoor Global Navigation Satellite Systems. *IEEE Signal Proc. Mag*. 29, 2, pp. 108–131.
13. Specht, C. (2007) *System GPS*. Biblioteka Nawigacji nr 1. Pelplin: Wydawnictwo Bernardinum.
14. Zalewski, P. (2014) Real-time GNSS spoofing detection in maritime code receivers. *Scientific Journals Maritime University of Szczecin, Zeszyty Naukowe Akademia Morska w Szczecinie* 38 (110), pp. 118–124.