Volodymyr KHOMA[1], Vitalii IVANYUK[2]

Opole University of Technology, Department of Electrical Engineering, Automatic Control and Informatics (1), "Lviv Polytechnic" National University, Institute of Computer Technologies, Automation and Metrology (2)

doi:10.15199/48.2017.02.55

High Sensitive Wiretap Detector: Design and Modeling

Abstract. *This article presents a novel method and improve system for monitoring of unauthorized connections on the subscriber's local telephone loop. In operation the detector displays electrical changes in impedance characteristics on the subscriber's telephone line to detect and alert about connecting of wiretapping equipment anywhere on the local loop.*

Streszczenie. *W artukule przedstawiono nową metdę udoskonalenia systemu monitoringu nieautoryzowanych podłączeń do abonenckiej pętli telefonicznej. Podczas pracy detektor rejestruje zmianę elektryczne w charakterystykach impedancji na abonenckiej linii telefonicznej w celu detekcji i alarmowania o podłączeniu podsłuchu w dowolnym miejscu na pentli aboneckiej.* (***Wysokoczuły detektor podsłuchu przewodowego: projektowanie i modelowanie***).

Keywords: Local Telephone Loop, Wiretapping Equipment , Unballanced Bridge Circuit, Phase Sensitive Detector.
Słowa kluczowe: abonecka pętla telefoniczna, podsłuch przewodowy,

Introduction

Despite the enormous progress in the development of telecommunications technology traditional telephony remains one of the most widespread and popular means of communication. Among the threads of Information Security of telephony subscribers the interception of phone messages and wiretapping of telephone-equipped apartments is the most probable [1,2]. Most frequently such threads are realized by unauthorized connection of the wiretapping equipment to the local telephone loop (LTL) [3].

Nowadays, a lot of methods and means of detection and localization of telephone wiretaps that work on different principles, are developed [3, 4, 5]. Significant widespread became detectors of unauthorized connections, which work is based on the monitoring of parameters of impedance of telephone lines. Connection of telephone wiretaps causes change in electro-physical parameters of the line, which is a decamouflage feature. Most attackers use parallel phone wiretaps, due to better technical and operational characteristics [2,3].

Shortcomings

However, the development of electronic technology makes it possible continuously to improve the technical and operational characteristics of telephone wiretaps, what results a decrease of effectiveness of existing monitoring of cable lines connection. That is why the search for new methods of detection of unauthorized connections to the LTL endures [6,7,8].

Aim of paper

The object of the article is the development and study of detection of illegal connections to the LTL, which is based on a linear adapter by way of unbalanced four-port axle of alternating current (AC) and processing path of the signals, built on the principle of phase-sensitive comparator.

Mathematic Model of Telephone Local Loop and Wiretaping Equipment

The classical model of cable lines (Fig. 1) is represented by the so-called primary parameters – linear capacity of C_O, inductance L_O, resistance R_O and conductivity G_O.

At radio frequencies the line model with distributed parameters, which consists of a certain number of cascade engaging of links, shown in figure 1, is used. The number of links for the model is determined by the ratio of the line's length and wavelength [9, 10]:

$$N = \frac{l}{\lambda} = \frac{l \cdot f}{v} \tag{1}$$

where: l is the length of line, λ and f is the wavelength and frequency of probe signal, υ is a velocity of wave propagation in transmission line.

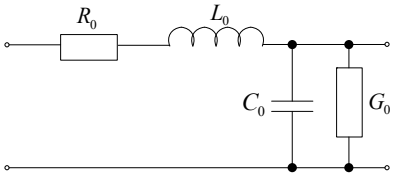

Fig.1. Lumped element model of transmission line

In the case of impulsive signals the number of links is determined by the formula [9]

$$N = \frac{l}{v \cdot \tau_R} \tag{2}$$

where τ_R – endurance of the front of impulse.

For telephone signals the model of line with lumped parameters is used, as the LTL length does not exceed the wavelength of the tone signal. Moreover, in the case of open-loop at the remote end of line model can be further simplified, since the absence of current lines the impact resistance and inductance can be neglected. So in the model of open-loop line (Fig. 1) only the capacity and conductivity are take into account.

The capacity of the line can be considered as a capacitor, which covers are two conductors and where the insulation materials are used as dielectric. The capacity of the cable line is called working capacity in opposite to the partial capacity (between two single conductors, between the conductor and insulated sheath, between the conductor and ground). For example, the Linear Capacity of category 5 cable is C_O = 50 pF/m [10, 11].

