УДК 621.396

МОДЕЛИ GPS-ПОДМЕНЫ ДЛЯ ГРАЖДАНСКОЙ НАВИГАЦИОННОЙ АППАРАТУРЫ ПОТРЕБИТЕЛЕЙ

MODELS OF GPS-SPOOFING OF CIVIL NAVIGATION EQUIPMENT OF CONSUMERS

А. В. Короткевич,
декан факультета радиотехники и электроники Белорусского государственного университета информатики и радиоэлектроники, канд. техн. наук, доцент, г. Минск, Республика Беларусь

Х. Х. Саад
аспирант кафедры информационных радиотехнологий Белорусского государственного университета информатики и радиоэлектроники, г. Минск Республика Беларусь

К. В. Ступин
аспирант кафедры информационных радиотехнологий Белорусского государственного университета информатики и радиоэлектроники, г. Минск Республика Беларусь.

A. Korotkevich,
Dean of the Faculty of Radioengeering and Electronics of Belarusian State University of Informatics and Radio electronics, PhD, Professor, Minsk, Republic of Belarus

H. Kh. Saad,
PhD Student of Information Radioengineering department of Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

K. Stupin,
PhD student of Information Radioengineering department of Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Дата поступления в редакцию — 15.12.2021.

В этой статье приведены принципы и модели GPS-спуфинга для гражданской навигационной аппаратуры потребителей, приведены данные по зарегистрированным инцидентам GPS-спуфинга, приведена классификация вариантов GPS-спуфинга.

Models of GPS spoofing of civil navigation equipment of consumers will be shown in this article, highlighting the most registered incidents, the principle of GPS spoofing, classification of GPS spoofing options.

Ключевые слова: GPS-спуфинг, математические модели, классификация, гражданская навигационная аппаратура потребителей.

Keywords: GPS spoofing, mathematical models, classification, civil navigation equipment of consumers.

Problem statement.

Examining the success or the failure of a GPS spoofing act depends on many features and parameters related to the navigation process, taking in consideration the number of targeted receiver(s) (single or multi-receivers) in addition to the signal's strength transmitted power, the distance between the spoofer and the victim, the time offset, Doppler shift, delay locked loop bandwidth, etc. To sum up, mathematical compensation formulations will be done to study the possible ways in order to differentiate between the possible GPS spoofing success and failure, to attain at the end the best methodology that should be followed to meet our aim in GPS spoofing.

Many GPS spoofing incidents have been registered in the modern technological history [1–9]. The most famous cases known either on the air or land or sea vehicles are shown in the following:

Regulus Tesla Spoofing Experiment; Regulus Cyber spoofed a Tesla Model 3 off the road during a test drive using Navigate on Autopilot (NOA). The driver was taken by surprise, by the time he grabbed the wheel, it was too late to correct the car's position and get it back on the highway smoothly [1].

"Ghost ships" circle off San Francisco coast; data analyst Bjorn Bergman discovered nine ships broadcasting false GPS signals from Point Reyes, just north of San Francisco, California [2]. In truth, the ships were thousands of miles away in locations as diverse as the Norwegian Sea, Eastern Mediterranean, and Nigerian coast.

Iran-U.S. RQ-170 incident; on December 5, 2011, Iranian forces commandeered a U.S. Lockheed Martin RQ-170 Sentinel stealth drone flying about 140 miles from Iran's border with Afghanistan [4]. The Iranian government announced that the drone was spoofed and "brought down with minimal damage" by a cyber warfare unit [5].

University of Texas researchers steer multimillion dollar yacht off its course; the experiment took place as the 213-foot yacht traveled across the Mediterranean Sea from Monaco to Greece [6].

GPS interference near Chinese ports (over 20 Chinese coastal sites); showing ships moving in "crop circles" up to a few miles away from their actual positions. Most interference sites were oil terminals and government installations, suggesting that spoofing could be a security or anti-surveillance measure used to conceal crude oil shipments; manipulation was still ongoing in four cities (Shanghai, Dalian, Fuzhou, and Quanzhou) as of May 2020 [7].

