Пропонується доповнити модель прийняття рішень про аномальні стани бездротової мережі в умовах невизначеності ще однією ознакою – місцем розташування бездротових мобільних і стаціонарних пристроїв в контрольованій мережі.

Розглянуто метод трилатерації, заснований на вимірюванні потужності сигналу в трьох точках. Цей метод має високу точність визначення місця розташування бездротового пристрою за умови побудови максимально точної моделі поширення радіохвиль. Але через особливості поширення радіохвиль усередині приміщень побудувати таку модель для них досить складно. Тому запропоновано скористатися методом радіоовідбитків. Він заснований на побудові радіокарти для кожної з трьох точок доступу, на якій вказується рівень сигналу від типового бездротового пристрою, що розміщується в певній кількості опорних точок. Також розглянуто можливість спільного використання двох методів, що дозволить визначати місцеположення бездротового пристрою навіть коли воно знаходиться за межами радіокарти.

Були проведені експериментальні дослідження, що включають в себе створення радіокарти для приміщення площею 70 м^2 з 26-ма опорними точками. Використовувалися три однакових роутера і один смартфон. В ході експерименту з'ясувалося, що в залежності від орієнтації мобільного пристрою (фактично, його антени) вимірювана потужність змінюється, тому радіокарти складалися виходячи з середньої потужності для шести різних положень мобільного пристрою. Показано, що рівень сигналу практично не залежить від положення дверей і вікон, що знаходяться в приміщенні.

Проведений аналіз принципів організації різних видів атак на бездротові мережі показав, що облік місця розташування дозволяє виявляти атаки типу «man in the middle» і «фальшива точка доступу», які в базовій моделі не виявлялися. Крім того, вдосконалена модель дозволяє визначити джерело перешкод при атаці «глушіння»

Ключові слова: потужність сигналу, трилатерація, метод радіоовідбитків, радіокарта, місцезнаходження безпровідного абонента

UDC 681.3.06:519.248.681
DOI: 10.15587/1729-4061.2019.157001

IMPROVING THE MODEL OF DECISION MAKING ABOUT ABNORMAL NETWORK STATE USING A POSITIONING SYSTEM

I. Antipov
Doctor of Technical Sciences,
Professor, Head of Department*
T. Vasilenko
Postgraduate student*
Nauky ave., 14, Kharkiv,
Ukraine, 61166
*Department of Computer
Radio Engineering and Technical
Information Security Systems
Kharkiv National University
of Radio Electronics

1. Introduction

According to data [1], as of 2018, almost half of Ukrainian organizations suffered from economic crimes and fraud over the past two years. In most cases, fraud was committed by the employees of organizations. The openness and simplicity of connecting to wireless networks that are rapidly being deployed everywhere can significantly simplify the task for attackers. The principle of wireless transmission itself makes it possible for unauthorized connections, and standard protection measures [2, 3] often do not provide adequate security.

Considering many flaws and vulnerabilities that permit malicious actions to successfully overcome information protection systems, it is a relevant task to undertake a research aimed at ensuring comprehensive security, using advanced analysis parameters to detect unauthorized access and identify the attacker.

2. Literature review and problem statement

There are many intrusion detection systems [2, 3]. However, they have several disadvantages that significantly deteriorate the quality of the wireless network. First, the determination of a clear boundary between the normal and abnormal behavior of the system leads to a large number of false signals. Second, they are not adaptive to changes in the network operation conditions. Third, these systems do not take into consideration the location of wireless users [4]. The problem of a clear boundary is solved by using fuzzy logic, and the problem of network adaptability – by taking into consideration the parameters affecting the network state (time of day, day of the week, season (vacation / not vacation), interferences). But this model does not take into consideration the location of users either. This means that part of the attacks will be skipped or detected already after the attacker has reached his goal.

In [5], the author explores the adaptability of positioning methods (recent developments provide positioning accuracy up to 1 meter [6]) in issues related to security. Using simulation modeling, the effectiveness of indoor positioning methods is proved. However, it should be noted that the studied methods are used only to provide access to networks with different security requirements. This means that the identification of the attacks themselves is carried out using classic detection systems that do not have a positioning service.

