ADVANCES IN CYBER-PHYSICAL SYSTEMS

Vol. 2, No. 2, 2017

INVARIANTS OF NOISE IN CYBER-PHYSICAL SYSTEMS COMPONENTS

Elena Nyemkova
Lviv Polytechnic National University, 12, S. Bandera str., Lviv, 79013, Ukraine
Author's e-mail: cyberlbi12@gmail.com

Submitted on 13.11.2017

Abstract: **The article is devoted to the invariant of internal electrical noise of electronic devices, which are components of cyber-physical systems. Time series of noise signals show chaotic behavior. Invariants are based on the autocorrelation function of dynamic time series. Insignificant differences on the micro-level devices lead to changes in the dynamics of time series. It is shown that the form of the autocorrelation function is unchanged for each electronic device of the cyber-physical system. The dynamic authentication algorithm has been developed, which consists of choosing a range of time series, defining and calculating invariants, making decisions about authentication. The result of the operation of the algorithm can be transferred to the executive mechanism, depending on the practical problems in cyber-physical systems. Also for the pseudorandom sequence of the embedded program generator, the following values are predicted on the basis of invariants. Estimated errors are calculated.**

Index Terms: **autocorrelation function, dynamic authentication, cyber-physical systems, chaotic time series, internal electrical noise signals.**

I. INTRODUCTION

Commercialization of such technologies as Internet of things, SCADA and others led to a sharp decline in the information security of cyber-physical systems. A huge number of structural elements, such as sensors of physical quantities and controllers were involved into computer networks, but the security of information exchange of these elements is very low, in some cases there is no protection against penetration into the system at the level of structural elements. A low level of security leads to the possibility of conducting cyber-attacks, where the targets can be either directly specific cyber-physical systems, or remote servers that are not related to particular systems, but related to specific cyber-physical systems through telecommunications. The inclusion in the interconnecting protocols of logical names of devices does not solve the problem of information security; logical names can be substituted by various attack technologies.

Modern networks and computer systems are exposed to several thousands of different attacks every day. A significant part of the attacks is due to an access violation when the attacker becomes a legitimate user. This is made possible by weak authentication attributes of legal entity. Biometrics techniques were developed for the admission of people. It is also necessary for electronic devices to develop similar techniques that would make it possible to uniquely identify a particular device in a critical facility management system, the Internet of Things, telemedicine, etc.

The purpose of this study is to show the possibility of natural noise usage of electronic devices for solving problems of the identification and authentication of devices in cyberspace. This requires choosing the noise parameter which does not depend on a particular time series, but only on the physical characteristics of the electronic device.

The challenge is to develop methods of recognition, which would provide unambiguous information on the specific unique device. Many researchers have come to the conclusion that such information may be inherent noise signals [1].

Any electronic device consists of a set of elements that are different in the parameters within limit variations. Nobody can make exactly the same elements at the micro-level, so that these differences are manifested in deviations of parameters at the macro level of devices: linear gain tract characteristics, resonant frequencies, noise ratio and others.

The authentication process of the electronic device is determined by measuring a parameter. Thus, impulse noise is used to identify the chip by implementing physical unclonable function [2].

Authentication accuracy is determined by quality measure which depends on the technical equipment, measurement methodology and the selected identifier. Therefore, comprehensive approach is needed to meet the challenges of authentication of electronic devices.

Uncontrolled changes in signals occur during the operation of electronic devices due to fluctuations in internal electromagnetic fields. Fluctuations can spread along cables or wires or by radiation in the form of electromagnetic waves. As a result, interference appears, they are undesirable for the normal operation of the device. There are many causes of interference. A sudden change in current or voltage is the main reason. A complex interference pattern of electromagnetic fields arises inside the electronic device connected to the power source; it is caused by the mutual influence of the components of the device. As a result, parasitic signals appear in the output circuit of the electronic device.

When designing devices, developers try to minimize these parasitic signals, but reducing their level to zero is impossible [3].

Parameters of parasitic signals (for example: phase, amplitude, frequency, dynamic spectrum) are determined by these internal electromagnetic fields, which in turn depend on the element base and design features of the device. Complete identity of devices cannot be provided because of the natural spread of parameters at the micro level even with the same selection of elements and their internal arrangement. The interaction of electromagnetic fields in the middle of the device depends on the values of the resonant frequencies of the device, which are the consequence of processes in circuits with distributed parameters. At the output of the device, signals will be present, which have fallen into the region of resonant frequencies. The signals at the output will vary for different devices of the same type, in other words, the parasitic signals at the output are individually similar to the individual biometric indicators of different people. Therefore, you can try to use them to identify electronic devices. Parasitic signals due to their minimization are very small, as a rule, it is about the noise at the output of the device.