Accidental GNSS Spoofing affects multiple mobile phones in a conference, happened in the Portland Convention Center at the 17-th annual ION GNSS+ Conference on September 28, 2017 [8]. Conference

attendees began noticing malfunctions with their mobile phones in the morning, for some, both texting and email were disabled. Many confused conference-goers saw their phone date and time reset to sometime in January 2014 and their current location reset to Toulouse, France.

'Circle-style' GPS spoofing is reported in Iran's capital, Tehran, around the Iranian Army training college, it's the first outside of China, where similar patterns were observed in Shanghai in 2019 [9].

In addition to the previous, there is an assumed incident that Somali pirates, for example, can acquire such technology, thus GNSS spoofing. It can be transmitted over a very long range, and the thing is, once the ship goes off-course close the coast of Somalia, it's not only at risk of being raided, but also when they call for help from the international force there meant to protect them, the location they will transmit won't be real. So, the intervention force will actually reach a location when there's nobody there.

On the other hand, GPS jamming cases are also recorded, some of which are: **an i**ntermittent GPS signal loss experienced by aircraft landing at Harbin airport in north-eastern China is traced to a jammer installed at a nearby pig farm [10]; Mexico passes an anti-jammer law, discovered that GPS jammers are being in 85 % of cargo vehicle thefts in the country [11].

Note that another GPS spoofing and jamming attacks happened, but we just list the most famous registered ones focusing on the more complex (spoofing).

The general principle of GPS spoofing/mathematical modelling.

In general, the consumer's navigation equipment will function in the presence of multipath, jamming, false navigation signals generated by one or more sources of spoofing, noise interference and internal noise of receiving channels. This situation is shown in Figure 1. GPS spoofing can be defined as transmitting fake GPS navigation messages to the targeted receiver in order to interrupt the position, navigation, and time solutions of the desired receiver, thus wrong position [12]. While GPS jamming is simple than spoofing, which is briefed in emitting the same frequency as that of the navigation satellite (NS) with a suitable level of power and estimated distance, the way which lead to interrupt the navigation signal leading to the nulling of the available signals from different satellites. Furthermore, multipath is an unintentional interference, which results from the reflection of the GNSS signals when hitting an obstacle as a tower, building, etc. Noise either external or internal is considered as a normal case of unintentional interference due to the thermal noise, noise figure and others in the receiver's equipment and other cases related to the surroundings and AWGN [13].

