UDC 621.396.94

MAIN PRINCIPLES OF THE SATELLITE SYSTEM PROVIDING PNT INFORMATION FOR MOVING OBJECTS UNDER GNSS VULNERABILITY

Viktor A. Gaidamanchuk, Mykola V. Matvienko

Wircom, Kyiv, Ukraine

Background. GNSS systems are the main source of PNT information (positioning; navigation; timing) for different systems that can be applied in industries, scientific research and defense. GNSS signal outages, whether natural or as intentional influence (jamming; spoofing), become an increasing problem and are the reason for research aimed at using alternative GNSS sources of PNT information, especially for moving objects.

Objective. General design synthesis of the system providing PNT information to moving objects based on atomic clocks, satellite communication system CSPC channels and VSAT spread spectrum stations with phased antenna array for application on both fixed and moving objects.

Methods. The satellite system providing PNT information modeling and research of possibility to realize main developed technical solutions based on FPGA and USPR technologies to be used on-board moving objects.

Results. Modeling and operation analysis of the system providing PNT information to moving objects based on atomic clocks, satellite communication system CSPC channels and VSAT spread spectrum stations with phased antenna array confirm possibility of using such solution for moving objects provided the maximum integration level of the devices to be installed on these objects.

Conclusions. Wide application of GNSS systems (GPS, BeiDou, GLONASS etc.) in a large number of critical industries suggests that their stable operation or timely redundancy in case of possible problems demands careful attention to development of different compensation scenarios for different applications. Discussed constructing principles of local satellite navigation system for GNSS vulnerability compensation can be of use in solving this important problem.

Keywords: GNSS vulnerability; PNT; UAS; UAV; SCPC; DSSS; VSAT.

I. Introduction

GNSS systems (GPS, BeiDou, GLONASS etc.) are widely involved in different areas of human activities and are used in a large number of critical industries such as telecommunications, transportation, finance sector, and defense to cover their needs for navigational information, time and frequency synchronization [1; 2].

But, as far as is known, GNSS systems are quite vulnerable due to unintended deny causes such as: a) natural or environmental: lightning hits, antenna icing, solar flares, atmospheric phenomena, foliage obscured GPS deployments; b) mechanical or human errors: antennas are easily damaged and can interfere with each other; GPS cable conduit dangling in the wind; harmonics or radiation from nearby electronics failures or misaligned transmission equipment; intentional influence on GNSS: jamming, spoofing and software attacks.

GNSS vulnerabilities, like cyber security, reach across virtually all world infrastructures – especially navigation and timing. Timing, and in particular GNSS-based timing as a part of navigation, is an essential cyber security component that is critical to this industry.

The importance and wide use of GNSS systems require a close analysis of both possible vulnerabilities due to different reasons and diverse scenario development for their redundancy or replacement.

II. Common Protection Scenarios Against GNSS Vulnerabilities

Naturally, for different applications, there are different reasons for vulnerabilities or faults in GNSS system operation, and they need different scenarios to prevent them or minimize possible losses [3; 4].

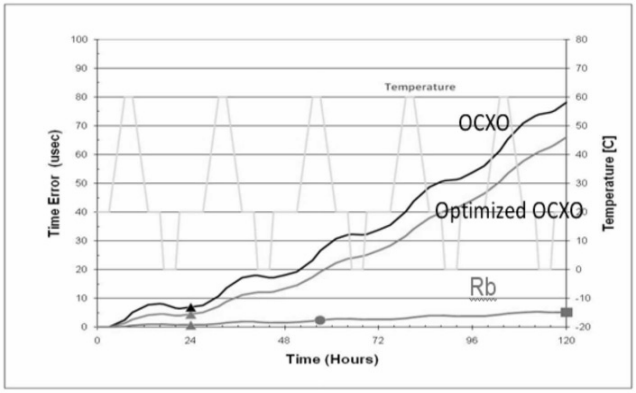

Fig. 1. Drift over time

© 2017, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"

Such scenarios are:

1) using built-in generators for holdover in case of short-term signal loss;

Fig. 1 shows a comparison of drift over time for oven controlled crystal oscillators (OCXO) versus a rubidium atomic clock (Rb).

Rubidium atomic clocks are a better solution, providing a much higher level of performance and precision with longer holdover period. Typical rubidium can hold 1,5 microsecond accuracy for up to 24 hours, while crystal oscillators ensure only 8 microsecond for up to 24 hours under the similar conditions [Fig. 2].

	Accuracy	Holdover Period
Crystal OCXO	± 8 µs	24 hours
Rubidium Atomic Clock	± 1.5 µs	24 hours

Fig. 2. 24 Hour holdover perfomance

2) using alternative synchronization signals delivered through PTP technology;

3) using GNSS receivers with built-in systems of intrusion (such as jamming and spoofing) detection and automatic switch to alternative available synchronization sources.