Talking about identification, it is necessary to determine the characteristics for identification. Noise signals are characterized by a level and a spectrum. In measuring practice, the concept of the noise coefficient is used – measuring the ratio of the output signal to the signal at the input. This is an integral parameter and it is not suitable for the identification indicator. It is necessary to find processes that could unambiguously characterize the features of this device. The appearance of parasitic signals at the output is associated with the internal structure of the device, and it becomes possible to determine the identification feature (identifier) with an appropriate choice of the parasitic signal parameter.

In Chumachenko's work, the task of recognizing electronic devices (digital microphones) was partially solved by using frequency analysis with the construction of spectrograms (creating a spectral image of the device) [4]. Such techniques were investigated as identification by a set of stationary components present in the signal, identification based on feature vectors, which are subsequently identified using artificial neural networks, and identification based on mixed Gaussian models. All the techniques are based on the assumption that two groups of features can be distinguished for which devices can be identified. There are signs of hardware and signs of post processing algorithms – equalization, echo cancellation, adaptive filtering, etc. The techniques use a fast Fourier transform to identify stationary components and their harmonics.

In this method, the use of spectral characteristics can give false results for a random distribution characteristic of noise. As our investigations have shown, the noise spectrum is essentially unsteady. In addition, it takes a lot of time and computing resources to calculate the noise spectrum.

Fractal analysis of traces of digital signal processing is applied [5]. The software "Fractal" is designed for identification and diagnostic studies of phonograms and digital sound recording devices, the methodology for carrying out such studies has also been developed. The recording of a phonogram is characterized by the influence of the noise of the recording device, therefore, in case of rewriting or recording on other equipment, the phonograms own noises have other characteristics. This makes it possible to identify the compilation of an audio file.

The possibility of using the Hearst coefficient of the noise signal was investigated for identification purposes [6].

The method for identifying computers on the network is proposed using the phase portraits of Fourier components of the noise of integrated audio cards [7]. Identification of the audio device is carried out by constructing phase portraits of different Fourier components (Fig. 1) and calculating their parameters, namely the displacement of the centers of the strange Fourier component attractors relative to the origin, (Fig. 2).

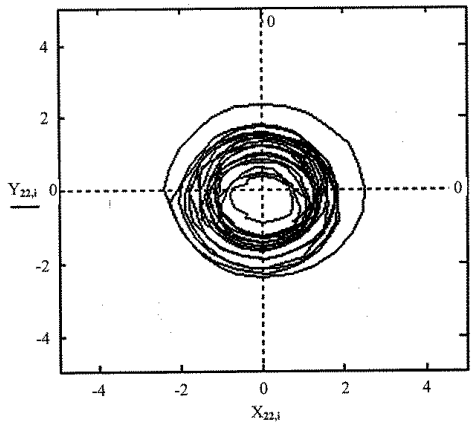

Fig. 1. The phase portrait for the low-frequency Fourier component (500 samples, n = 22)

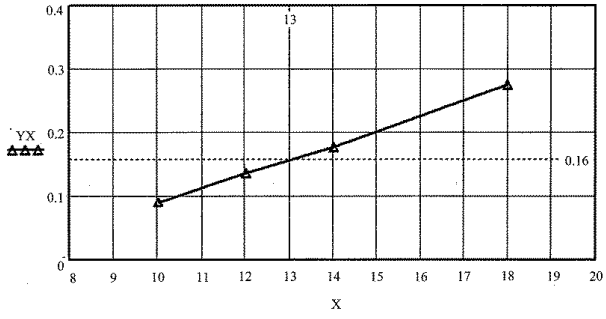

Fig. 2. Relative displacement of the center of the boundary cycle as a function of the low frequency of the model. The low frequency is plotted along the horizontal axis. The center offset is vertical (Normalized by diameter)

Authentication occurs by comparing the position of the centers of the attractors with respect to the origin.

The attractor is the trajectory of the system in the phase space, which does not deviate from the stability points and which is responsible for the oscillatory processes in the system with dissipation. The points of stability determine the set of natural frequencies of the system, which, in turn, are individual for a specific electronic device. For these measurements, the attractor had the form of a set of limit cycles. The displacement of the centers of attractors is used in the work as an authentication feature.

