híradástechnika

VOLUME L.

1999/6

50th ANNIVERSARY

journal on communications

5 computers

convergence

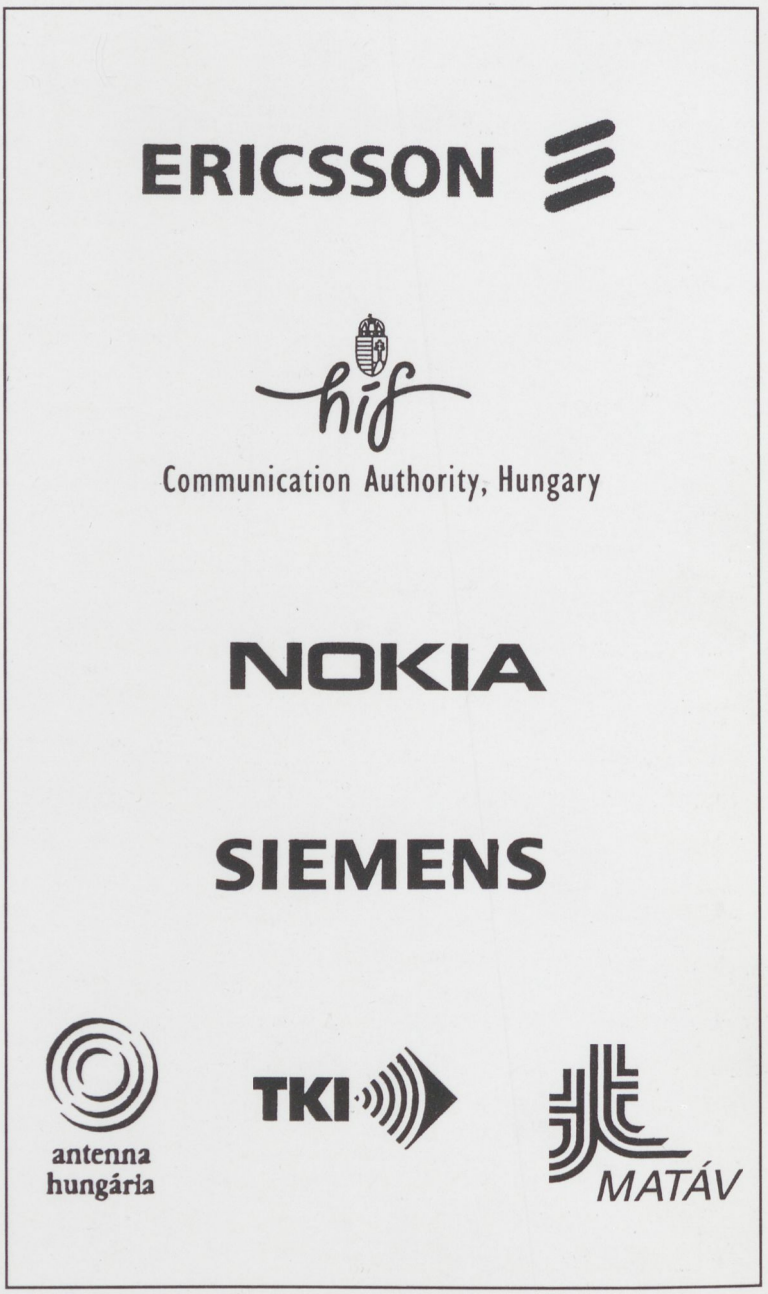
contents

companies

JOURNAL ON C[5]

A PUBLICATION OF THE SCIENTIFIC SOCIETY FOR TELECOMMUNICATIONS, HUNGARY

SPONSORED BY



Szerkesztőség / Editorial office
HÍRADÁSTECHNIKA
Budapest, VI. Paulay E. u. 56. II.14/A.
Telefon:(361) 341-6421, (361) 325-9058
Fax: (361) 341-6421, (361) 325-9058
Előfizetés / Orders to
HÍRADÁSTECHNIKA/TYPOTEX
H-1024 Budapest, Retek u. 33-35.
Tel./Fax: (361) 316-3759

1999-ES ELŐFIZETÉSI DÍJAK
Hazai közületi előfizetők részére
1 évre 20000 Ft +12% ÁFA = Btto 22400 Ft; Egyes számok 2000 Ft +12% ÁFA = Btto 2240 Ft
Hazai egyéni előfizetők részére
1 évre 4000 Ft +12% ÁFA = Btto 4480 Ft; Egyes számok 400 Ft +12% ÁFA = Btto 448 Ft
HTE tag előfizetők részére
1 évre 2000 Ft +12% ÁFA = Btto 2240 Ft; Egyes számok 200 Ft +12% ÁFA = Btto 224 Ft
Subscription rates for foreign subscribers
12 issues 100 USD, single copies 10 USD
Transfer should be made to the Hungarian Foreign Trade Bank
Budapest, 10300002-20321411-00003285

HÍRADÁSTECHNIKA, JOURNAL ON C[5] is published monthly, in English and in Hungarian by TypoTEX Ltd.
H-1024 Budapest, Retek u. 33-35. Phone/Fax: (361) 316-3759. Publisher: Zsuzsa Votisky.
Type-setting by TypoTEX Ltd. Printed by Regiszter Ltd.
HU ISSN 0018-2028