The conductivity of the insulation of cable line consists of the insulation's conductivity and depends on the dielectric looses and current frequency $G_O = g_0 f^G$, where for a given type of cable the parameters are next G = 1.38 and g_0=0.235·10^{-15} Sm/m [10]. For example, at a frequency of 1 kHz Linear conductivity come to G_O = 3,24·10^{-12} Sm/m, ie tgδ=10^{-5}. So, if the operating frequency of the detector will be equal to f = 1 kHz, the influence of the conductivity can be neglected, so it could be considered that the model of open-loop lines is represented by the only one parameter – capacity.

Most attackers use the so-called parallel telephone loops. To ensure secrecy of unauthorized connections

incoming impedance of the parallel phone loop should be as big as possible [3, 6]. In this sense the most suitable way to connect the Telephone wiretaps is the way shown in figure 2, due to which LTL impact is minimal. The capacitor C_S prevents an input of direct-current voltage on the LTL. With the $C_S >> C_{IN}$, $R_{IN} >> 1/2\pi f_O C_{IN}$ i $C_{IN} << C_L$ the impact of the Telephone wiretaps is primarily manifested in the slight increase in lines' capacity $C_X \approx C_L + C_{IN}$.

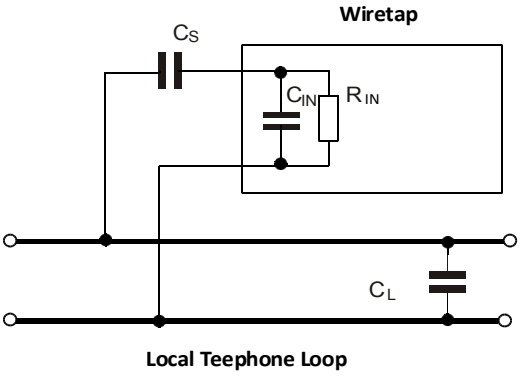

Fig. 2. The variant of connection of a parallel telephone wiretap

So, the capacity of the controlled cable line can take values:
- For "clean lines"

(3,a) $$C_X = C_L$$

- In the case of connection lines with capacity wiretap C_{IN}

(3,b) $$C_X \approx C_L + C_{IN}$$

Improving the telephone wiretaps parameters and reducing of their impact on the parameters of the telephone line complicates the task of their identifying. The means of control, based on already known methods, due to limited sensitivity could not find a telephone wiretaps with the high impedance (200 MOhm). That is why important is the search of new methods of detection of telephone wiretaps and development of means of control of LTL based on them. A target in this area is the development of highly sensitive linear adapter invariant to external impact of destabilizing factors.

Adapter based on Unbalanced Bridge Circuit

The adapter provides the physical connection of unauthorized connection detection device to the telephone line and generates an alarm signal in case of change of capacity line. To achieve high sensitivity the projected line adapter is based on unbalanced four-arm bridge of alternating current (Fig. 3) [8].

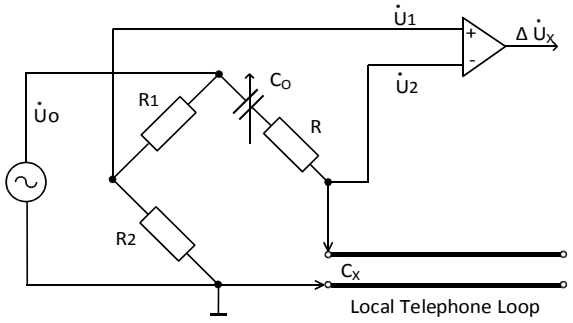

Fig. 3. Scheme of adapter based on unbalanced four-arm bridge of alternating current

Bridge Adapter turns on on the place of the telephone, and the line is previously de-energized by disconnection of its controlled area from the subscribers' telephone station in the distribution cabinet. Thus, the "clean line" is represented by the capacity and conductivity between the two cable conductors.

Unbalance of the bridge circuit is caused by the use of R_1 and R_2 on the right side of resistors, and capacitive elements (in the lower arm of controlled cable line with a capacity of C_X, and consistently switched regulated capacitor C_O and low-resistant resistor R at the top) on their left side.