To ensure safety, it is necessary to set the measures or consider at least a few attributes. To solve this problem, authors in [7] developed a method for automating an intrusion detection system using a positioning system using the RSSI method, a received signal level estimation, and the TDoA method, a signal arrival time difference method. Despite the practical significance of research [7] for open space, they are inapplicable for premises. In addition, this paper does not show the accuracy with which the location is determined.

Consequently, more research is needed on the consideration of indoor location as one of the factors for analyzing abnormal behavior in wireless networks for intrusion detection systems.

3. The aim and objectives of the study

The aim of this study is to improve the decision-making model of the abnormal state of the wireless network [4] by applying a positioning system for subscribers of the wireless network, which will help reduce the number of non-detectable attacks.

To achieve this goal, it is necessary to solve the following tasks:

– to select a method for determining the location of the subscriber in the network;

– to experimentally determine the error of finding the location of the subscriber in the protected space;

– to clarify the model of making decisions about the abnormal state of the wireless network, taking consideration the location of the subscriber, based on the selected method.

4. Materials and methods for determining the location of wireless devices

Positioning systems can be classified by the parameters that are used to calculate the coordinates of devices that emit a radio signal. There are three basic measurement methods:

– based on the angle of signal arrival (AoA – Angle of Arrival) [8, 9];

– based on the time of arrival of the signal (ToA – Time of Arrival and TD-A Time Difference of Arrival) [9–11];

– based on the power level of the received signal (RSSI – Received Signal Strength Indicator) [12, 13].

Comparative characteristics of these methods are given in Table 1.

Table 1

Comparative characteristics of measurement methods

Method	Accuracy	Advantages	Limitations	Applications
AoA	The accuracy is affected by the reflection and shading of the signal	Potentially high positioning accuracy in open space	Low positioning accuracy due to multipath signal reflections in the room, requiring a rotary antenna or antenna system	Zones with low numbers of overlaps and barriers to signal
ToA	up to 6 meters	Three-dimensional positioning capability	Requiring an accurate clock synchronization	In open space
TDoA	up to 6 meters	Requiring no clock synchronization	High cost of sensors, requiring an additional equipment	In open space
RSSI	up to 1 meter	High accuracy, no extra cost	Requiring a radio propagation model	In closed space

For further research, we chose the RSSI method. The choice is based on the fact that these mechanisms do not require large financial expenditures and, in comparison with others, show high positioning results. This method is not among the "classic" positioning methods, but for a Wi-Fi network deployed in a limited area, it turns out to be the simplest and most effective.

To determine the coordinates of wireless devices, the base method is the trilateration [13] (position determination based on estimating distances from three or more objects with known coordinates). From the geometrical point of view, the trilateration task is to find the coordinates of the intersection point of three circles, as shown in Fig. 1.

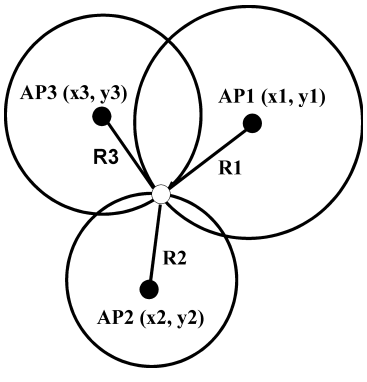

Fig. 1. Geometric circular trilateration approach for free space

To implement this method, it is necessary to simulate the propagation of the signal inside the building. The most commonly used model is COST231 and the ITUR P1238 statistical model *recommended* by the International Telecommunication Union [14]. Radio signal propagation of a wireless Wi-Fi network inside a building is a complex interference pattern that is formed as a result of the joint action of the mechanisms of multipath radio waves, reflection, refraction, diffraction and diffusion. Multiple reflections lead to a decrease in field strength in some places of the room and an increase in others. In some cases, this can also lead to so-called fading ("dead zones"), in which the arrival of a signal is very difficult. As a result, a completely accurate radio wave distribution model is virtually impossible to build, which will affect the accuracy of positioning.