HÍRADÁSTECHNIKA

Vol. L. No. 6, JUNE, 1999
HU ISSN 0018-2028

JOURNAL ON C[5]

50 years

from the Telecommunications Scientific Society

CONTENTS 1

Abstract: In this issue 8 papers are presented. Section **Communications** is represented by 2 contributions on The Multifunction N-Ports Biquads and on The Maximal Power Matching. Section **Computers** is comprised of 2 contributions on The WWW Based Information Systems and on The Internet Systems Security. Section **Convergence** is formed by a single poster contribution written on the Microwave Magnetic Envelope Solitons. Section **Contents** and distribution of multimedia is containing 1 contribution from the Hungarian experiences focusing on the Internet Legal Regulation. Section **Companies** is now dealing with 2 contributions on the Realisation of Distributed and Object Oriented Stock Systems and on the Ultrasonic Navigation Device for Blind People, both from Technical University of Budapest. In this issue 8 submitted papers of the 8 ones are scientifically evaluated by 4 senior reviewers. These papers have been accepted by the reviewers as scientific contributions. They are marked on their first pages by the sign of $\mathcal{L}$ giving the evidence of the scientific nature.

MULTIFUNCTION N-PORT BIQUADS USING MODERN ACTIVE ELEMENTS

JOSEF CAJKA, KAMIL VRBA, VÁCLAV ZEMAN

DEPARTMENT OF TELECOMMUNICATIONS, TECHNICAL UNIVERSITY OF BRNO
PURKYOVA 118, 612 00 BRNO, CZECH REPUBLIC
FAX: +420 5 411 491 92, E-MAIL: VRBAK@UTKO.FEE.VUTBR.CZ

A method is described of designing multifunction networks that can be used as filters in various operation modes. The initial network is an autonomous circuit with an appropriate characteristic equation. The procedure is demonstrated on networks with the general characteristic equation $Y_1Y_3 + Y_2Y_4 = 0$. Used as active elements are nullors, second-generation current conveyors and transconductors.

Keywords: Nullors, current conveyors, transconductors, autonomous circuits, multifunction networks, analogue filters.

1. INTRODUCTION

Here, a multifunction network is understood to be an n-port that can be used in the design of various filters working in different modes, depending on the type of connection. Recently, universal n-port networks working either in the voltage mode or in the current mode have attracted significant research attention [1], [2]. In the following, the design of such a universal second-order network (biquad) containing some modern active elements (current conveyors, four-terminal floating nullors, transconductors) will be described.

In the design we start from the general autonomous circuit with appropriate general characteristic equation (CE). We have chosen a general CE of the type

$$Y_1Y_3 + Y_2Y_4 = 0 \qquad (1)$$

where Y_1, Y_2, Y_3, Y_4 are admittances of passive RC elements.

It is well known that the CE remains the same if we connect an ideal voltage source into its arbitrary branch or if we connect an ideal current source to an arbitrary terminal pair of the network. Considering only one driving source we can create a two-port network if we take as the output quantity an arbitrary port-voltage or an arbitrary branch-current [3].

2. GENERAL AUTONOMOUS CIRCUIT

2.1. Prototype circuit

Consider an autonomous circuit called two nullors on a ring [4] shown in Fig. 1. The nullor is a pair of singular elements nullator-norator. The CE of this circuit is

$$Y_1Y_3 - Y_2Y_4 = 0 \qquad (2)$$

It follows from Eqn. (2) that in the schematic diagram in Fig. 1 we can interchange the elements with admittances $Y_1 \longleftrightarrow Y_3$ or $Y_2 \longleftrightarrow Y_4$, or we can interchange arbitrarily the two elements with Y_1, Y_3 and the elements with admittances Y_1, Y_4, without altering CE (2).

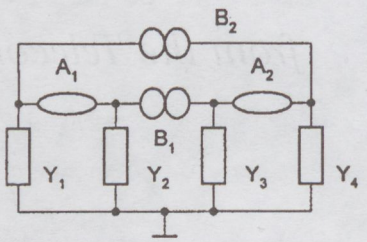


Fig. 1. Two nullors on a ring circuit

It is obvious that CE (1) will be obtained from relation (2) if the sign of any admittance is changed. This can be realized in the circuit in Fig. 1 by using a negative immittance converter with conversion -1.

Three-terminal nullors can be replaced by other active elements, as shown in the following.

2.2. Networks with current conveyors

First, replace the two three-terminal nullors in Fig. 1 by second-generation current conveyors. The current conveyor, whose schematic diagram is given in Fig. 2, is a three-port immittance converter with one independent current I^* and two independent voltages. For second-generation current conveyors [5] the following relations hold between the nodal voltages and the nodal currents: $V_x = V_y$, $I_x = I^*$, $I_y = 0$, $I_z = BI^*$, with V_y and V_z being independent voltages. If $B = 1$, we speak about the current conveyor CCII+, if $B = -1$, we have to do with the current conveyor CCII−. Some time ago it was possible to realize the current conveyor CCII+ by means of the CCII01 device (LTP Electronics, UK), while still used as CCII+ can be part of the AD844 transimpedance operational amplifier (Analog Devices, USA), and commercially available is the OPA660 so-called *Diamond Transistor* (Burr-Brown, USA). The current conveyor CCII− is not commercially available but it can be replaced by means of two current conveyors CCII+ (Fig. 4) [6]. We have proposed a new combined current conveyor CCII+/− in integrated form. Its schematic symbol is shown in Fig. 2b, the schematic diagram for its realisation is in Fig. 3. It is a four-port immittance converter with one independent current I^*, for which it holds: $V_x = V_y$, $I_x = I^*$, $I_y = 0$, $I_{z+} = I^*$, $I_z = -I^*$.