II. TECHNIQUES IDENTIFICATION OF COMPLEX SYSTEMS

The problems of identifying complex systems, not just components of cyber-physical systems, must be solved at the system level. These problems attract the stable interest of researchers. In [8] we can see bibliography of the issue, many methods and models of identification and their classification. The two main tasks are solved in the study of complex systems. The first task is the identification of the system. Identification of the system means finding certain invariant characteristics. The second task is the prediction of the behavior of the system. Often the first task precedes the second, because the mathematical prediction is based on the basic properties of a complex system, such as the dimension of the embedding, the correlation entropy, as shown in [9]. Usually, complex systems are non-linear systems with dissipation, in which the development of chaotic processes is possible.

Active and passive methods for the identification of complex systems are currently used. An external signal is applied to the system and its response is examined at an active approach. The study of the response can be carried out on the basis of a mathematical model of a complex system or with the help of neural networks, as shown in [10]. Patra and Kot improved the method significantly [11]. But this method requires a large amount of calculations, a lot of time and many examples for training.

Today it has become known a growing number of relatively simple examples of spontaneous appearance of temporary structures in disordered systems [12]. It is a testament to the self-organization processes in irreversible processes. For electronic devices the presence of self-oscillatory systems is characteristic. Spontaneous pattern formation takes place in trigger-type systems [13]. A limit cycle is characterized by constant amplitude. The trajectory describes the stationary harmonic oscillations. Nonlinear oscillator model is used in the research of noise in radio frequency integrated circuits [14].

The passive method is based on the analysis of the system's own signals. This is actually in those cases when the process under study is almost impossible to describe mathematically. Supposing the observed variable, a series of N numbers, is present. These are the values of some measured dynamic variable $x(t)$ with a constant step τ in time, $t_i = t_0+(i-1)\tau$: $x_i=x(t_i)$, $i=1,...,N$. The main requirement for identification is the following. The invariant characteristics of the initial system and those obtained from the time series must coincide. These characteristics can be determined from the experiment without knowing all the dynamic variables of the system.

Sometimes, to identify complex systems, researchers use the calculated spectrum of a dynamic variable [15]. At the same time, the danger of aliasing is with uniform sampling. For signals in telecommunication systems, the process of digitizing an analog signal is preceded by filtration, and the aliasing effect disappears. In some practical cases, the dynamic variable is represented only as a discrete series, filtration is impossible in principle. The use of non-uniform sampling is also impossible. Therefore, the identification of such systems by means of the spectrum has a fundamentally unrecoverable error. In this case, in order to obtain an adequate result, one must be sure that the spectrum of the investigated signal is limited by the frequency from above, and the sampling rate satisfies Kotelnikov's theorem. The identification of specific complex system is provided by means of the autocorrelation function in [16, 17].

Identification should be based not on the logical name of the system, but on the essence of the processes occurring in the system itself. Since each system is unique at the microscopic level, the dynamic variable $x(t)$ will have a unique trajectory. If it is possible to find invariant characteristics for each complex system based on the sequence $x(t)$ (passive methods for the identification), then this is a solution to the problem of identifying the system without constructing mathematical models of this system. For example, the identification of a person by his signature is performed by calculating the characteristic features (invariant) in writing letters. A person can be uniquely identified, despite the visual difference of many of his signatures made at different times.

There are deep analogies in the organization and functioning of complex systems, despite the fact that they can differ significantly in specific manifestations and details. Most real systems are dissipative with chaotic dynamics. As it is shown in [18], reconstruction of attractors is possible. It should be noted that most complex systems are characterized by flicker noise. Dynamic variable shows the properties of flicker noise. This property is inherent in natural systems [19].

The identification of complex systems is necessary to obtain access rights to confidential information or a control system for the tasks of the Internet of things. The main requirements for such identification are as follows. Firstly, among the many such systems, it is necessary to identify the one that has access rights. Secondly, identification should be carried out in real time, i.e. for a very short time. Thirdly, the identification procedure should not require many calculations. The second and third conditions limit the volume of mathematical operations with the time series of the dynamic variable $x(t)$. Now identification of devices in telecommu-

nications networks is carried out using logical names or cryptographic protocols. Evaluation of parameters of mathematical models of technical devices takes a long time and involves the participation of a man; this problem is well-known [20].

The task of this study is to find the invariant characteristic of complex system on the basis of the time series data $x(t_i)$ without carrying out external influences on the complex system and without computing the spectral characteristics. The solution must assume full automation.

A stochastic process is called stationary, if its basic properties are unchanged in time. The stationary process (stationary series) is characterized by the following four properties:

1) The mathematical expectation E of a stationary series is a constant.

2) The variance of the stationary series D is a constant quantity.

3) The autocovariance of the stationary series R is a constant; it depends only on the lag value l.