An alternative to mathematical algorithms for signal propagation is the fingerprinting method [15]. It is based on building a radio map indoors and has two stages of implementation. The first stage involves the collection of information about the RSSI of a set of reference points from base stations (at least three) and the formation of a database of storage of these points, as well as a floor plan. Power from available Wi-Fi access points should be tied to the local or global coordinates of the room. The second stage is to continuously monitor the users' equipment RSSI and compare them with the existing database, in order to find matches or the nearest value.

This method provides high accuracy of positioning, provided the radio map is up to date.

5. Experimental research to determine the error of finding the location of the subscriber in the protected area

For an example of the implementation of the radio indentation method, we consider a three-room apartment of a panel house with an area of 70 m^2 with three access points (AP1, AP2, AP3), a plan for placing and placing access points is shown in Fig. 2. Also reference points on the plan at which the results of the signal level measurements were made.

Access points are located around the periphery of the coverage area, at different levels, which provides good data about devices that would otherwise look equidistant from all other access points. We made a radio survey of the premises in order to allocate channels and adjust the power in the range of access points.

Based on the obtained data, we can conclude that the three access points are sufficient for an area of up to 100 m^2. In the case of using more points, the equipment will prevent with each other's work (which is due to the feature of Wi-Fi technology), and the use of a smaller number will lead to a decrease in positioning accuracy.

For the experiment, we used three identical Asus RT-N10E Wireless N Routers with the following technical parameters: operating frequency – 2.412 GHz; antenna gain – 2 dBi; transmitter power is 19 dBm. The smartphone Lenovo S898t+. During the experiment, it turned out that, depending on the orientation of the mobile device (in fact, its antennas), the measured power varies, therefore the radio maps were compiled based on the average power at a height of 1 meter, for 60 seconds for six different positions of the mobile device (vertical position and down; horizontally – 0°, 90°, 180°, 270°), for 10 seconds in each of them. The results of the experiment are given in Table 2.

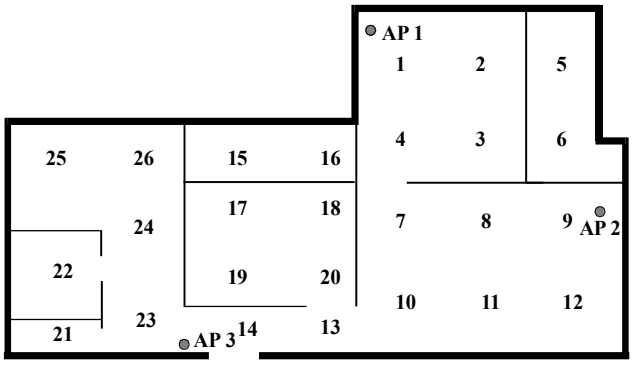

Fig. 2. Plan of the room with the placement of reference points and access points

In Fig. 3 a graphical representation of experimental measurements of the propagation of a Wi-Fi signal, which proves the placement of wireless equipment. Signal levels at the same reference point are significantly different from the three access points.