It is well known that the equivalent current conveyor CCII− (Fig. 4) can replace any three-terminal nullor. The characteristic equation of the autonomous circuit does not change if the two nullors in Fig. 1 are replaced by the current conveyors CCII+ that we connect in the same manner as if we connected the current conveyors CCII−.

An autonomous circuit of this type for A1-B1 and A2-B2 nullors is shown in Fig. 5. Symbols A1, A2 denote in Fig. 1 nullators, whereas symbols B1, B2 retate there to norators.

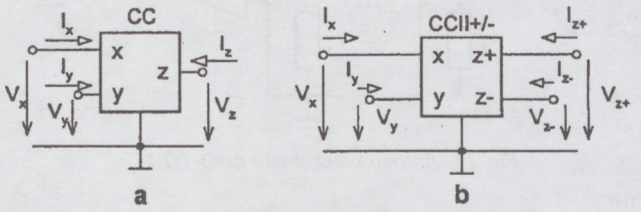


Fig. 2. Schematic diagram a) of a current conveyor, b) of a CCII+/− element

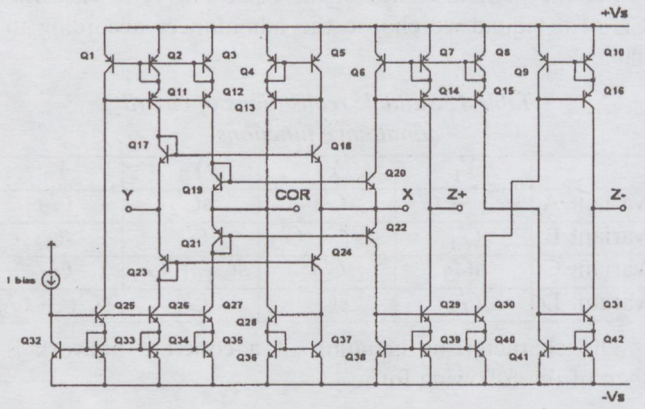


Fig. 3. Realisation of the CCII+/− element in integrated form

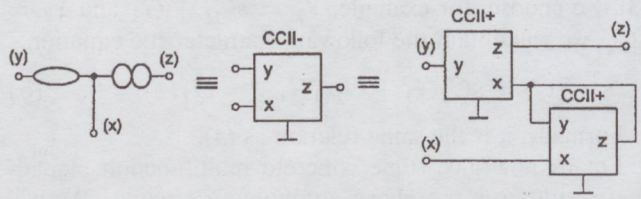


Fig. 4. Equivalent three-terminal elements

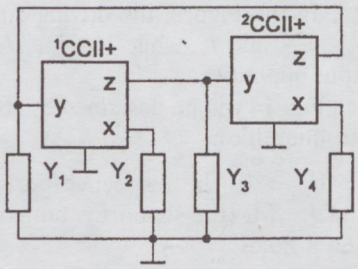


Fig. 5. Autonomous circuit using two CCII+ elements

Since there exists a simple negative immittance converter (NIC) with one CCII+ current conveyor (Fig. 6), we can change the sign of any admittance in Fig. 5 using the above NIC and thus obtain the required CE (1). Fig. 7 gives one variant of the above autonomous circuit that satisfies condition (1). The sign of admittance Y_2 was changed using ^{3}CCII+ element. According to Fig. 4 the conveyors ^{3}CCII+ and ^{1}CCII+ can be replaced by one current conveyor CCII−. We have found that the autonomous circuit with CE (1) can be obtained directly from the circuit in Fig. 1 by replacing one three-terminal nullor by a CCII− conveyor and the remaining nullor by a CCII+ conveyor.

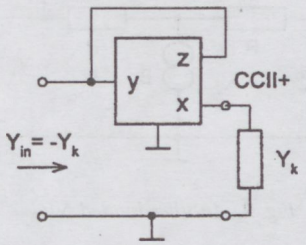


Fig. 6. Loaded negative immittance converter (NIC)

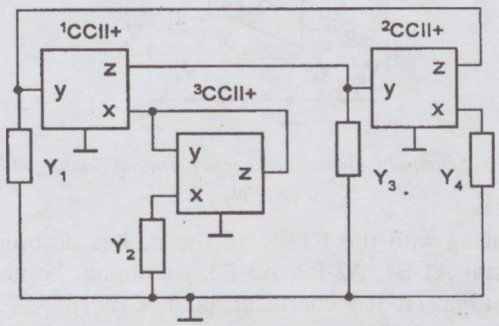
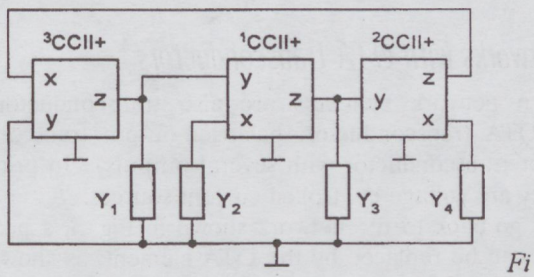