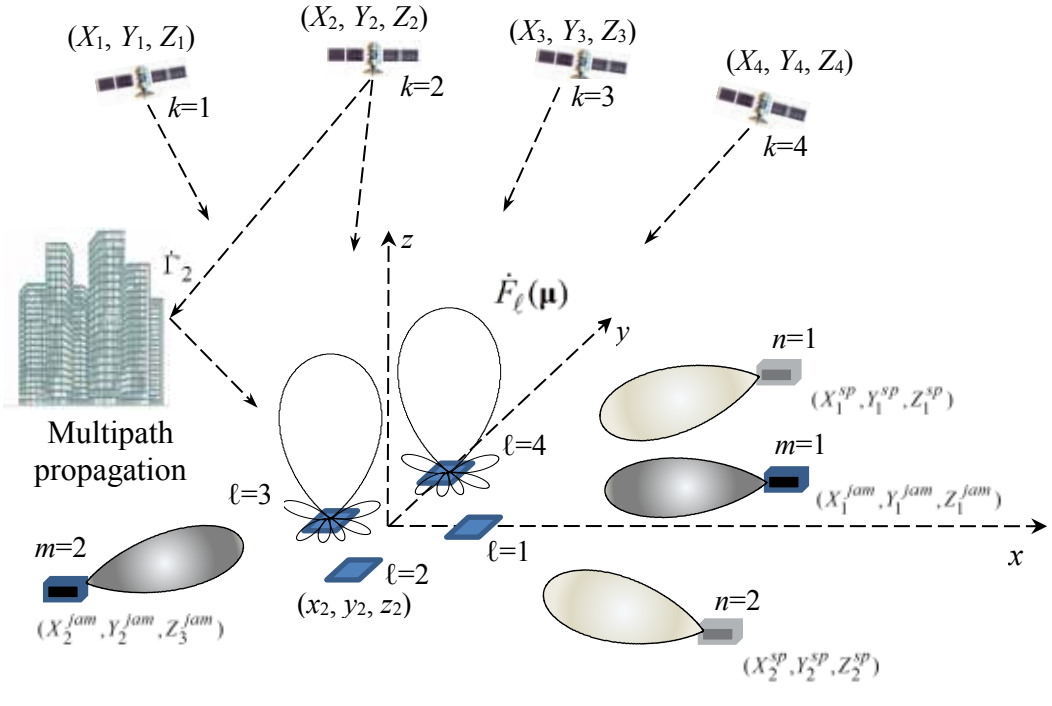

Figure 1. The different possible types of interference on the consumer navigation equipment

In our modeling, we will assume that the antenna system of the consumer's navigation equipment (CNE) includes $\ell = \overline{1, L}$ receiving channels with coordinate vectors of phase centers $\boldsymbol{\eta}_\ell(t) = (x_\ell(t), y_\ell(t), z_\ell(t))^{\mathrm{T}}$, where the dependence on time t reflects the law of motion of the center of mass of the consumer's equipment and the possible rotational movements of the antenna system of the equipment. The distances between the phase centers and the geometric center of the antenna system with $\boldsymbol{\eta}_0(t)$ coordinates are such that $|\boldsymbol{\eta}_\ell - \boldsymbol{\eta}_0| << c / \Delta f_0$, where Δf_0 - is the width of the navigation signal spectrum. The coordinate vector $\boldsymbol{\eta}_0(t)$ defines the phase center of the antenna system and is used to simplify the description of the navigation signals' time delays.

The coordinates of the $k = \overline{1, K}$ NSs are $\boldsymbol{\mu}_k(t) = (X_k(t), X_k(t), Z_k(t))^{\mathrm{T}}$. Signs of visibility of NSs $V_k^{ns} = 0$, if the satellite is below the horizon line (not visible) and $V_k^{ns} = 1$ if the satellite is above the horizon line (visible). The time index is omitted in this case, since it is assumed that the visibility conditions of the satellites do not change during the analysis.

To describe multipath propagation when the signal of the *k*th NS is reflected from some object (area), we assume that the reflected signal comes to the receiving channel from some point in space $\boldsymbol{\mu}_k^{\mathrm{mul}}(t)$ with a time delay τ_k relative to the true signal. The scale factor for the amplitude of the reflected signal is $\dot{\Gamma}_k$, where the argument $\varphi_k = \arg(\dot{\Gamma}_k)$ takes into account both the reflection from the object and the delay during multipath propagation.

Destructive effects are created by $m = \overline{1, M_{jam}}$ sources of jamming with $\boldsymbol{\nu}_m(t) = (X_m^{jam}(t), Y_m^{jam}(t), Z_m^{jam}(t))^{\mathrm{T}}$ coordinate vectors and $n = \overline{1, N_{sp}}$ sources of false navigation signals (spoofing) with $\boldsymbol{\upsilon}_n(t) = (X_n^{sp}(t), Y_n^{sp}(t), Z_n^{sp}(t))^{\mathrm{T}}$ coordinates. Each of the sources of false navigation signals can create $V_{n,k}^{sp}(t) = 1$ or not create $V_{n,k}^{sp}(t) = 0$ false navigation signal from the k -th NS, and these conditions may change during observation.