4) The autocorrelation coefficient ρ_l of a stationary series with lag l depends only on the lag value l.

If these four properties are satisfied, then the process is stationary.

Considering a few almost identical complex stationary systems, which do not significantly differ in their components. The temporal realization of the series of dynamic variables $x_j(t_i)$ of each system j will be different. It can be expected that the values of the autocorrelation and autocovariance coefficient for a given lag l will be slightly different for another systems. Each system will demonstrate the constancy of the autocorrelation function of the time series, regardless of the count start (under the assumption that the system is closed, i.e. the influence of external factors on the system is negligible). Thus, each virtually identical complex system can be characterized by its autocorrelation function. The autocorrelation function can be taken as a template – an identifier for a complex system.

In practice, the time series of the dynamic variable of a stationary system is noise-like. Slow trend for the dynamic variable $x_i(t_i)$ will lead to that condition 1 and 2 will not be executed. If the systems demonstrate quasi-stationary behavior, then the feasibility of conditions 3 and 4 will depend on how much the mathematical expectation of the series deviates from the original value at the length of the autocorrelation function definition.

All assumptions made about the behavior of systems should be tested experimentally for each type of complex systems that require identification. The graph of the autocorrelation function of the time series is a discrete set of points. If we connect these points by direct lines, we obtain a broken line. For each complex system there will be calculated its own broken line. The identification of a complex system among many other similar ones comes to finding one among the set of broken lines (autocorrelation functions) that corresponds to this system.

Research methodology

Due to the low level of the noise signal, it was necessary to develop a technique for processing the output signal of an electronic device, which would enable us to detect differences between different devices, i.e. determine the authenticator. For this purpose, autocorrelation functions are calculated based on the oscillograms of the output signal. They represent a discrete sequence of values of a_n (where n is the autocorrelation function reference number) for N equidistant samples taken at the sampling frequency.

The noise signal from the audioplate's amplifier was digitized by the ADC and recorded in the memory buffer, then the results of the digitization were rewritten in the file using the Oscillometr software (Shmelev), which allows measuring signals at a level of 10 μV. The noise signal to the input of the ADC is recorded in a file with the extension wav. This software oscilloscope allows you to change the sampling frequency from 2 kHz to 400 kHz. In this case, it is possible to observe visually on the monitor screen the spectrum of the signal and its variation in time.

Measurements of the noise signal of computer's audioplate were carried out according to the technique [6]. The sampling frequency at digitization of the noise signal was 44.1 kHz. A total of 20 computers were examined from computer classes of NULP. On each computer, several measurements were taken at different time intervals from a few seconds to several tens of days. The duration of each file was up to 10 seconds. The number of samples in the file for each channel (right and left channels) was up to 440 thousand. The steady-state processes occurred in each record for the first 1500 counts. In further calculations, the stable mode exit section was excluded, the 1000-sample recording sections were analyzed, these sections were taken from different parts of the recording file and for them, and the autocorrelation functions were calculated for the analysis. All calculations, plotting and writing programs carried out in Mathcad. Function *lkorr* was used to calculate the autocorrelation function; the function *lkorr* produces centering process on the mean value and the estimated variance normalization.

The results of the experiment show that the plot form of the autocorrelation function of the audio plate's noise signal for each particular computer does not change, whereas for different computers the plot form differs significantly (Fig. 3). Autocorrelation function value for the zero offset equal to one. The peculiarity of the behavior of the autocorrelation function (the shape of the broken line formed from the values of the autocorrelation coefficient remains unchanged for each computer), which was used as the main idea for identifying a particular computer, is not observed throughout the interval of change of the argument. For this study, only a section of full graphic was used, where this feature is present.

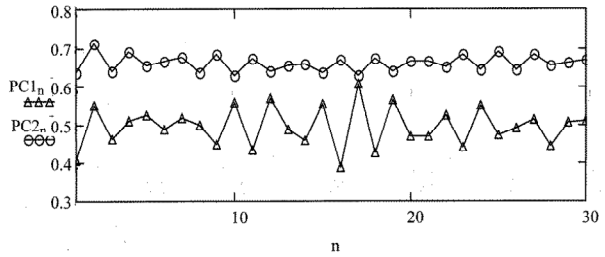

Fig. 3. Functions of autocorrelation of noise of two different computers

It does not depend on the shift of the selected sequence of samples within each file (Fig. 4).