Fig. 7. Autonomous circuit with characteristic equation (CE)

$$Y_1 Y_3 + Y_2 Y_4 = 0$$

There is yet another possibility how to change the sign of either admittance Y_1 or admittance Y_3, namely by converting the direction of current through the two-terminal element by means of another conveyor ^{3}CCII+. In Fig. 8 we change the direction of current through the dipole with admittance Y_1 while the initial voltage on the element does not change.



Fi

Fig. 8. Autonomous circuit with the same CE as that in Fig. 7

2.3. Networks with four-terminal floating nullors

A simple NIC with one nullor is shown in Fig. 9. Let us suppose that this circuit will be used to change the sign of admittance Y_1 in the network in Fig. 1. This will again yield an autonomous circuit with CE (1). A novel element in integrated form has been proposed, which is denoted either FTFN (four-terminal floating nullor) [7] or OMA (operational mirrored amplifier) [8]. It is a four-terminal nullor (the nullator is separated from the norator). In the following, the schematic symbol in Fig. 10 will be used for the FTFN. Here it holds that $I_a = I_b = 0$, $V_a = V_b$, $I_d = -I_c$.

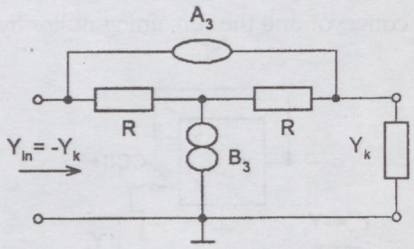


Fig. 9. Another loaded NIC

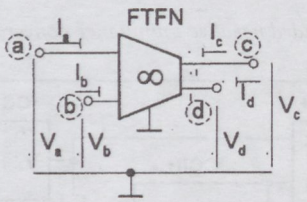


Fig. 10. Schematic diagram of a four-terminal floating nullor (FTFN)

Replacing with the FTFN all the nullors according to the variant A1-B1, A2-B2, A3-B3, we obtain the network shown in Fig. 11. It is characterised by CE (1).

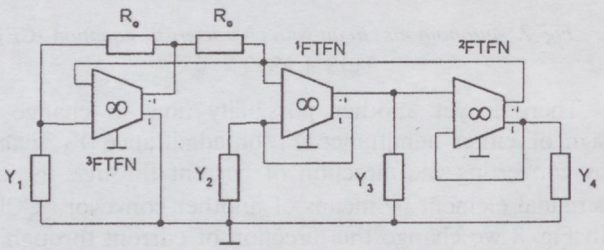


Fig. 11. Autonomous circuit using FTFNs

2.4. Networks with OTA transconductors

Modern network elements are also transconductors (simple OTA transconductor, balanced-output transconductor, or transconductor with several outputs). In principle, they are voltage-controlled current sources.

Let us go back to the network shown in Fig. 5, a part of which can be replaced by the OTA element, as shown in Fig. 12. The direction of output current (marked in the Figure by a small boldface triangle) can be changed by inverting the input voltage. The value of transconductance G_m is set electronically. Then the network in Fig. 5 is easy to change into an autonomous system as shown in Fig. 13. Its general characteristic equation is in the form

$$Y_1 Y_2 + G_{m1} G_{m2} = 0. \tag{3}$$

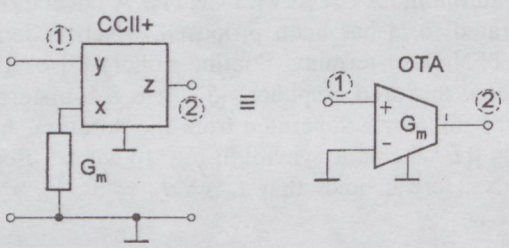


Fig. 12. Realisation of an OTA

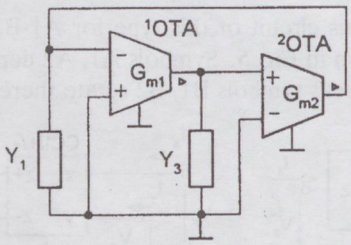


Fig. 13. Autonomous circuit using OTAs

3. MULTIFUNCTION N-PORTS

3.1. Realization structures

For the general characteristic equation (1) to yield the CE of a biquad we choose the admittances according to Table 1.

Table 1. Suitable realisations of circuit admittance functions

	Y_1	Y_2	Y_3	Y_4
Variant A	$sC_1 + G_3$	$G1$	sC_2	G_2
Variant B	G_1	$sC_1 + G_3$	G_2	sC_2
Variant C	sC_2	G_2	$sC_1 + G_3$	G_1
Variant D	G_2	sC_2	G_1	$sC_1 + G_3$

The characteristic equation of a concrete network is then of the following form

$$s^2 C_1 C_2 + s C_2 G_3 + G_1 G_2 = Q(s) = 0. \tag{4}$$

If for the network in Fig. 13, which is described by CE (3), we choose, for example, $Y_1 = sC_1 + G_1$ and $Y_2 = sC_2$, we will obtain the following characteristic equation

$$s^2 C_1 C_2 + s C_2 G_1 + G_{m1} G_{m2} = Q_1(s) = 0. \tag{5}$$

Formally, it is the same relation as (4).