The received implementation at the output of the ℓth receiving channel can be represented as:

$$\dot{Y}_\ell(t) = \underbrace{\sum_{k=1}^{K} V_k^{ns} \dot{S}_k(t) \dot{F}_\ell(\boldsymbol{\mu}_k)}_{\text{true signals}} + \underbrace{\sum_{k=1}^{K} V_k^{ns} \dot{\Gamma}_k \dot{S}_k(t - \tau_k) \dot{F}_\ell(\boldsymbol{\mu}_k^{\mathrm{mul}}(t))}_{\text{multipath}}$$
$$+ \underbrace{\sum_{n=1}^{N_{sp}} \sum_{k=1}^{K} V_{n,k}^{sp}(t) \dot{W}_n(t,k) \dot{F}_\ell(\boldsymbol{\upsilon}_n)}_{\text{spoofing}} + \underbrace{\sum_{m=1}^{M_{jam}} \dot{U}_m(t) \dot{F}_\ell(\boldsymbol{\nu}_m)}_{\text{jamming}} + \underbrace{\dot{N}_\ell(t)}_{noise}, \quad (1)$$

where $\dot{S}_k(t)$ is the true navigation signal from the kth NS at the output of the isotropic receiving antenna; $\dot{F}_\ell(\mathbf{v})$ is the radiation pattern of the ℓth receiving channel in the direction of a point with Cartesian coordinates $\mathbf{v}$, and the phase of the radiation patterns is counted from the common phase center for all elements of the antenna system; $\dot{W}_n(t,k)$ is the false signal of the kth NS generated by the source of spoofing at the output of the isotropic receiving antenna;

$\dot{U}_m(t)$ — interference from the mth source of jamming at the input of an isotropic receiving antenna;

$\dot{N}_\ell(t)$ — intrinsic noise of the ℓth receiving channel with a power of $\sigma_\ell^2 = |\dot{N}_\ell(t)|^2 = \sigma_0^2$.

The model (1) is universal and allows reproducing a large number of situations characterized by different conditions of multipath propagation, the presence of one or more sources of spoofing and jamming, in addition to external and internal noise interference. Further complication of the model is achieved by: increasing the number of beams for multipath propagation of true signals and introducing multipath propagation for false navigation signals; introduction of polarization parameters of true and false navigation signals (including

multipath) and jamming and the use of vector radiation patterns of receiving channels in a given polarization basis.

Let's write down the components of the model (1). For the true signal from the *k*th NS:

$$\dot{S}_k(t) = \sqrt{P_k} C_k(t + \tau_k^{ns} - t_{r_k}) D_k(t) \mathrm{e}^{j((\omega_0 + \Omega_k(t))t + \varphi_k)}, \qquad (2)$$

where P_k is the signal power from the *k*th NS at the output of the isotropic receiving antenna, determined by the distance to the satellite and the conditions of propagation of electromagnetic waves;

$C_k(t) = -1;1$ is the rangefinder code of the *k*th NS;

τ_k^{ns} is the offset of the time scale of the *k*th NS relative to the time scale of the navigation system;

$t_{r_k} = |\boldsymbol{\mu}_k(t) - \boldsymbol{\eta}_0(t)|/c$ is the signal delay from the NS to the CNE's antenna;

c is the speed of propagation of electromagnetic waves;

$D_k(t) = -1;1$ is a true navigation message, the spectrum width of which is much smaller than the spectrum width of the rangefinder code;

ω_0 is the carrier frequency, for the GPS system $f_0 = \frac{\omega_0}{2\pi} = 1575,42$ MHz;

$\Omega_k(t) = \frac{\omega_0}{c}\frac{d}{dt}|\boldsymbol{\mu}_k(t) - \boldsymbol{\eta}_0(t)|$ is the Doppler frequency shift of the signal from the *k*th NS;

φ_k is a random but constant phase shift of NS signal during the observation interval.

For the false navigation signal of the *k*th NS created by the *n*th source of spoofing, we write:

$$\dot{W}_n(t,k) = \sqrt{P_{n,k}^{sp}} C_k(t + \tau_n^{sp} - t_{n,k}^{sp}) D_{n,k}^{sp}(t) \mathrm{e}^{j((\omega_0 + \Omega_{n,k}^{sp}(t))t + \varphi_{n,k}^{sp})}, \qquad (3)$$

where $P_{n,k}^{sp}$ is the power of the false signal of the *k*th NS created by the *n*th source of spoofing at the output of the isotropic receiving antenna;

τ_n^{sp} — the time scale offset of the nth source of suffixing relative to the time scale of the navigation system;

$t_{n,k}^{sp}$ is the delay of the false signal of the kth NS created by the nth spoofing source;

$D_k^{sp}(t)$ is a complex navigation message created by the kth NS;

$\Omega_{n,k}^{sp}(t)$ is the law of change of the Doppler frequency shift;

$\varphi_{n,k}^{sp}$ — the initial phase.