Assuming $R_1 = R_2$ the output signal of the adapter, defined by the potential difference U_1 and U_2 on the left and right arms of the bridge, is described by:

(4) $$\Delta\dot{U} = \frac{\dot{U}_O}{2} \cdot \frac{C_X/C_O - 1 + j\omega_O C_X R}{1 + C_X/C_O + j\omega_O C_X R}$$

where: U_O is a probing voltage.

The setup of a bridge adapter is made on the "clean line" when the equality is realized (3,a) by the selection of a capacity of controlled capacitor, so that

(5) $$C_O = C_L$$

Thus, the "clean line" output voltage of the adapter is described by the formula:

(6) $$\Delta\dot{U}_X = \frac{\dot{U}_O}{2} \cdot \frac{j\omega_O C_O R}{2 + j\omega_O C_O R}$$

As for the case of connection to the wiretap's line with capacity C_{IN} the expression of adapter's output voltage is rather cumbersome [12], but it can be simplified by assuming that $C_{IN}/C_L << 1$ i $\omega_O R C_X << 1$:

(7) $$\Delta\dot{U}_X \approx \dot{U}_O \cdot \frac{C_{IN}/C_O + j\omega_O C_X R}{4\left(1 + C_{IN}/C_O\right)}$$

Research shows that informative parameters which maximize the selectivity and sensitivity to changes in electro-physical parameters of the telephone line is phase

(8) $$Arg\left(\Delta U_X\right) = \varphi = arctg\left(\frac{\omega_O \cdot R \cdot C_X}{C_{IN}/C_O}\right)$$

and in-phase component of the output voltage

(9) $$\mathrm{Re}\left(\Delta U_X\right) = \left|U_O\right| \cdot \frac{C_{IN}}{4 \cdot C_X}$$

instead of amplitude and quadrature components vary slightly by connecting the phone wiretaps with the capacity of C_{IN}.

Characteristics of linear adapter depend on the values of resistances and capacitances of the bridge circuit elements. Obviously, the capacitance value range C_O of the adjustable capacitor should cover possible capacitance value C_L of the controlled area of subscriber telephone lines. Regarding the passport data of working capacity of telephone cables and considering the length of the line in the area from the telephone to the distribution cabinet, the capacitance value C_L typically will be in the range from 1000 pF to 10 nF. For researches is used the value where C_L = 5 nF.

Figure 4 shows the results of the study of mathematical models of linear adapter when the capacity of the phone wiretaps C_{IN} is from 5 pF to 50 pF, which accounts 0.1% and 1% of the capacity C_L of the telephone line and probing

voltage U_O = 10 V. The chosen frequency of probing signal is f_O = 1 kHz, as it is convenient from the side of terms of performance of measuring channel elements and acceptable values of current in the bridge circuit arms. As $Xc = 1/2\pi f_O C_O$ ≈ 30 kΩ, the value of resistance of the resistive divider are chosen to be equal $R_1 = R_2$ = 10 kΩ.

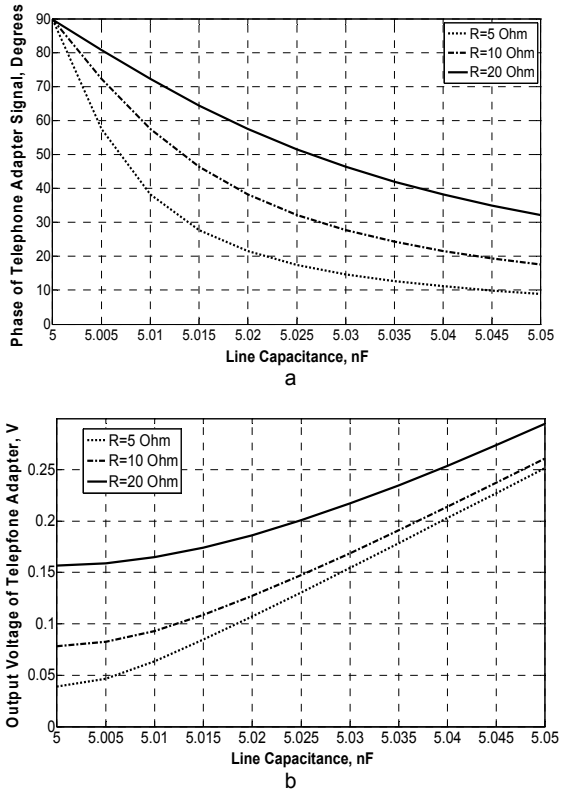

Fig. 4. Dependence phase (a) and the bridge adapter output voltage (b) changes of capacity telephone lines for different values of resistance additional resistor

The resistance of the additional resistor R directly affects the signal strength imbalance of the bridge circuit (fig. 4, a). Studies have shown that reducing R increases the sensitivity of the bridge adapter (fig. 4, b), but decreases the immunity by reducing its output voltage. For reasons of compromise the value of R is chosen to be R = 10 Ω. Under these assumptions the level of output voltage of the bridge adapter decreases due to probing voltage on -42 dB for the "clean line" or -32 dB in case of wiretap connection with the capacity of 50 pF.