Let us now give some concrete multifunction biquads that result from the above autonomous circuits. We will start with the circuit in Fig. 8. Choosing the admittances in the circuit according to variant A will yield the six-port shown in Fig. 14. In the Figure, the driving quantities are denoted V_{i1}, V_{i2}, V_{i3} and I_i, while V_o, I_{o1}, I_{o2}, I_{o3} and I_{o4} are the output quantities.

The six-port in Fig. 14 will be described by the following output and input quantities:

a) When $V_4 = V_5 = 0$ (the respective ports are short-circuited) and $I_i = 0$ (the six-port is not supplied with current), then it holds

$$\mathrm{V_o} = \frac{\mathrm{s^2 C_1 C_2 V_{i1} - s C_2 G_2 V_{i2} + G_1 G_2 V_{i3}}}{\mathrm{Q(s)}} \tag{6}$$

and

$$I_{o4} = \frac{G_3 V_0}{Q(s)}. \tag{7}$$

b) If $V_{i1} = V_{i2} = V_{i3} = V_4 = V_5$, we establish by

$$I_{o1} = \frac{s^2 C_1 C_2 I_1}{Q(s)}, \tag{8}$$

$$I_{o2} = \frac{s C_2 G_1 I_1}{Q(s)}, \tag{9}$$

$$I_{o3} = \frac{sG_1G_2I_1}{Q(s)}\,, \tag{10}$$

and

$$V_o = \frac{sC_2I_1}{Q(s)}\,. \tag{11}$$

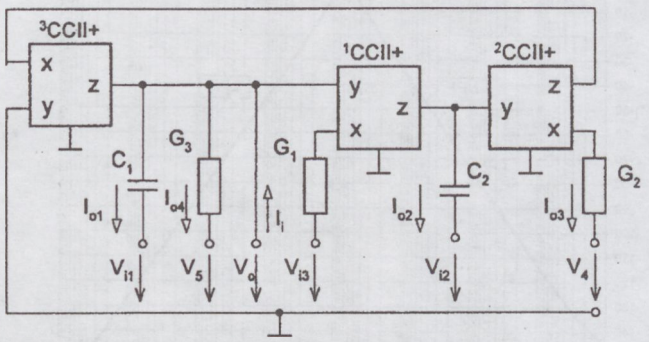


Fig. 14. Mulifunction network using three CCII+ elements

Another multifunction six-port will be obtained from the autonomous circuit in Fig. 5 by considering the element ^{1}CCII− instead of ^{1}CCII+. The two conveyors are then replaced by appropriately connected elements CCII+/−, as is, after transformation, evident from Fig. 15. In circuit realization we applied variant A from Table 1. By calculation we establish that the six-port in Fig. 15 is also described by equations (6) to (11).

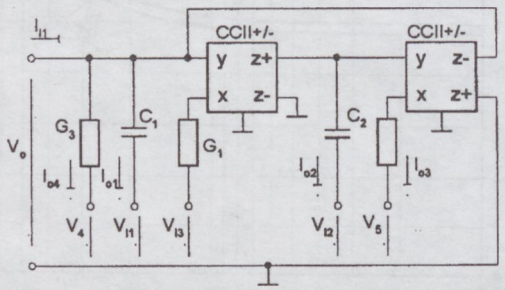


Fig. 15. Multifunction network with CCII+/− elements

When transforming the autonomous circuit with FTFN elements in Fig. 11 using variant C from Table 1, we obtain the six-port shown in Fig. 16. In this case, too, the network is described by equations (6) to (11).

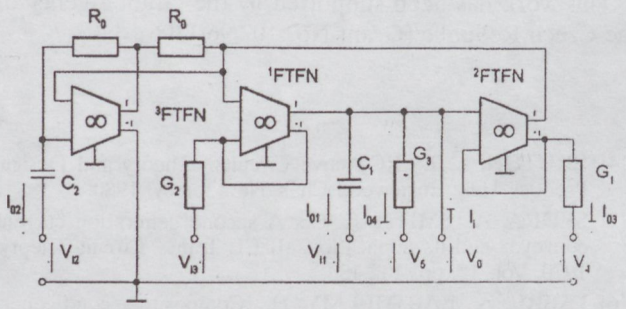


Fig. 16. Multifunction network using FTFNs

From the autonomous circuit in Fig. 13 a multifunction network can be obtained the properties of which differ from these of the preceding biquads. Choosing the above admittance values we create a multifunction four-port as given in Fig. 17. The input quantities are V_{i1}, V_{i2}, I_{i1} and I_{i2} while the output quantities are V_{o1}, V_{o2}, I_{o1} and I_{o2}. Between the output and the input quantities the following relations evidently hold

$$\mathrm{V_{o1}} = \frac{\mathrm{s^2C_1C_2V_{i1} + sC_2G_1V_{i2}}}{\mathrm{Q_1(s)}}\ (\mathrm{I_{i1} = I_{i2} = 0})\,, \tag{12}$$