Noise interference $\dot{U}_m(t)$ is a Gaussian random process with a uniform (within the bandwidth of the receiving channels) spectral power density $N_m = P_m^{jam} / \Delta f_0$, where $P_m^{jam} = \overline{|\dot{U}_m(t)|^2}$ is the power of the *m*th source of jamming at the output of an isotropic receiving antenna. Interference from various sources and internal noise are uncorrelated $\overline{\dot{U}_m(t)U_n^*(t)} = \delta(m-n)P_m^{jam}$, $\overline{\dot{U}_m(t)N_\ell^*(t)} = 0$, where $\delta(m)$ — the Kronecker symbol.

Note that the model (1) taking into account (2), (3) is universal. By controlling the parameters $P_{n,k}^{sp}$, $t_{n,k}^{sp}$, $\Omega_{n,k}^{sp}$ in (3) in terms of spoofing, the parameters $\dot{\Gamma}_k, \tau_k, \boldsymbol{\mu}_k^{mul}$ in (1) in terms of multipath propagation, as well as the parameters $P_m^{jam}, \mathbf{v}_m$ in terms of jamming, situations of any complexity can be reproduced.

In order to understand more the issue of GPS spoofing, one should take into account the different parameters concerning the principle of this attack. On the other hand, understanding and obeying the laws and standards of the GPS spoofing options and the features of classification of this type of spoofing would lead to the desired deliverables. Table 1 shows the most options of GPS spoofing.

Table 1

GPS spoofing options

Classification feature	Possible options with
By the number of points for creating false navigation signals	single position; multi-position
According to the parameters of the movement of the source of false signals	static; variable
By the type of basing of false signal sources	from earth; from the building or tower; from the flight-lifting vehicle
How to remove the source of false signals from the spoofing area	directly in the field of spoofing ; at a distance from the spoofing area
By the achieved effect	with an imitation of a stationary object; with an imitation of a moving object
According to the stage of functioning of the navigation equipment, on which the impact is focused	at the stage of searching for navigation satellite signals and entering the synchronization of tracking systems by delay time and frequency/phase; at the stage of navigation definitions
According to the principle of creating false navigation signals	with the generation of navigation messages based on the known structure of the rangefinder code and the expected parameters; with the relay of GNSS signals with a delay time/frequency shift
By the polarization of a false signal	FRPA-Fixed Radiation Pattern Antenna; CRPA-Controlled Radiation Pattern Antenna
By the number of false parameters	with playback of only fixed time delays; with playback of fixed time delays and frequency offset; with the reproduction of the law of changes in time delays and frequency shift during the movement of navigation satellites
By combining with masking interference	without combining with masking interference; joint use with masking interference

Such act can be done either directly by using a GPS signal generator or by receiving the GPS navigation signals and re-transmitting them with changing the different parameters to the victim receiver. Moreover, many parameters play an essential role in the GPS spoofing technique, such as:

– the power of the spoofing signal and the power related parameters such as: carrier to noise density ratio, absolute received signal power, power variations, L1/L2 band power ratio;

– time relayed parameters;

– sample values at correlator output;

– spatial processing thus detecting multiple signals with the same direction of arrival, cryptographic security and protection measures.

The basic concept of GPS spoofing.