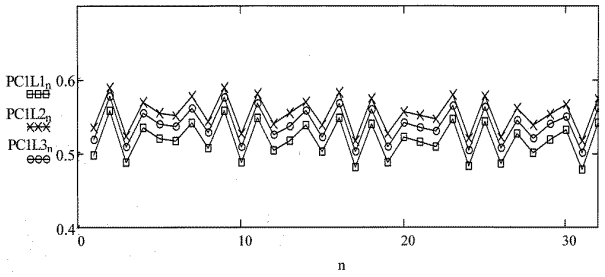

Fig. 4. Functions of autocorrelation of noise of one computer for different shifts from the beginning of a file. L1 = 53456, L2 = 41000, L3 = 49000 samples

It is practically constant for noise signal files recorded at different instants of time (Fig. 5).

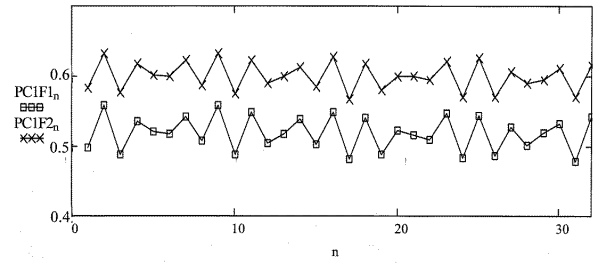

Fig. 5. Functions of autocorrelation of noise files of one computer. The recording is done at different times

Thus, the form of the autocorrelation function's plot can be used for identification of computer in network. The identification procedure is presented in the next section. It should be noted that the average value and variance of the selected sequences are not constant, i.e. noise signal is non-stationary. This is also confirmed by the visually non-stationary nature of the spectrum observed.

The accuracy of estimating the discrete values of the autocorrelation function is determined by the accuracy of the measured values of the noise signal samples, which, in turn, depends on the magnitude of the measured signal and the ADC resolution. In the experiments, a 20-bit ADC of a Realtek audioplate was used. The noise level was 200 μV. The maximum intensity of the input signal level by the microphone input is 5 V. Therefore, the minimum signal that can be measured in this case is 4.7 μV. The error in measuring the samples of the noise signal was 1 %. The accuracy of the estimation of the autocorrelation function will be somewhat smaller, of the order of 5 %.

III. FORMATION OF THE AUTHENTICATION SIGNS

The task of authentication of electronic devices with internal electrical noise is based on the uniqueness of the spread of the parameters as a component base at the microscopic level, and their constructive location. The task is solved by the method of calculating the autocorrelation function of the noise signal, which is characteristic for each electronic device and characterizes its own resonant frequencies. Based on the autocorrelation function, the bit and amplitude patterns of the device are calculated. Although the autocorrelation function is practically individual for each device, different autocorrelation functions are used for authentication. It is necessary to compare. As such a value the template is proposed, it consists of a bit sequence (bit template) and a sequence that characterizes the amplitude of the samples (amplitude template).

A bit pattern is a sequence of zeros and ones that are formed by the following rule: if the next value of the autocorrelation function a_{n+1} is not less than the previous an ($a_{n+1} \geq a_n$), then one is written to the bit sequence, if less, ($a_{n+1} < a_n$), then zero is written. The length of this bit sequence is one less than the number of samples of the autocorrelation function and is *N-1*. To compare two bit sequences obtained from different autocorrelation functions, the specific Hamming distance is calculated. The Hemming distance is normalized to the length of the sequence of autocorrelation values.

Necessary length of the autocorrelation function is of importance. Not equal bits in bit sequence are not equidistant. The set of not equal bits for two computers are shown in the Fig. 6.

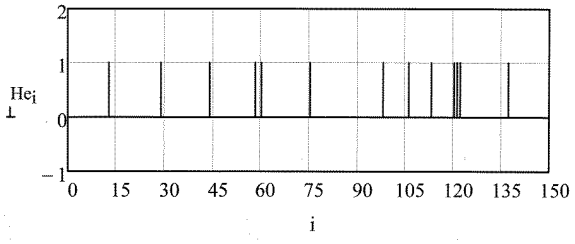

Fig. 6. Set of not equal bits of bit sequence for two computers

The set of not equal bits for two computers are shown in the Fig. 7.

The comparisons of normalized Hemming distance for bit sequence of two computers and the one of one computer are shown, that the 1000 bit length is enough for computer authentication. The results are in Table 1.