But existing methods are not enough and can not fully compensate GNSS vulnerability, and in many cases can not be used due to specifics of applications.

III. Example Application Where Special Protection Scenario is Needed

One of the example applications, where special protection scenario is needed, is using GNSS signals to support navigation for Unmanned Aircraft System (UAS).

Taking into consideration that using of the above objects involves possibility of long-term staying in the regions of intentional usage of methods which cause trouble in using or make GNSS signals unavailable for long period, the development of alternative secure satellite channel is the topical problem because it will deliver signals for navigation support of the object under loss or vulnerability of GNSS signal reception [5].

Fig. 3 depicts a scenario of Unmanned Aerial Vehicle (UAV) operating in the environment, where the proposed system can be necessary to maintain right flight direction.

Using GPS jammers (1) with highly directional antennas long-distance (over 250 km) areas (2) can be developed, where traveling UAV after losing GNSS signal guiding reference direction (3) will move in a false direction (4) which could greatly deviate from a reference (right) one.

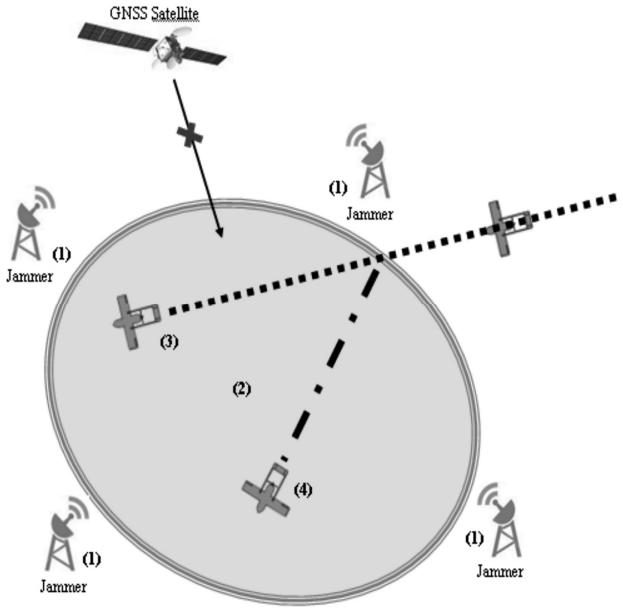

Fig. 3. Example where UAV needs a local satellite navigation system to compensate GNSS vulnerability

IV. Main Constructing Principles of Local Satellite Navigation System for GNSS Vulnerability Compensation

The research resulted in development of elements for UAS with UAV working under GNSS vulnerability or intentional suppression [Fig. 4].

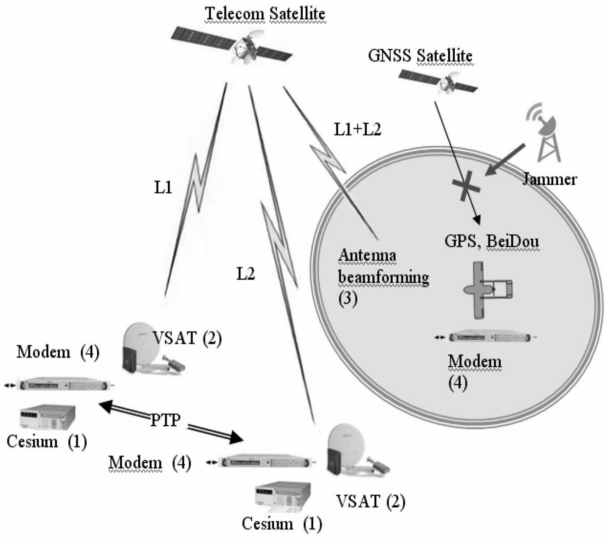

Fig. 4. Local satellite navigation system protecting autonomous UAV navigation against GNSS vulnerability

Key features of this system are:

- earth timing nodes equipped with atomic clocks (1) and VSAT (2);
- using direct point-to-point telecom satellite channel according to SCPC (single channel per carrier) topology;
- using onboard antenna units based on phased antenna array with electronic scanning ray (3) and receivers with FPGA and USRP (Universal Software Radio Peripheral) based on DSSS (Direct Sequence Spread Spectrum) modems for hardware (hybrid analog-digital codec) spread spectrum signal processing (4) [6;7;8];
- using high-precision small size atomic clocks;
- using special software for optimization of precise time synchronization of receiving and processing signals and navigation data processing.

The description of realization of the local satellite navigation system compensating GNSS vulnerability for navigation of the UAV traveling in the region of intentional GNSS signal suppression is shown in Fig. 4.