To deceive the receiver, a high power RF noise must first be transmitted to force the receiver to lose its lock to the genuine signal [14], followed by the counterfeit signal with a much higher power level than the real signal. This kind of spoofing can be easily detected because both the loss of the lock and the abnormally high SNR will alert the receiver, but most current civilian GPS receivers cannot detect this and successful attacks have already been demonstrated [15]. Intermediate spoofing is an attack via a spoofer's receiver, which is composed of a GNSS receiver and a signal generator. The receiver tracks satellite signals to accurately synchronize with the satellite time and emphasis with estimates of the Doppler frequencies and code phases of every satellite signal tracked by the victim receiver [16]. Then the signal generator uses this information to generate counterfeit signals synchronized to the genuine signal. The spoofer's receiver adjusts the code phase and the carrier frequency of the fake signal to align with the genuine signal and then increases the power a

little to control the correlation peak so as to lead the correlation peak away from the genuine peak [17]. This kind of spoofing can deceive a receiver without breaking the tracking state, which is hard to detect by receivers except for the multi-antenna receivers. The normal spoofing process can be confined in the following steps:

1. The spoofer tracks the true signals and estimates the code phase and the carrier frequency that the targeted receiver tracks, using the targeted receiver information related to the synchronization with the satellite time, estimation of Doppler frequencies and satellites code phases [18].

2. The spoofer generates the fake signal at a low power and many code chips away from the true one tracked by the targeted receiver [19].

3. The spoofer adjusts the code phase to align with the true signal (acting like a multipath signal), and then increase the signal power to control the tracking points.

4. The spoofer adjusts the code phase to drag the correlation peak away from the true signal to then completely control the targeted receiver [20].

Generalization of ways to protect against spoofing.

The results of the analysis of well-known and universal works on countering GPS spoofing in civilian consumer equipment shows that the general principle of constructing protection methods is to perform four operations:

– detection of the presence of false navigation signals;

– selection of true and false navigation signals for each navigation satellite or, if there is a lack of processing capacity, for the selected constellation of satellites;

– evaluation and compensation processing, which includes estimating the parameters (delay time, Doppler frequency shift and complex amplitude) of false navigation signals and their compensation by subtracting a scaled copy of the signal from the received implementation [21];

– processing of the implementation obtained after evaluation and compensation processing by standard methods with obtaining estimates of the $(\hat{x}, \hat{y}, \hat{z})$ coordinates of navigation equipment and their derivatives.

The specified sequence of actions is shown in Figure 2.

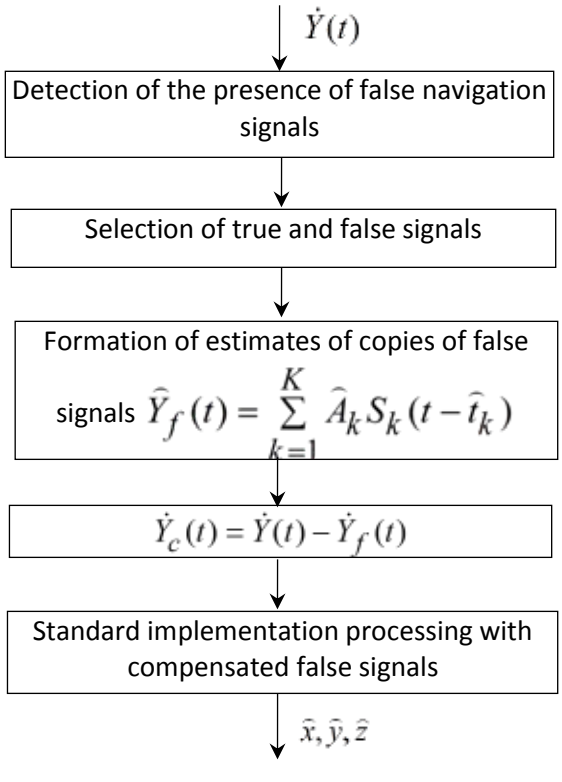

Figure 2. General structure of the GPS-spoofing protection algorithm

The basis of this sequence is evaluation and compensation processing, which allows using the well-proven structure of consumer navigation equipment in the coherent reception of navigation signals.

When selecting true and false signals, two situations must be taken into account:

– before the appearance of spoofing or jamming, the consumer equipment functioned normally and the time scales of the navigation system and equipment were aligned; sufficiently high accuracy of the alignment of the time scales will be maintained during the time interval determined by the stability of the frequency of the master generator of the navigation equipment; an increase in the mismatch of the time scales can be taken into account in (2) if the parameter τ_k^{ns} is made dependent on the current time t;

– navigation equipment begins to function in conditions of spoofing or jamming and the coordination of time scales has not been completed.