Table 2

Results of experimental RSSI measurements

Point No.	AP1, average level of RSSI, dBm		AP2, average level of RSSI, dBm		AP3, average level of RSSI, dBm	
	windows / doors are closed	windows / doors are opened	windows / doors are closed	windows / doors are opened	windows / doors are closed	windows / doors are opened
1	–36.9	–36.1	–60.3	–62.1	–71.5	–69.0
2	–43.0	–44.0	–61.0	–62.4	–68.4	–67.4
3	–42.0	–43.7	–65.7	–64.1	–72.4	–72.5
4	–43.0	–44.6	–61.4	–58.0	–64.5	–64.9
5	–53.5	–52.2	–65.8	–65.1	–76.0	–75.0
6	–49.2	–48.6	–59.3	–58.4	–79.1	–74.9
7	–54.0	–53.4	–54.7	–54.4	–59.5	–57.4
8	–58.0	–59.4	–47.4	–46.3	–58.4	–48.7
9	–69.8	–67.8	–36.8	–35.3	–57.0	–54.5
10	–61.0	–59.0	–52.0	–53.6	–53.4	–43.1
11	–63.0	–64.2	–44.7	–43.0	–52.2	–51.8
12	–59.2	–61.1	–41.5	–39.6	–45.1	–52.3
13	–68.2	–66.3	–59.2	–58.1	–37.7	–40.4
14	–78.4	–77.5	–65.6	–64.2	–38.8	–37.5
15	–67.4	–68.9	–75.9	–76.0	–60.3	–63.3
16	–59.9	–60.1	–76.2	–77.9	–62.5	–63.7
17	–66.4	–66.5	–69.7	–69.0	–56.5	–56.2
18	–68.2	–66.7	–68.5	–67.2	–59.3	–62.6
19	–74.0	–73.0	–62.7	–63.1	–55.8	–53.2
20	–70.2	–69.8	–60.8	–60.6	–51.4	–52.5
21	–81.8	–78.3	–75.9	–74.4	–42.1	–41.7
22	–78.2	–78.4	–73.6	–74.0	–49.2	–46.7
23	–78.4	–81.1	–69.4	–68.6	–40.8	–38.5
24	–75.2	–73.5	–73.1	–74.1	–56.0	–56.2
25	–78.9	–79.9	–74.7	–77.0	–61.9	–60.6
26	–75.8	–76.3	–78.0	–76.3	–61.0	–60.6

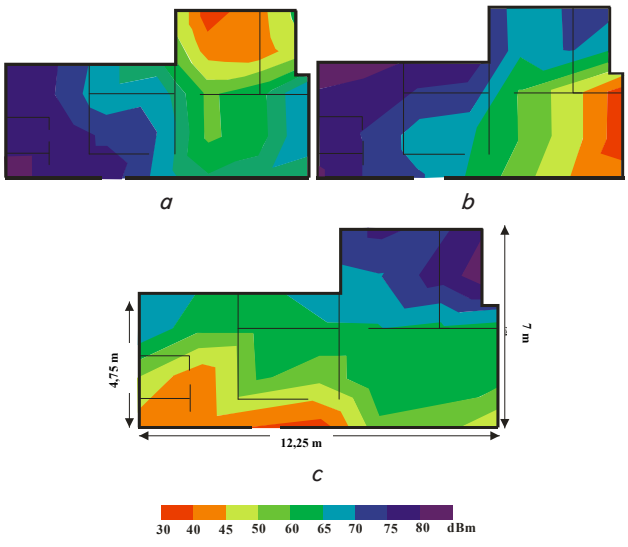

Fig. 3. Map of signal propagation:
a — TD1; *b* — TD2; *c* — TD3

Based on data from Table 2, we can conclude that the signal level is essentially independent of the position of the doors and windows in the room (the error is 1–2 dBm). In the process of forming a radio map in different positions, the results differed from 3 dBm to 10 dBm. The maximum deviation is fixed only at five points, in the other reference points the difference in measured signal levels did not exceed 5 dBm. As can be seen from Fig. 4, the error in determining the power of 5 dBm is equivalent to the error in determining the location of 2.5 m when using the deterministic (Euclidean distance) approach to determine the coordinates. The accuracy of determining a positioning object using a radio map is comparable to market positioning systems. To increase the accuracy of the results, the number of reference points can be increased by fixing them through each meter and determining the coordinates using other methods of intellectual analysis.

6. Clarification of the model for making decisions about the abnormal state of the network, based on the location of the wireless subscribe

Decisions about the abnormal state of the network consists of several stages [4]. At the first stage, quantitative estimates of parameters (actual data transfer rate, number of subscribers, signal level, average packet length) are converted to fuzzy logic values by comparing them with typical parameters. The parameters are then converted to fuzzy logic values using estimated scales and linguistic variables. Depending on the time of day, typical parameters, the curve by which the degree of abnormal state of the network is estimated changes its appearance. At the last stage, a comprehensive assessment of all parameters is carried out, taking consideration the weighting, the level of interference and the database of previous incursions. This system can work both in automatic mode (it makes the decision itself) and with the help of an operator (the expert, after analyzing the results, depending on the situation, makes the decision himself).

The algorithm for making decisions about the abnormal state of the network, supplemented by a attribute of the subscriber's location, is shown in Fig. 4.