The system considers at least 2 sources of precise timing based on Cesium clocks with long-term stability of $\leq 5{,}0 \times 10^{-14}$ and traced by means of PTP 1588 v2.

The algorithm of generating a stable frequency and time source is based on pair comparison of at least three signals of roughly the same quality assessed by stability factor resulted in three "aggregate" variances as a system of three linear equations with three unknowns.

The signals are transmitted by means of the device based on special DSSS modem which transmits 1PPS signal phase using pseudo noise signal coding. The use of very long code sequences for data transmission in this system ensures security and noise immunity, which essentially complicates fast detection of the system and doesn't allow taking efficient countermeasures against it.

Fig. 5. VSAT "Epigram" with phased antenna array, in which discussed technical solutions were tested

Time stamps from both timing nodes, through the VSAT terminals with DSSS modems, are transferred according to SCPC of the corresponding telecom satellite and received by phased antenna array of DSSS modem located onboard the UAV assuring its precise traceability to UTC. Furthermore, optimum choice of anti-noise coding type and reception quality estimating methods is important for system accuracy improvement. It is known that the reception performance may be estimated for a busy channel in a wide-band satellite communication system, but it means that existing algorithms for such estimation are either made substantially more complicated, as the case of ones based in signal-noise ratio measurement, or are not applicable at all, as when test are employed. Error-correcting codes applied to correct errors also make it more complicated to estimate the reception performance and require a priori knowledge of numerous channel characteristics [9;10].

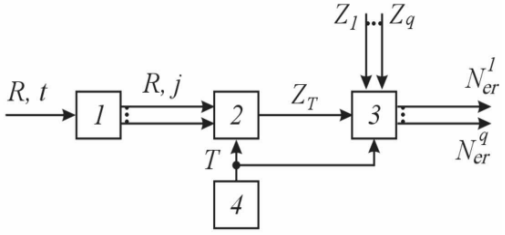

Fig. 6. Structure diagram of detector

Fig. 6 shows the structure diagram of the detector for algorithm reception performance estimation in wide-band error-correcting systems. The error codes of multiplicity K with period t pass to the decoder 1, which identifies errors having $R \geq j$, whose number Z_T during T is counted by the adder 2. When T is elapsed a signal from the synchronizer 4 passes Z_T to the comparator 3, which other inputs receive the codes for the previously calculated Z_1 - Z_q corresponding to the quality gradations N^1_{er} - N^q_{er}. Using capabilities of spread spectrum error-correcting systems ensures signal receiving secrecy and jamming resistance and essentially complicates countermeasures when signals are transmitted.

Phased antenna array with electronic scanning beam in the receiver, through using the code processing results used during signal transmission, allows identifying satellite signal for retranslation and extract needed data from it.

There's also possibility to adjust initial device operation procedure including changing of target path coordinates or other essential parameters.

V. Conclusion

Wide application of GNSS systems (GPS, BeiDou, GLONASS etc.) in a large number of critical industries suggests that their stable operation or timely redundancy in case of possible problems demands careful attention to development of different compensation scenarios for different applications. Discussed constructing principles of local satellite navigation system for GNSS vulnerability compensation can be of use in solving this important problem.

References

[1] D. Mills. The Network Time Protocol On Earth and in Space. – CRC Press, Second Edition, 2011. – 445 p.

[2] C. Audoin, B. Guinot. The Measurement of Time. – Cambrige University Press, 2001. – 397 p.

[3] Rubidium sync holdover ensures mobile service availability. White Paper. Microsemi Corporation, 2014.

[4] V. Gaidamanchuk, A. Semenko et al. Peculiarities of TWSTFT modem development for national time dissemination system // 2016 International Conference Radio Electronics & Info Communications (UkrMiCo). – 2016. – P. 1–2.

[5] J.J. Spilker. Digital Communications by Satellite. – Prentice-Hall Inc., 1977. – 592 p.

[6] Vinogradov G., Gaidamanchuk V. Microstrip Array Beam Control By Means Modification of Antenna Elements Resonance Characteristic // Proceedings of XXIV Scientific Conference "Theory and practice of antennas." – Moscow. – 1985. – Vol. 1. – P. 56–58. [in Russian].

[7] Gaidamanchuk V.A., Guziy V.I. et al. FFPA distortion compensation device with DSP on the basis of FPGA // Proceedings of 15th International Conference "Microwave Engineering and Telecommunication Technology" (CriMiCo 2005), Sevastopol, Ukraine, September 12–16 2005. – Sevastopol, 2005. – Vol. 1. – P. 154–155.

[8] Gaidamanchuk V. A., Savchuk A. V. et al. Features of Viterbi Decoder VLSI Set Designing // Proceedings of Scientific and Research Institute of Radio. – Moscow. – 1997. – P. 77–86 [in Russian].