For the first of these situations, estimates $(\hat{x},\hat{y},\hat{z})$ will be determined, for the second — $(\hat{x},\hat{y},\hat{z},\hat{t})$.

As we have said previously, some countermeasures should be followed in order to minimize the risk of the illegal use of GPS spoofing. Table 2 indicates a list of proposed protective measures against GPS spoofing, either by using a single channel or multi-channel antenna, knowing that the last may be rotational beamforming array antenna or adaptive array antenna (adaptive beamforming).

Table 2

Protection measures against GPS spoofing

Type of navigation equipment	Possible options
Single channel receiver	The detection of the presence of two (or more) of signals from one navigation satellite, selection of false signals on the level (amplitude), estimation of time delay, the complex amplitude and phase signals about their subtraction (estimated-compensation processing) of the accepted implementation with the subsequent processing of the implementation in the traditional way. Breeding of false signals in the residual rate of change of time delay and Doppler frequency shift. 3. Selection of false signals based on the content of the navigation message (taking into account the available a priori data). 4. Selection of false signals based on the synchronicity of amplitude changes for different navigation satellites when the antenna is rotated
Multi-channel receiver	1. Measurement of bearings, thus the phase difference of receiving channels, for detected navigation signals, selection of false signals based on the same set of phase differences and evaluation and compensation processing (estimation of arrival time, complex amplitude and frequency, subtraction of a scale copy of the signal from the received implementation in the selected receiving channel without spatial processing). 2. Measurement of bearings for detected navigation signals, selection of false signals and their spatial compensation (nulling or zeros' formation towards the direction of the GPS spoofing source). 3. Combination of methods 1 and 2 with methods of the first group

Conclusion/

The article describes the concept of spoofing the navigation equipment of a GPS consumer. Based on the available information the main recorded incidents are presented. A general mathematical expression has been developed for the satellite signal received by the GPS receiver, taking into account both the signal itself and the spoofing signals and noise. Possible protection measures against various types of spoofing attacks are also presented. It is concluded that GPS spoofing is indeed a problem that our navigation world faces today, affecting various areas both in the military sphere and the navigation equipment of civilian consumers. While this is currently considered the most difficult form of deliberate interference, protective measures should be taken mainly against the illegal use of such an attack.

References:

1. Tesla model 3 spoofed off the highway — regulus navigation system hack causes car to turn on its own [Electronic resource] // REGULUS. Ed. REGULUS. 4 August 2019. — Mode of access: https://www.regulus.com/blog/tesla-model-3-spoofed-off-the-highway-regulus-navigation-system-hack-causes-car-to-turn-on-its-own. — Date of access: 12.08.2021/

2. Mystery unsolved: ghost ships circling off California [Electronic resource] // BIG THINK. Ed. HARD SCIENCE. 18 March 2021. — Mode of access: https://bigthink.com/hard-science/circle-spoofing/. — Date of access: 14.07.2021/

3. Did Russia make this ship disappear? [Electronic resource] // CNN BUSINESS. Ed. CNN Tech. 3 November 2017. — Mode of access: https://money.cnn.com/2017/11/03/technology/gps-spoofing-russia/index.html. — Date of access: 24.03.2021.

4. Iran — U.S. RQ-170 incident [Electronic resource] // en.wikipedia.org Mode of access: https://en.wikipedia.org/wiki/Iran%E2%80%93U.S._RQ-170_incident. — Date of access: 12.08.2021.

5. Top 10 GPS Spoofing Events in History [Electronic resource] // Mit, Roi. THREAT TECHNOLGY. 2021. — Mode of access: https://threat.technology/top-10-gps-spoofing-events-in-history/. — Date of access: 19.06.2021.