Low level of output voltage of the bridge adapter complicates the selection phase as informative parameter. Studies have shown that false response of wiretap detector occur in the case of noise's intensity 1 μV.

Sampling Type Phase Sensitive Detector Algorithm

Besides the control phase, to identify unauthorized connections the in-phase component of output voltage $\mathrm{Re}(\Delta U_X)$ of the bridge adapter (10) can be measured. The figure 5 shows the dependence $\mathrm{Re}(\Delta U_X)$ on capacitance values of telephone wiretap. The advantage of this variant of wiretap realization, which is obvious thanks the comparison of expressions (9) and (10), is invariance to frequency's instability of probing signal f_O and deviation resistance R of the additional resistor.

While the output voltage of the bridge adapter is low, the authors see the appropriateness of synchronous detection usage, as noise-immune method of processing signals [13,14]. The structure of the telephone wiretap detection device based on such an approach is shown in the Fig. 6.

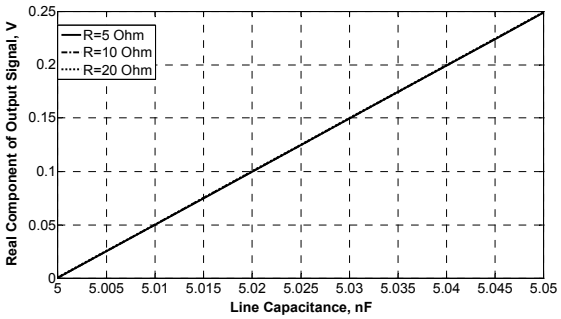

Fig. 5. Dependence of in-phase voltage component of the bridge adapter on changes of the telephone line's capacity

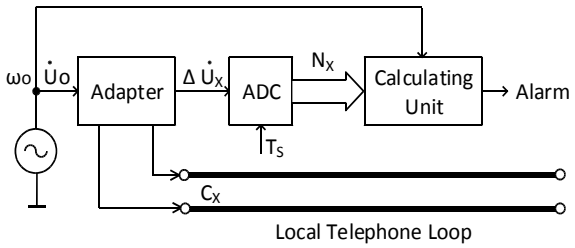

Fig. 6. Structure of the telephone wiretap detection device based on synchronous detector

The feature of the proposed device is a digital version of implementation the synchronous detection. To do this, digitized samples of the measurement and reference voltages are multiplied. Later works of prepared summarized [15]:

$$\dot{X}(f_O) = \sum_{n=0}^{N-1} x(n) \times \left[\cos\left(\frac{2\pi f_O n}{N} \right) \right] \tag{10}$$

where: $x(n)$ and $X(f_O)$ – are the sample of adapter voltage ΔU_X and its spectrum with frequency of probing signal f_O, n and N – sample's number and the amount of samples in the block, $\cos(2\pi f_O n/N)$ – vector of reference signal made by digital signals' synthesizer.

Expression (11) can be shown as an algorithm of One Point Digital Cosine Transform. To get the results, the N multiplications should be made, that means that some processing power is needed. Therefore, the authors studied the alternative way of Simultaneous detection's realization, which does not require the multiplication.

Output voltage adapter ΔU_X is digitized by using of the Analog to Digital Converter (ADC) and in the form of samples $x(n)$ of the Two's Complement format comes to the compute block (Fig. 6). Besides, needed for synchronous detection reference signal comes from the Direct Digital Syntesis (DDS). Figure 7 shows a block-scheme of an algorithm for synchronous detection realization without operation of multiplication.

At the beginning all the registers and counters CU are at zero-point. The counter starts counting pulses of DDS, that means numbers of samples from the moment when the probing voltage phase U_O is zero. The pulses' counting are synchronous to the data reading $x(n)$ of the ADC of the Two's Complement format.