$$\mathrm{V_{o2}} = \frac{\mathrm{sC_1G_{m1}V_{i1} + G_1G_{m1}V_{i2}}}{\mathrm{Q_1(s)}}\ (\mathrm{I_{i1} = I_{i2} = 0})\,, \tag{13}$$

$$\mathrm{I_{o1}} = \frac{\mathrm{s^2C_1C_2I_{i1} + sC_1G_{m2}I_{i2}}}{\mathrm{Q_1(s)}}\ (\mathrm{V_{i1} = V_{i2} = 0})\,, \tag{14}$$

$$\mathrm{I_{o2}} = \frac{\mathrm{sC_2G_1I_{i1} - G_1G_{m2}I_{i2}}}{\mathrm{Q_1(s)}}\ (\mathrm{V_{i1} = V_{i2} = 0})\,, \tag{15}$$

$$\mathrm{I_{o1}} = \frac{\mathrm{s^2C_1C_2G_1I_{i1}V_{i2}}}{\mathrm{Q_1(s)}}\ (\mathrm{V_{i1}0, P_{i1} = I_{i2} = 0})\,, \tag{16}$$

$$\mathrm{V_{o1}} = \frac{\mathrm{sC_1I_{i1} - G_{m2}I_{i2}}}{\mathrm{Q_1(s)}}\ (\mathrm{V_{i1} = V_{i2} = 0})\,, \tag{17}$$

$$\mathrm{V_{o2}} = \frac{\mathrm{G_{m1}I_{i1}}}{\mathrm{Q_1(s)}}\ (\mathrm{I_{i2} = 0, V_{i1} = V_{i2} = 0})\,, \tag{18}$$

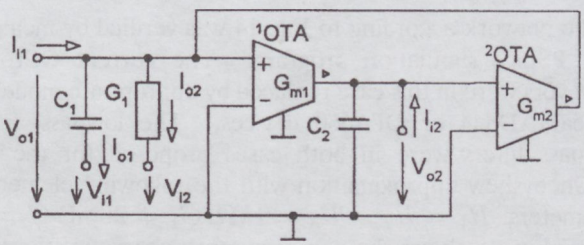


Fig. 17. Multifunction network with OTA elements

3.2. Application of proposed networks

All the six-ports in Figs 14 to 16 can be used as filters (two-ports) which work

a) in the voltage mode (V_o/V_{in}) (see relation (6)), namely as
   (i) lowpass filters if $V_{in} = V_{i3}$, $V_{i1} = V_{i2} = 0$,
   (ii) bandpass filters if $V_{in} = V_{i2}$, $V_{i1} = V_{i3} = 0$,
   (iii) highpass filters if $V_{in} = V_{i1}$, $V_{i2} = V_{i3} = 0$,
   (iv) notch filters if $V_{in} = V_{i1} = V_{i3}$, $V_{i2} = 0$,
   (v) allpass filters if $V_{in} = V_{i1} = V_{i2} = V_{i3} = 0$, $G_2 = G_3$;

b) as short-circuited two-ports with transadmittance (I_{o4}/V_{in}) with all the possibilities as under a) (as follows from Eqn. (7));

c) in the current mode (I_{out}/I_i) (see relations (8) to (10)) as
   (i) highpass filters if $I_{out} = I_{o1}$,
   (ii) bandpass filters if $I_{out} = I_{o2}$,
   (iii) lowpass filters if $I_{out} = I_{o3}$,
   (iv) notch filters if $I_{out} = I_{o1} + I_{o3}$;

d) as bandpass filter if the input quantity is current I_i and the output quantity voltage V_o (see relation (11)).

Similarly, the four-port in Fig. 17 can be used as a two-port which works

a) in the voltage mode (V_{out}/V_{in}) (see relations (12) and (13)) as
(i) a lowpass filter if $V_{in} = V_{i2}$, $V_{out} = V_{o2}$, $V_{i1} = 0$,
(ii) a bandpass filter if $V_{in} = V_{i2}$, $V_{out} = V_{o1}$, $V_{i1} = 0$ or if $V_{in} = V_{i2}$, $V_{out} = V_{o2}$, $V_{i2} = 0$,
(iii) a highpass filter if $V_{in} = V_{i1}$, $V_{out} = V_{o1}$, $V_{i2} = 0$;

b) in the current mode (I_{out}/I_{in}) (see relations (14) and (15)) as
(i) a lowpass filter if $I_{in} = I_{i2}$, $I_{out} = I_{o2}$, $I_{i1} = 0$,
(ii) a bandpass filter if $I_{in} = I_{i2}$, $I_{out} = I_{o1}$ or if $I_{in} = I_{i1}$, $I_{out} = I_{o2}$, $I_{i2} = 0$,
(iii) a highpass filter if $I_{in} = I_{i1}$, $I_{out} = I_{o1}$, $I_{i2} = 0$;

c) in the hybrid mode (Iout/Vin) (see Eqn. (16)) as
(i) a highpass filter if $V_{in} = V_{i2}$ a $I_{out} = I_{o1}$;

d) in the hybrid mode (Vout/Iin) (see Eqns (17) and (18)) as
(i) a lowpass filter if $I_{in} = I_{i2}$, $V_{out} = V_{o1}$, $I_{i1} = 0$ or if $I_{in} = I_{i1}$, $V_{out} = V_{o2}$,
(ii) a bandpass filter if $I_{in} = I_{i1}$, $V_{out} = V_{o1}$, $I_{i2} = 0$