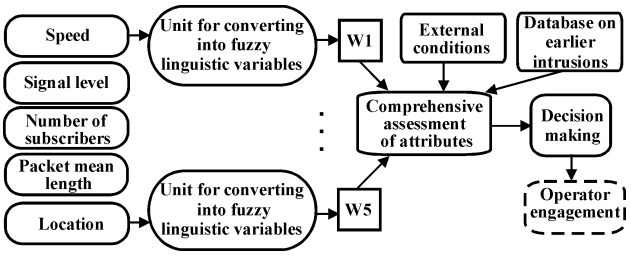

Fig. 4. Algorithm for making decisions about the abnormal state of the wireless network based on location:
W — weighting factor of each of the attributes

The availability of a positioning service in the implementation of wireless network security will solve the following problems.

1. Identification of abnormal states. Combined with other features of a wireless network, it will identify abnormal states of a wireless network. For example, an employee in the protected area uses atypical traffic, and the speed of data exchange is significantly reduced, this causes suspicion to this subscriber and requires further monitoring. By adding an atypical location, you can most likely talk about unauthorized actions on his part.

2. Access control. Positioning will allow to limit connections to the network only within the physical perimeter, blocking attempts to connect from areas outside the physical perimeter, even if a completely legal client is connected.

3. Control of stationary equipment. Provides complete control of stationary wireless equipment (computers, cameras, printers, etc.). Changing the location of stationary devices indicates illegal actions (for example, theft).

4. Locating the source of unauthorized actions. The decision-making model of the abnormal state of a wireless network with fuzzy logic elements [4] allows detecting suspicious activity or blocking a possible attack, however, like any other intrusion detection system. For organizations with commercial secrecy, this is not always enough. To minimize the risk of leakage of confidential information, the positioning service allows you to quickly identify the source of unauthorized actions and take appropriate actions, restarting the normal operation of the wireless network.

5. Determining the location of the source of unauthorized actions outside the physical perimeter of the protected area. If the signal of the wireless device is received only by one or two access points, then it will be appropriate to use the trilateration method.

A comparative characteristic of the ability to detect attacks of a model with and without positioning is given in Table 3.

The analysis of the principles of organizing various types of attacks on wireless networks showed that location accounting allows detecting "man-in-the-middle" and "false access point" attacks that were not detected in the base model. Implementing these attacks using equipment, whose coordinates are radically different from the legal ones. In addition, an improved model allows to determine the source of interference in the attack "jamming".

Thus, an improved model for making decisions about the abnormal state of a wireless network, supplemented by a positioning function, is capable of detecting more attacks on wireless networks than without a position detection function.

Table 3

Comparative characteristics of the ability to detect attacks and their sources with and without positioning

Name of attack	Essence of the attack	Detection of the invasion fact		Detection of the source	
		Out of pos.	With pos.	Out of pos.	With pos.
Muting	Radio noise generation, at the frequency of the wireless network, suppressing it in whole or partly	+	+	–	+
«man in the middle»	An attacker gets into the communication channel between the router and the victim's computer and listens to them, appearing to be a different side for each interlocutor	–	+	–	+
False access point	Legal access point is blocked to redirect clients to their access point	–	+	–	+

7. Discussion of the experiment results and refinement of the decision-making model about the abnormal state of the wireless network taking into consideration a subscriber's location

The results of experimental measurements RSSI presented in Table 2, and the constructed signal propagation maps shown in Fig. 3, constructed by the method of radio prints, indicate the applicability of this method for indoor positioning. The data Table 2 confirms that the three access points for the room under study are sufficient to position the wireless devices, since the RSSI levels at the same point from three different sources are quite different. Therefore, using prepositional methods, it is possible to obtain positioning accuracy of 2.5 m. at low cost.

The improved model of making decisions about the abnormal state of a wireless network based on the subscriber's location, based on the chosen method, will qualitatively complement the existing security model, reducing the risks of unsanctioned actions among staff. A similar technique is presented in [7], but unlike the TDoA method proposed by the authors, the radio impression method does not require the installation of additional equipment and the purchase of expensive sensors, and provides positioning accuracy more than two times higher.