[9] V.A. Gaidamanchuk, A.A. Palamarchuk et al. An algorithm for reception performance estimation in a wide-band error-correctiong communication system // Radioelectronics and Communications Systems. – New York: Allerton Press, Inc. – 1989. – Vol. 32. – No. 3. – P. 89–91.

[10] Gaidamanchuk V.A., Semenko A. I. et al. Spread Spectrum Signals Digital Receiver for Sattelite Communications Systems / Patent of Russian Federation № 1467787 [in Russian].

Гайдаманчук В.А., Матвієнко М.В.

Основні принципи побудови супутникової системи забезпечення інформацією PNT рухомих об'єктів в умовах вразливості GNSS

Проблематика. Системи глобальної навігації GNSS – основне джерело інформації "PNT" (позиціонування; навігація; час) для різноманітних систем у багатьох критичних застосуваннях у промисловості, наукових дослідженнях та обороні. Перебої у прийманні сигналів GNSS, чи то природні, чи то в якості умисної протидії (jamming; spoofing) стають все більшою проблемою та спонукають дослідження, спрямовані на можливість використання альтернативних GNSS джерел інформації PNT, особливо для рухомих об'єктів.

Мета досліджень. Синтез загальної схеми системи забезпечення інформацією PNT рухомих об'єктів на основі використання атомних стандартів часу, каналів CSPC системи супутникового зв'язку та VSAT станцій (з шумоподібним сигналом і ФАР з електронним скануванням) для застосування як на стаціонарних, так і на рухомих об'єктах.

Методика реалізації. Моделювання системи та дослідження можливості реалізації розроблених рішень на основі технологій FPGA та USPR для розміщення на борту рухомих об'єктів.

Результати досліджень. Моделювання та аналіз функціонування системи забезпечення інформацією PNT рухомих об'єктів на основі використання атомних стандартів часу, CSPC каналів системи супутникового зв'язку та VSAT станцій з шумоподібним сигналом та ФАР з електронним скануванням підтверджують можливість використання такого рішення для рухомих об'єктів за умови максимальної інтеграції пристроїв, призначених для встановлення на цих об'єктах.

Висновки. Широке застосування систем GNSS (GPS, BeiDou, GLONASS та ін.) в чисельних критичних галузях передбачає, що стабільна робота таких систем або їх вчасне резервування у разі можливих проблем вимагає особливої уваги до розробки різних компенсаційних сценаріїв для різних застосувань. Викладені принципи побудови локальної супутникової навігаційної системи для компенсації вразливості GNSS можуть бути застосовані для вирішення цієї важливої проблеми.

Ключові слова: вразливість GNSS; PNT;UAS; UAV; SCPC; DSSS; VSAT.

Гайдаманчук В.А., Матвиенко Н.В.

Основные принципы построения спутниковой системы обеспечения информацией PNT движущихся объектов в условиях уязвимости GNSS

Проблематика. Системы глобальной навигации GNSS являются основным источником информации “PNT” (позиционирование; навигация; время) для различных систем во многих критических применениях в промышленности, научных исследованиях и обороне. Перебои с приемом сигналов GNSS, то ли естественные, то ли в виде преднамеренного противодействия (jamming; spoofing), становятся все большей проблемой и являются причиной исследований, направленных на возможность использования альтернативных GNSS источников информации PNT, особенно для движущихся объектов.

Цель исследований. Синтез общей схемы системы обеспечения информацией PNT движущихся объектов на основе использования атомных стандартов времени, CSPC каналов системы спутниковой связи и VSAT станций (с шумоподобным сигналом и ФАР с электронным сканированием) для применения как на стационарных, так и движущихся объектах.

Методика реализации. Моделирование системы и исследование возможности реализации разработанных решений на основе технологий FPGA и USPR для размещения на борту движущихся объектов.

Результаты исследований. Моделирование и анализ функционирования системы обеспечения информацией PNT движущихся объектов на основе использования атомных стандартов времени, каналов CSPC системы спутниковой связи и VSAT станций с шумоподобным сигналом и ФАР с электронным сканированием подтверждают возможность использования подобного решения для движущихся объектов при условии максимальной интеграции устройств, предназначенных для установки на этих объектах.

Выводы. Широкое применение систем GNSS (GPS, BeiDou, GLONASS и др.) в большом количестве критических отраслей предусматривает, что стабильная работа таких систем или их своевременное резервирование в случае возможных проблем требует особенного внимания к разработке разных компенсационных сценариев для разных применений. Изложенные принципы построения локальной спутниковой навигационной системы для компенсации уязвимости GNSS могут быть использованы для решения этой важной проблемы.

Ключевые слова: уязвимость GNSS; PNT; UAS; UAV; SCPC; DSSS; VSAT.