4. SIMULATION RESULTS

The network according to Fig. 14 was verified by means of a PSpice simulation program. The current CCII+ conveyors were in this case replaced by appropriate models of real AD844 or OPA660 devices. The lowpass and highpass filters were in both cases proposed for the 3 dB Chebyshew approximation with the following element parameters: $R_1 = R_2 = R_3 = 1k\Omega$, $C_1 = 29$ nF, $C_2 = 17$ nF. Fig. 18 shows the gain-frequency characteristics of lowpass/highpass filters working in the voltage mode for 10 kHz cut-off frequency. Evidently, the curves are nearly identical for both AD844 and OPA660 devices. The small difference the two characteristics is apparent in detail in Fig. 19.

5. CONCLUSION

We have described a method of deriving an RC active n-port from an autonomous circuit with chosen general characteristic equation. This n-port can be used in various filter types working in different modes. A similar procedure has been used by the authors of [10], who refer to the initial circuit as the Grundschaltung. As an example of the above proposal a simple circuit for the synthesis of second-order filters has been described together with the possibilities of their application.

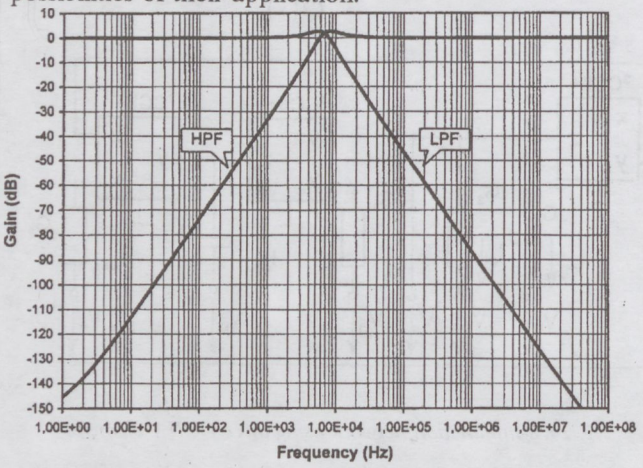


Fig. 18. Gain-frequency characteristics of voltage mode lowpass and highpass filters in Fig. 14 with simulated CCII+ elements (AD844 or OPA660)

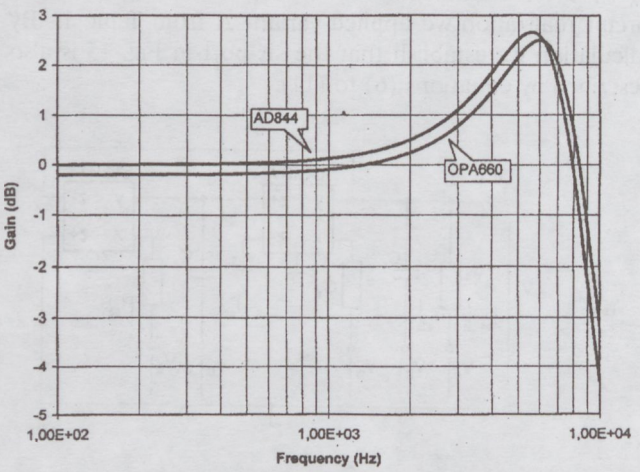


Fig. 19. Detailed comparison of voltage mode frequency gain response of LPF using AD844 or OPA660

6. ACKNOWLEDGMENT

This work has been supported by the Grant Agency of the Czech Republic (Grant No. 102/96/1306).

REFERENCES

[1] WENG, R.-M., LEE, M.-H.: Novel universal biquad filters using only three followers. Int. J. Electronics, 1977, Vol. 82, No. 2, pp 621-628.

[2] OZOGUZ, S., ACAR, C.: Single-input and three-output current-mode universal filter using a reduced number of active elements. Electronics Letters, 1998, Vol. 34, No. 7, pp 605-606.

[3] CAJKA, J., LINDOVSKY, D.: Universal RC-active network using CCII+. J. Electrical Engineering, 1997, Vol. 48, No. 3-4, pp 98-100.

[4] BRUTON, L. T.: RC-Active Circuits. Theory and Design. Prentice-Hall, Englewood Cliffs, New Jersey, 1980.

[5] SEDRA, A., SMITH, K. C.: A second generation current conveyor and its application. IEEE Trans. Circuit Theory, 1970, Vol. 17, pp. 132-134.

[6] FABRE, A., BARTHELMY, H.: Composite second-generation current conveyor with reduced parasitic resistance. Electronics Letters, 1994, Vol. 30, No. 5, pp. 377-378.

[7] LIU, S.-I., LEE, J.-L.: Insensitive current/voltage mode filters using FTFN. Electronics Letters, 1996, Vol. 32, No. 12, pp. 1079-1080.