6. Spoofing a Superyacht at Sea [Electronic resource] // Zumalt, Erik. UT NEWS. Ed. The University of Texas at Austin. 30 July 2013. SCIENCE & TECHNOLOGY. — Mode of access: <https://news.utexas.edu/2013/07/30/spoofing-a-superyacht-at-sea/>. — Date of access: 30.06.2021

7. Samson, Brian Weeden and Victoria. GLOBAL COUNTERSPACE CAPABILITIES. Ed. Brian Weeden and Victoria Samson. Colorado, Washington: Secure World Foundation, 2021.

8. GPS Spoofing Nails Cell Phones in Portland [Electronic resource] // Scott, Logan. RESILIENT NAVIGATION and TIMING FOUNDATION. Ed. Blog. 10 October 2017. Gibbons Media & Research LLC. — Mode of access: <https://rntfnd.org/2017/10/10/spoofing-incident-report-an-illustration-of-cascading-security-failure/>. — Date of access: 19.09.2021.

9. GPS circle spoofing discovered in Iran [Electronic resource] // Goward, Dana. GPS WORLD. Ed. spirent. 21 April 2020. swift NAVIGATION. — Mode of access: <https://www.gpsworld.com/gps-circle-spoofing-discovered-in-iran/>. — Date of access: 07.04.2021.

10. A fierce fight in a pig farm that repels drones with a gang VS radio interference system that spreads swine cholera virus [Electronic resource] // Dutton, Julian. Gigazine. Ed. Pascal Debrunner. 23 December 2019. December 2019. — Mode of access: https://gigazine.net/gsc_news/en/20191223-flight-systems-jammed-pig-farm/. — Date of access: 21.12.2020.

11. GPS Jamming & Spoofing, 2020 Year in Review — Spirent's Guy Buesnel [Electronic resource] // Goward, Dana A. "Linked in." 5 December 2020. Ed. Guy Buesnel. December 2020. — Mode of access: <https://www.linkedin.com/pulse/gps-jamming-spoofing-2020-year-review-spirents-guy-buesnel-goward>. — Date of access: 21.02.2021.

12. Ali Jafarnia-Jahromi, Ali Broumandan, John Nielsen, and Gérard Lachapelle. "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques." Hindawi 2012.GPS spoofing (2012): 17.

13. Noise in Wireless Receiver Systems [Electronic resource] // Rouphael, Tony J. "ScienceDirect." 2014. — Mode of access: <https://www.sciencedirect.com/topics/engineering/system-noise-figure>. — Date of access: 29.08.2020.

14. Yang Gao, Hong Li, Mingquan Lu, and Zhenming Feng. "Intermediate Spoofing Strategies and Countermeasures." ieeeexplore 18.GPS Spoofing (2013): 7.

15. Humphreys, Mark L. Psiaki and Todd E. "GNSS Spoofing and Detection." (n.d.): 11.

16. Nils Ole Tippenhauer, Christina Pöpper, Kasper B. Rasmussen, and Srdjan ˇCapkun. "On the Requirements for Successful GPS Spoofing Attacks." IEEE (n.d.): 12.

17. Brady W. O'Hanlon, Mark L. Psiaki,Jahshan A. Bhatti, Daniel P. Shepard,Todd E. Humphreys,. "Real-Time GPS Spoofing Detection via Correlation of Encrypted Signals." Journal of the Institute of Navigation GPS spoofing (2013).

18. Beomju Shin, Minhuck Park, Sanghoon Jeon, Hyoungmin So, Gapjin Kim, and Changdon Kee. "Spoofing Attack Results Determination in Code." sensors 19.Spoofing attacks (2019): 22.

19. M. R. Mosavi, Z. Nasrpooya and M. Moazedi. "Advanced Anti-Spoofing Methods in." THE JOURNAL OF NAVIGATION 69, 883–904.GPS Spoofing (2016): 22.

20. Aanjhan Ranganathan, Hildur Ólafsdóttir, and Srdjan Capkun. "PREE: a spoofing resistant GPS receiver." The 22nd Annual International Conference. 2016.

21. Сосулин, Ю. Г. Оценочно-корреляционная обработка сигналов и компенсация помех / Ю. Г. Сосулин, В. В. Костров, Ю. Н. Паршин. — М.: Радиотехника, 2014. — 632 с.