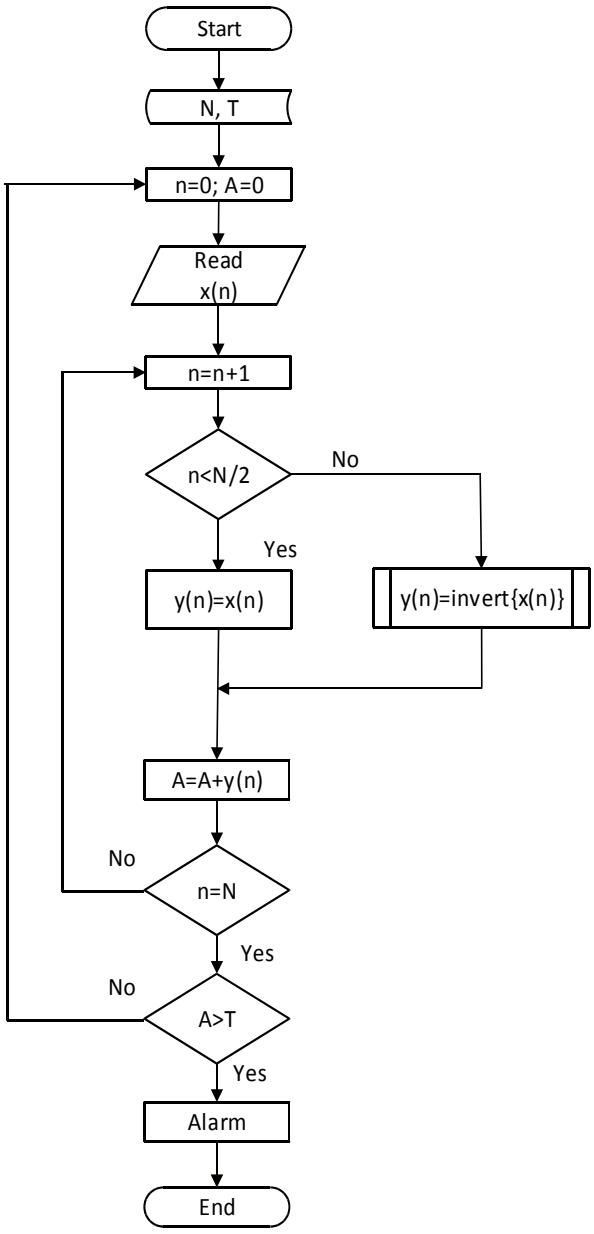

Fig. 7. The block-scheme of an algorithm for synchronous detection

If the samples belongs to the first half-period $n \leq N/2$ of probing voltage U_O, they are written to the battery without any changes. Instead of that, during the second half-period $n > N/2$ bits of each sample are inverted, and only then written to the battery. At the end of the period, that means at the time $n = N$, the read of battery content and its comparison with the battery threshold T took place. In case of exceeding of the threshold signal an Alarm signal is generated. If the threshold is not exceeded, registers and counters CU are equal to zero ($n = 0$, $A = 0$) and the new cycle of the measuring process is started.

Experiment Results of Detector Signal Processing

Researches of metrological qualities of Wiretap Detector based on synchronous detection, including its noise immunity, are conducted in the software package Matlab.

Figure 8 shows the samples during one period including sign changes.

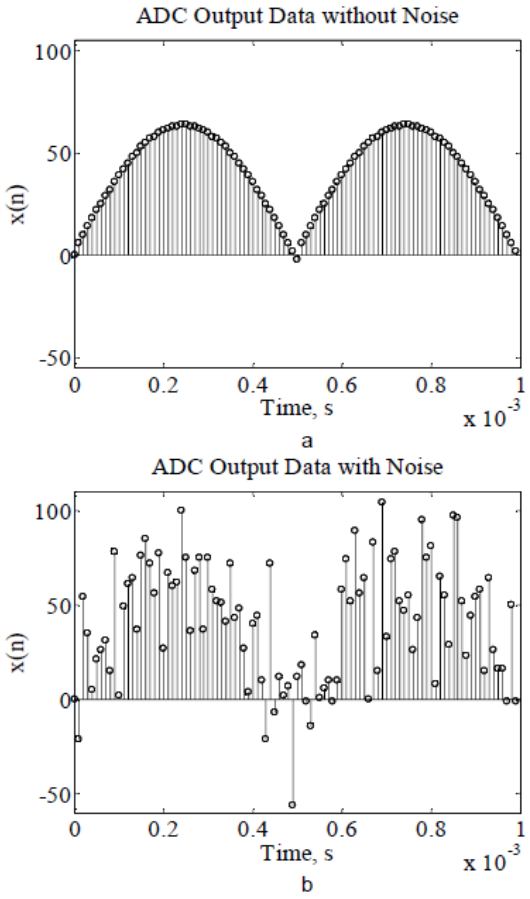

Fig. 8. The samples during one period including sign changes: a – upon the noise absence; b – upon the presence of noise