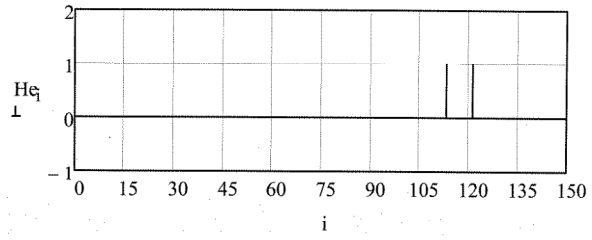

Fig. 7. Set of not equal bits of bit sequence for one computer

Table 1

Normalized Hemming Distances

Length of bit sequence	Normalized Hemming distance for two computers	Normalized Hemming distance for one computer
10	0.000	0.000
20	0.050	0.000
30	0.067	0.000
40	0.050	0.000
50	0.060	0.000
60	0.083	0.000
70	0.071	0.000
80	0.075	0.000
90	0.067	0.000
100	0.070	0.000
150	0.087	0.013
200	0.095	0.010
300	0.100	0.010
400	0.103	0.010
500	0.098	0.008
600	0.095	0.007
700	0.099	0.009
800	0.101	0.009
900	0.102	0.009
1000	0.100	0.009

The normalized Hamming distance for the two computers and one computer differ approximately in 10 times. This makes it possible to reliably distinguish these computers on the network.

Thus, the constant form of the autocorrelation function makes it possible to form an invariant – the normalized Hamming distance. This invariant can be used to authenticate the device on the network.

Authentication is carried out as follows. The oscillogram of the internal noise signal of the PCi computer is recorded using a software oscillometer. The sequence of the noise signal samples is fed to the input of the autocorrelation calculation program. The computed autocorrelation is recorded in the template folder of the PCi computer. This procedure is carried out for all N personal computers of the laboratory, office. Templates are stored on the server in the authentication database.

Autocorrelation functions are similarly obtained for each PC1-PCN computer. They are sent to the input of the comparison program with templates of the authentication database. For example, all pairs of autocorrelation functions are sequentially compared when authenticating a PCJ computer. In pair, one of them corresponds to the PCJ being tested, and the other one corresponds to each computer in the network.

The dynamic authentication algorithm has been developed, which consists of choosing a range of time series, defining and calculating invariants, making decisions about authentication. The result of the operation of the algorithm can be transferred to the executive mechanism, depending on the practical problems in cyber-physical systems.

IV. INVARIANT CHARACTERISTICS OF STOCHASTIC TIME SERIES WITH VARYING DISPERSION

The property of preserving the form of the function of autocorrelation of the studied time sequences enables the prediction of the following values of the sequence data.

Below, the simulation is performed for a pseudo-random sequence {*rnd*(1)-0.5}. The time realization of a series of dynamic variables $x_i(t_i)$ of each system *j* will be different. Calculations show that for noise-like time series the autocorrelation functions change insignificantly, they retain their own form, Fig. 8.

The function *lcorr*(*x*,*x*) was used to calculate the autocorrelation. The result represents 100 values for each subsequence. The procedure of linear interpolation *linterp*(*i*,*y*(*i*),*x*) was applied to the values of autocorrelation for convenience of comparison.

Three characteristic features are observed. Firstly, the form of the autocorrelation function for different subsequences of each sequence under study remains practically constant. Secondly, there are samples for which the autocorrelation function of different subsequences is the same with great accuracy. For example, samples number 25 and number 28 are in the Fig. 8. Thirdly, the autocorrelation function for the cross-rate of currencies is similar to the autocorrelation of flicker noise, which was investigated earlier.

It is possible with great accuracy to perform prediction of the sample number 101 for the first subsequence using the first and second characteristic features. The next method is proposed for this prediction. The sample with number 101 for the first subsequence is the sample number 100 for the second subsequence. The value of this sample $R2_{100} = y$ can take any value from the range of possible values: from *-0.5* to *+0.5* in increments of *0.01* (for example), y_i*=-0.5+0.01*(*i-1*), *i=1...101*. For each value y_i, the autocorrelation functions $A3(y_i)$ are calculated and the values $A3(y_i)_l$ for lag *l* are selected. Each of them is compared with the value of the autocorrelation function $crR1_l$ with the lag *l* from the first subsequence. The value y_i, which is the solution of the equation $A3(y_i)_l = crR1_l$, determines one

of the hundred numbers i and y_i. It should be noted that $crR1_l \approx crR2_l$. The graphical solution of the equation $A3(y_i)_l = crR1_l$ is shown in Fig. 9. The function $root(A3(y)\text{-}crR1_l)$ was used to determine y_i analytically.