It is worth noting that this method of positioning is valid only for classic devices that do not use directional antennas for their purposes. To protect against such attacks, you must also use directional antennas at each access point.

Further research is feasible to develop in the direction of increasing the accuracy of positioning by applying additional mechanisms for analyzing the results of the radio map. Also considered methods are applicable for identifying the location of objects with previously unknown technical characteristics, which will help to increase the level of security in combination with other protection measures.

8. Conclusions

1. To determine the location of the wireless network subscriber, the RSSI method was selected using the radio prints method. These methods determine the location of users with an accuracy of 2.5 meters in indoor conditions, as they take into consideration the conditions of propagation of radio waves.

2. It was experimentally shown that the error in determining the location is 2.5 m when using the deterministic (Euclidean distance) approach to determining the coordinates. This allows you to argue about the effectiveness of the selected methods and will avoid additional financial expenditure for expensive equipment.

3. The model for making decisions about the wireless network abnormal state has been clarified in the form of accounting for an additional feature, the location of the wireless network subscriber. Due to this addition, based on the nature and principles of organizing various types of attacks on wireless networks, it becomes possible to detect "man-in-the-middle" and "false access point" attacks that were not detected in the basic model. A decrease in the number of undetected attacks indicates an increase in the effectiveness of this model.

References

1. Vsesvitnie doslidzhennia ekonomichnykh zlochyniv ta shakhraistva 2018 roku: rezultaty opytuvannia ukrainskykh orhanizatsiyi // PwC. URL: https://www.pwc.com/ua/uk/survey/2018/pwc-gecs-2018-ukr.pdf
2. Kotov V. D., Vasil'ev V. I. Current state of network intrusion detection // Vestnik Ufimskogo gosudarstvennogo aviacionnogo tekhnicheskogo universiteta. 2012. Vol. 16, Issue 3 (48). P. 198–204.
3. Los' A. B., Danielyan Yu. Yu. Sravnitel'nyy analiz sistem obnaruzheniya vtorzheniy, predstavlennyh na otechestvennom rynke // Vestnik Moskovskogo finansovo-yuridicheskogo universiteta. 2014. Issue 3. P. 181–187.
4. Antipov I. E., Yashchenko T. A., Nasif N. T. Primenenie nechetkoy logiki dlya povysheniya bezopasnosti besprovodnyh setey na baze tekhnologii Wi-Fi // Radiotekhnika. 2011. Issue 165. P. 103–106.
5. Markin D. O. Issledovanie effektivnosti algoritmov opredeleniya mestopolozheniya mobil'nyh ustroystv vnutri pomeshcheniya // Vestnik RGRTU. 2015. Issue 54. P. 32–39.
6. The Cisco Hyperlocation Module: Best of Interop Awards Finalist // Cisco Blogs. URL: https://blogs.cisco.com/wireless/the-cisco-hyperlocation-module-best-of-interop-awards-finalist
7. Yurkin D. V., Nikitin V. N. Intrusion detection systems in IEEE 802.11 local wireless networks // Informacionno-upravlyayushchie sistemy. 2014. Issue 2. P. 44–49.
8. Niculescu D., Nath B. Ad hoc positioning system (APS) using AOA // IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428). 2003. doi: https://doi.org/10.1109/infcom.2003.1209196