Research methodology included the formation of white noise of given intensity and overlay on the low-level output voltage ΔU_X of bridge adapter. As ΔU_X value depends on the capacity wiretap C_{IN}, the ratio signal to noise ratio was calculated through the formula

$$SNR = 20\lg\left(\frac{\Delta U_X}{\sigma_\xi}\right) \tag{11}$$

where: ΔU_X is root mean square of output bridge voltage, σ_ξ^2 - variance of the noise.

Table 1 presents the results of detector's researches upon the noise intensity σ_ξ = 1 mV. If the threshold is T = 1, the correct results of wiretaps identifying can be obtained starting with C_{IN} = 2 pF, which is less than 0.05% of the nominal capacity of the line.

Table 1. The dependence of the results of detector functioning on the capacity of wiretap in the noise background of 1 mV

C_{IN}, pF	0	1	2	5	10	20	50
SNR, dB	-5.8	-4.3	-1.6	4.7	10	16	24
A_N	-0,16	0,84	1,87	4,85	9,82	19,8	49,5

Table 2 presents the results of research of detector upon the noise intensity σ_ξ = 10 mV. If the threshold is T = 1, the correct results of wiretaps identifying can be obtained starting with C_{IN} = 5 pF, which is almost 0.1% of the nominal capacity of the line.

Table 2. The dependence of the results of detector functioning on the capacity of wiretap in the noise background of 10 mV

C_{IN}, pF	0	1	2	5	10	20	50
SNR, dB	-26	-24	-22	-15	-9.6	-3.7	4.2
A_N	-1,4	-0,31	0,61	3,7	8,6	18,6	48,4

The results can be improved through the K-periods' number increasing, during which the data is accumulated. Table 3 presents the results of research of detector upon the noise intensity σ_ξ = 10 mV and K = 10. If the threshold T = 1, the correct results of wiretaps identifying can be obtained starting with C_{IN} = 2 pF, which is less than 0.05% of the nominal capacity of the line. Thus, the increase of destabilizing impact of the higher intensity can be neutralized by the appropriate number's increase of K-periods of data accumulation.

Table 3. The dependence of the results of detector functioning on the capacity of wiretap in the noise background of 10 mV and accumulation of data for 10 periods

C_{IN}, pF	0	1	2	5	10	20	50
SNR, dB	-25	-23	-21	-14	-8.5	-2.6	5.3
A_N	-0,14	0,86	1,86	4,8	9,8	19,8	49,6

The proposed variant of phase sensitive detector can be used in measuring devices, such as devices, measuring the impedance's deviation from the rated value. Figure 9 shows the dependence of error of deviation of the measured capacitance from the rated value 5 nF.

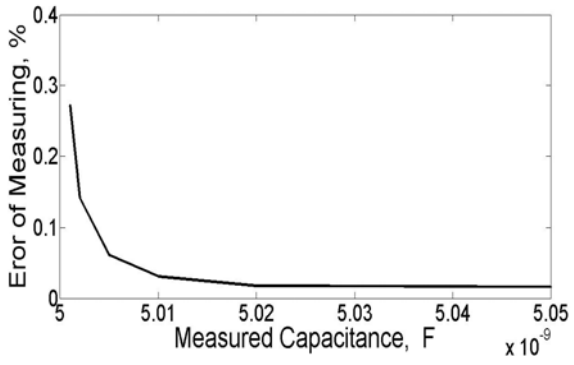

Fig. 9. Eror of measuring capacitance

Error value was calculated by the formula

$$\gamma(T) = \left(\frac{A_N}{C_X - C_{Nom}} - 1 \right) \cdot 100\% \quad (12)$$

where: A_N – measurement result recorded in a battery after samples' processing, C_X i C_{Nom} – which are measured and rated values of capacity.