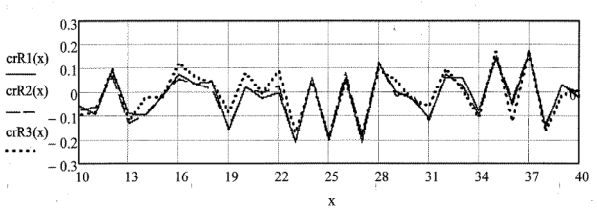

Fig. 8. Autocorrelation functions of subsequences of a pseudo-random sequence {rnd(1)-0.5}

The forecast was made for a pseudo-random sequence {*rnd*(1)-0.5}. The first forecast value coincided with the true one with great accuracy. In general, the calculations were carried out for the next 10 samples; all the calculated values practically coincided with the true ones. The results of the forecast are presented in Table 2. For clarity, the coincident numerals of the predicted samples and true samples are underlined.

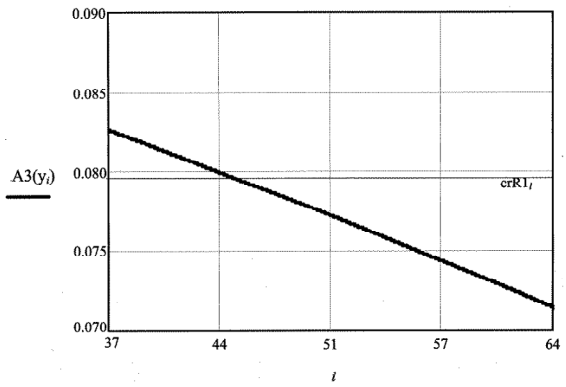

Fig. 9. Graphical solution of the equation to determine the predicted value of the sample

Table 2

Results of forecasting the values of 10 samples of the sequence {rnd(1)-0,5}

Number i	Predicted r	True r	δ
1	-0.0633244	-0.0633169	$-7.5\cdot10^{-6}$
2	0.0778651	0.0778666	$-1.5\cdot10^{-6}$
3	0.1287013	0.1286670	$34.3\cdot10^{-6}$
4	0.0041477	0.0041493	$-1.5\cdot10^{-6}$
5	0.1957697	0.1957680	$1.7\cdot10^{-6}$
6	-0.3100367	-0.3100483	$11.6\cdot10^{-6}$
7	-0.3216296	-0.3216249	$-4.7\cdot10^{-6}$
8	-0.0425355	-0.0425416	$6.0\cdot10^{-6}$
9	-0.4024815	-0.4024773	$-4.2\cdot10^{-6}$
10	-0.4056022	-0.4055958	$-6.4\cdot10^{-6}$

The forecast was made for a pseudo-random sequence {*rnd*(1)-0.5}. The first forecast value coincided with the true one with great accuracy. In general, the calculations were carried out for the next 10 samples; all the calculated values practically coincided with the true ones. The results of the forecast are presented in Table 2. For clarity, the coincident numerals of the predicted samples and true samples are underlined.

Thus, the constant form of the autocorrelation function as an invariant makes it possible to find the predicted values of the noise signal samples.

V. CONCLUSION

The authentication method for components of cyber-physical systems is proposed, which is based on invariants of internal electrical noise signals. The Hemming distance between two bit sequences is formed when comparing the autocorrelation functions of two signals from similar electronic devises. The experimental study confirmed the proposed method of authentication.

The proposed method can be used to authenticate network devices for which there is a possibility of measuring the noise signal in real time. The reliability of authentication (the template characterizes only this particular device), the speed of calculations, the possibility of full automation are important advantages of the proposed method. The area of such authentication is the Internet of things, the identification of devices and people using their noise-like signals.

The limitations of the proposed method are as follows: external conditions should not lead cyber-physical systems out of a quasi-stationary state. Additional authentication parameters can reduce false positives and false negatives.

ACKNOWLEDGMENT

The author thanks associate professor Shandra Z. A. of Lviv Polytechnic National University for useful discussions of the topic.

REFERENCES

[1] Jakob Hasse, Thomas Gloe, Martin Beck Forensic Identification of GSM Mobile Phones [Electronic resource]. – Access: http://www.dence.de /publications/Hasse13_GSMMobilePhone Identification.pdf (online).

[2] Toshiba Develops New Chip Authentication Technology Using Transistor Noise [Electronic resource]. – Access: http:// www.toshiba.co.jp/ rdc/rd/detail_e/e1506_03.html, 10 August 2016 (online).

[3] Князев А. Д. Элементы теории и практики обеспечения электромагнитной совместимости радиоэлектронных средств. – М.:Радио и связь, 1984. – 336 с.