9. Teoreticheskie osnovy radiolokacii / Shirman Ya. D., Golikov V. N., Busygin I. N., Kostin G. A., Manzhos V. N., Minervin N. N. et. al. Moscow: Sovetskoe radio, 1970. 560 p.
10. PinPoint: An asynchronous time-based location determination system / Youssef M., Youssef A., Rieger C., Shankar U., Agrawala A. // Proceedings of the 4th international conference on Mobile systems, applications and services – MobiSys 2006. 2006. P. 165–176. doi: https://doi.org/10.1145/1134680.1134698
11. Cong L., Zhuang W. Hybrid TDOA/AOA mobile user location for wideband CDMA cellular systems // IEEE Transactions on Wireless Communications. 2002. Vol. 1, Issue 3. P. 439–447. doi: https://doi.org/10.1109/twc.2002.800542
12. Bargshady N., Garza G., Pahlavan K. Precise Tracking of Things via Hybrid 3-D Fingerprint Database and Kernel Method Particle Filter // IEEE Sensors Journal. 2016. Vol. 16, Issue 24. P. 8963–8971. doi: https://doi.org/10.1109/jsen.2016.2616758
13. Atia M. M., Noureldin A., Korenberg M. J. Dynamic Propagation Modeling for Mobile Users' Position and Heading Estimation in Wireless Local Area Networks // IEEE Wireless Communications Letters. 2012. Vol. 1, Issue 2. P. 101–104. doi: https://doi.org/10.1109/wcl.2012.020612.110279
14. ITU-R P.1238-9 – Propagation data and prediction methods for the planning of indoor radio communication systems and the radio local area networks in the frequency range 300 MHz to 100 GHz. Geneva: ITU-R Recommendations, 2017.
15. Zymbler M. L., Miniakhmetov R. M., Rogov A. A. The survey of indoor positioning algorithms for mobile devices // Bulletin of the South Ural State University. Series «Computational Mathematics and Software Engineering». 2013. Vol. 2, Issue 2. P. 83–96. doi: https://doi.org/10.14529/cmse130207

Обговорюються основні тенденції використання електрогідравлічних актуаторів, вимоги до параметрів. Обґрунтовано необхідність використання автоматичних методів тестування електрогідравлічного актуатору спільно зі штатною апаратною частиною електронного блоку управління. Методики випробувань контуру управління електрогідравлічного актуатору, викладені в даній роботі, дозволяють виключити ефекти взаємного накладення (впливу) динамічний і статичних характеристик приводу і апаратної частини електронного блоку управління. Були запропоновані методики автоматичної ідентифікації моделі актуатору і методики автоматичного визначення основних параметрів і характеристик актуатору: зміщення нуля, зони нечутливості, амплітудно-частотної, фазо-частотної і швидкісний характеристик. При впровадженні запропонований методик була вирішена проблема обробки швидкісних характеристик приводу, які мають сильну зашумленість, пов'язану з імпульсним характером похідною дискретного сигналу положення актуатору (12 біт). З метою виключення внесення похибки в форму сигналу, крім стандартних методів фільтрації з використанням цифрових фільтрів, було запропоновано проводити апроксимацію зашумленої характеристики актуатору Кривою Безьє. Була запропонована методика, що дозволяє реєструвати гістерезис швидкісної характеристики, за рахунок циклу безперервного зміни швидкості переміщення вихідної ланки актуатору за робочий хід. Методика автоматичної ідентифікації спрощеної моделі актуатора дозволяє значно знизити трудоємкість під час обробки експериментальних даних. Параметри моделі актуатора, знайдені для різних відхилень по параметрам і різних умов роботи актуатору (зовнішніх діючих факторів), дозволяють покращити якість синтезу систем керування

Ключові слова: електрогідравлічний актуатор, швидкісна характеристика, зона нечутливості, амплітудно-частотна характеристика, фазо-частотна характеристика

UDC 629.735

DOI: 10.15587/1729-4061.2019.154837

DEVELOPMENT OF PROCEDURES FOR DETERMINING THE PARAMETERS OF AN AIRCRAFT SERVO ACTUATOR

E. Kononykhin
Head of Research Department
PrJSC FED
Symska str., 132, Kharkiv,
Ukraine, 61000
E-mail: ekononykhin@icloud.com

1. Introduction

Electrohydraulic servo actuators (EHSA) are most widely used in systems of automatic control of aircraft engines for moving mechanization elements and in flight control systems for controlling steering surfaces [1, 2]. Liquid taken from a high-pressure fuel pump in automatic control systems of aircraft engines (ACS AE) or from hydraulic pumps of the flight control systems is the working fluid for an electro-hydraulic actuator. Upon electrical commands, electrohydraulic amplifier (EHA) which is a part of the actuator converts low-power control signals into proportional hydraulic commands of considerable power. Upon distribution, working fluid enters hydraulic cylinder (to servo piston) and forms mechanical command.