Conclusions

Detection of telephone wiretaps with the help of wiretap detectors is important countermeasure for mitigating of information security risk. Due to the constant improvement of telephone wiretaps the increase of the sensitivity and noise immunity of wiretap detectors is needed.

The implementation of disagreeing requirements for increase of sensitivity and noise immunity became possible thanks combination of highly sensitive bridge adapter's qualities projected by the authors and noise-immune method of processing its signal based on the use of phase sensitive detecting. The authors developed also a simple and effective way of realization of phase sensitive detecting in digital form. The peculiarity of this method is absence of samples multiplication operations of measured and reference signals.

Through the study of mathematical model of bridge adapter ascertained is that high sensitivity to changes in capacity of controlled line is provided upon measuring of such parameters as phase or in-phase component of its output voltage. Considering the potentially higher noise immunity, the authors chose the phase sensitive detecting allotment of in-phase component. Upon the results of simulation modeling in MatLab package the noise immunity of authors proposed method of realization of phase sensitive detecting is investigated and confirmed.

***Authors**: Prof., dr hab. inż. Volodymyr Khoma,* Politechnika Opolska, Instytut Automatyki i Informatyki, *E-mail: v.khoma@po.opole.pl; Vitalii Ivanyuk, mgr inż.,* Narodowy Uniwersytet „Politechnika Lwowska", *E-mail: vitalikivaniuk@gmail.com*

REFERENCES

[1] Anderson R.J., Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Ed. New York: *John Wiley & Sons*, (2008)

[2] Taylor C.L., Telephone Eavesdropping and Detection, 1st Ed. *Taylor Hill Pub Co,* (1989)

[3] *Advanced Wiretap Detector.* Instruction Manual. *TT-46 General Information / http://www.pimall.com/nais/ccdownloads/tt46manual.pdf*

[4] Swift T.N., Wiretap Detection Techniques. A Guide to Checking Telephone Lines / *Thomas Investigative Publications, Inc.* (2010), *http://www.pimall.com/nais/bk.wire.html*

[5] Roger T., Wiretap And Bug Detection. The Basic Principals of Bug and Wiretap Detection / *California Association of Licensed Investigators Newsletter. http://www.bugsweeps.com/info/wiretap_detection.html*

[6] TALAN Telephone and Line Analyzer / *Thomas Investigative Publications, Inc. http://www.pimall.com/nais/protelan.html*

[7] Svintzov I.V., Protalinski O.M., Svintzov V.Ya., Fazovoy metod obnaruzheniya niesankcionirovannogo podklyucheniya k slabotochnoy linii svyazi, *Sensors and systems*. (2009), nr 7, 2-4 (In Russian)

[8] UA Patent 108186, H 04M 1/68, H 04 L 12/22. Pristrijj dlya viyavlennya nesankcionovanogo pidklyuchennya do abonentskoi telefonnoi linii / Ivanyuk V.M., Khoma V.V., Mar., (2015)

[9] Howard W. J., Graham M. High Speed Signal Propagation: Advanced Black Magic First Edition,/ *Williams Publishing House,* (1993)

[10] Acatauassu D., Höst S., Chenguang Lu, Berg M., Klautau A., Börjesson O. Simple and Causal Copper Cable Model Suitable for G.fast Frequencies, *IEEE Transactions on Communications,* Vol. 62, No. 11, (2014), 4040-4051

[11] Lao R. The Twisted-Pair Telephone Transmission Line // *High Frequency Electronics*, November (2002), 20-30

[12] Ivanyuk V.M., Khoma V.V. Phase detection method embedded devices in telephone line // *Ukrainian Information Security Research Journal*, 16 (2014), nr 3, 243-251

[13] Trieu P.Q., Due N.A. Implementation of the digital sensitive system for low signal measurement, *VNU J. Sci., Math. Phys.*, Vol. 24, (2008), 239–244

[14] Vandenbussche Jean-Jacques, Lee Peter, Peuteman Joan. On the Accuracy of Digital Phase Sensitive Detectors Implemented in FPGA Technology, *IEEE Transactions on Instrumentation and Measurement,* Vol. 63, No. 8, (2014), 1926-1936

[15] AD 5933. 1 MSPS, 12 bit Impedance Converter, Network Analyzer. *Preliminary Data Sheet – http://www.analog.com/UploadedFiles/Data_Sheets/AD5933.pdf*