[4] Чумаченко А., Идентификация цифровых микрофонов по неидеальностям тракта записи / Д. Рублёв, А. Чумаченко, О. Макаревич, В. Фёдоров // Известия ЮФУ, Технические науки, Тематический выпуск "Информационная безопасность", Таганрог, 2007. – № 8. – С. 84–92.

[5] Rybalsky O. Signalogramm Structure and Universality of the Fractal Approach to the Development of the Phonoscope Assessment Toolkit / V. Zhuravel, O. Rybalsky, V. Solovyev // Informatics & Mathematical Methods in Simulation. – 2013. – Vol. 3. – Is. 3. – P. 225–232.

[6] Nyemkova E. Technique of Measuring of Identification Parameters of Audio Recording Device / E. Nyemkova, V. Chaplyha, Z. Shandra // Selected Papers of the 18 International

Conference on Information Technology for Practice 2015. – Octouber 2015, Ostrava, Czech Republic. – P. 209–218.
[7] Немкова О. Ідентифікація елементів кібер-фізичних систем за шумовими характеристиками / О. Немкова, В. Чаплига, З. Шандра // Матеріали V Міжнародної науково-технічної конференції Захист Інформації і Безпека Інформаційних систем. – Львів, 2016. – С. 158–159.
[8] Diligenska, A. N *Identification of control objects*, Samara State Technical University publishing, 2009, 220 p.
[9] Loskutov, A. (2009) *Lectures time series analysis*, [Online], Available: http://chaos.phys.msu.ru/loskutov/PDF/Lectures_ time_series_analysis.pdf [20 Aug 2017].
[10] Patra, J.C. (1999) 'Identification of nonlinear dynamic systems using functional link artificial neural networks'. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*. Vol. 29, Is/ 2, pp. 254–262.
[11] Patra, J.C. and Kot A.C. (2002) 'Nonlinear dynamic system identification using Chebyshev functional link artificial neural networks'. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*. Vol. 32, Is/ 4, pp. 505–511.
[12] G. Nicolis, I. Prigogine, Self-Organization in Nonequilibrium Systems, Ney York, 1977.
[13] W. Ebeling, Stochastis Theorie nichtlinearer irreversibler Prozesser, Rostock, 1977.
[14] A. Mehrotra, "Simulation and Modelling Techniques for Noise in Radio Frequency Integrated Circuits", University of California at Berkeley, 1999.
[15] Dyvak M., Kasatkina N., Pukas A., Padletska N. 'Spectral analysis of information signal in the task of identification the recurrent laryngeal nerve during thyroid surgery', *Proceedings of the 13th International Workshop "Computational Problems of Electrical Engineering"*, Grubow, Poland, 2012, p. 55.
[16] Dyvak M., Padletska N., Pukas, A., Kozak O. 'Identification the Recurrent Laryngeal Nerve by the Autocorrelation Function of Signal as Reaction on the Stimulation of Tissues in Surgical Wound', *Proceedings of the XIIth International Conference CADSM'2013*, Lviv, Ukraine, p. 89–92.
[17] Loskutov A., Kotlyarov O. 'Local approximation: A new method of forecasting of economic indexes'. *Currency Stag*, No. 11, 2008, p. 8–13.
[18] Kuzovlev, Yu. E. 'Why nature needs 1/f noise'. *Physics-Uspekhi*, Vol. 58, no. 7, 2015, pp. 719–729.
[19] Nikulchev, E. B. Identification of dynamic systems based on symmetry of reconstructed attractors, Moscow, Moscow state university of printing publishing, 2010.
[20] Petrovich, V. N. 'Identification of parameters of mathematical models of dynamic control system'. *Artificial Intelligent*, Is. 4, 2011, pp. 343–349.

Elena A. Nyemkova graduated from the Specialty Faculty of Physics, Moscow Engineering Physics Institute, Moscow, Russia in 1984. She received specialty in solid-state physics and qualification as an engineer-physicist. She graduated from postgraduate studies in the Moscow Engineering Physics Institute in the specialty radiophysics, including quantum radiophysics in 1987; then she defended a dissertation for a Ph.D. in Physics and Mathematics in 1988.

Since 1988 she has been working at the Research Institute of Radio Engineering in Lviv, Ukraine as a research associate on the problem of construction of ultra-high frequency devices. Since 2004, she began working in higher education. In 2011 she received the scientific title of Associate Professor at the Department of Information Security. She is a co-author of the monograph, has more than 40 scientific works after Ph.D. Since 2015 she has been working at the Department of Information Technology Security at Lviv Polytechnic National University. Her scientific interests include the authentication of electronic devices by internal electronic noise, the identification of complex systems in terms of time series of variables of observation and forecasting time series.