[8] SENANI, R., MALHOTRA, J.: Minimal realisations of a class of operational-mirrored-amplifier-based floating impedances. Electronics Letters, 1994, Vol. 30, No. 14, pp. 1113-1114.

[9] MAHMOUD, S. A., SOLIMAN, M.: A CMOS programable balanced output transconductor for analog signal processing. Int. J. Electronics, 1997, Vol. 82, No. 6, pp. 621-628.

[10] HERPY, M., BERKA, J.-C.: Aktive RC-Filter. Franzis-Verlag, München/Akadémiai Kiadó, Budapest 1984.

MULTIFUNKCIONÁLIS N-KAPUK MODERN AKTÍV ELEMEK FELHASZNÁLÁSÁVAL

JOSEF CAJKA, KAMIL VRBA, VÁCLAV ZEMAN

DEPARTMENT OF TELECOMMUNICATIONS, TECHNICAL UNIVERSITY OF BRNO
PURKYOVA 118, 612 00 BRNO, CZECH REPUBLIC
FAX: +420 5 411 491 92, E-MAIL: VRBAK@UTKO.FEE.VUTBR.CZ

A cikk egy multifunkcionális n-kaput ír le, amely különféle típusú elektronikus szürök megvalósítására szolgálhat. Az említett áramkör különböző üzemmódokban müködhet (feszültség, áram és hibrid mód). A cikkben multifunkcionális n-kapuk egy autonóm áramkörből való tervezését írjuk le az (1) összefüggésnek megfelelő általános CE-egyenletből. A tervezésnél az autonóm áramkörben ideális feszültségforrásokat kötünk az összes tesztelt ágba (melyeknek belső ellenállása 0), az összes csomópont és tesztpontok közé pedig ideális áramforrásokat iktatunk (melyeknek belső ellenállásuk végtelen). Ezzel a változtatással a CE nem módosul. Ezután az összes feszültség, áram, rövidzárási admitancia, és üresjárati impedancia átvitelét vizsgáljuk az összes kétkapunál, amelyek az említett n-kapuból származtathatók. Végezetül pedig csak a megfelelő átviteli függvényekkel rendelkező kétkapukat választjuk ki. A cikk csak aktív RC-tagokat tárgyal. Aktív elemekként négypólusú lebegő nullort FTFN (four-terminal floating nullor) (10. ábra), második generációs ún. áram-konvejorokat CCII+, CCII−, CCII+/− (2. és 3. ábra) és OTA transzkonduktanciát (operational transconductance amplifier) választottunk (12. ábra). A CCII+ tag a kereskedelmben vagy AD844 (Analog Devices, USA) referenciájú áramkörként, vagy mint OPA660-as, ún. gyémánttranzisztor (Burr-Brown,USA) szerezhető be. OTA transzkonduktanciaként pedig az OPA2662-es hivatkozású áramköri elem (Burr-Brown) használható. A cikkben említett bekötéseket a két hurokba kötött nullor elvén (two nullors on a ring) alapuló általános autonóm áramkörből származtatjuk. Ez az áramkör könnyen átalakítható két CCII+ konvejorból (5. ábra), ill. két OTA transzkonduktanciából (13. ábra), vagy pedig FTFN elemekből (11. ábra) álló rendszerekre. Ahhoz, hogy a CE (2)-ből levezethessük a CE (1)-et, két egyszerű negatív immitancia konvertert, egy CCII+ tagot (6. ábra), és egy nullort (9. ábra) használunk fel. Ezzel az áramkör bármely admittanciájának előjelét megváltoztathatjuk. Az összes lehetséges áramkör közül, melyek az (1) egyenletnek felelnek meg, négyet említünk (7., 8.,11., és 13. ábra). A továbbiakban a kiválasztott általános autonóm áramkörből multifunkcionális áramköröket származtatunk. (Többnyire hat-kapukat a 14.–17. ábrák alapján.) A 14.–16. ábrán szemléltetett hatkapukat a következő módon használhatjuk fel:

a) A (6) összefüggés alapján feszültségmódban (V_{out}/V_{in}) mint aluláteresztő, felüláteresztő, sávátereszto és sávzáró szürő, valamint fáziskorrektor.

b) A (7) összefüggés alapján mint (I_{out}/V_{in}) transzadmittanciájú rövidrezárt kétkapu az a) pontban felsorolt lehetőségekkel.

c) A (8)–(10) egyenletek alapján árammódban (I_{out}/I_{in}) mint aluláteresztő, felüláteresztő, sávátereszto és sávzáró szürő.

d) A (11) egyenlet alapján (V_{out}/V_{in}) átviteli impedanciával (transinpedance) rendelkező üresjárati kétkapu mint sávszürő.

Valamivel kevesebb lehetőséget nyújt az OTA elemekből álló négykapu (17. ábra), mint ahogy azt a (12)–(18) egyenletek is mutatják. Végül a 14. ábrán bemutatott áramkörökből kapott aluláteresztő és felüláteresztő szürök frekvenciakarakterisztikája látható a Pspice-ban készített modellek alapján. Mindezekből látható, hogy az AD844-ből származtatott kétkapu tulajdonságai alig térnek el az OPA660-on alapuló (19. ábra) kétkapu tulajdonságaitól.

Josef Cajka is a professor emeritus. He taught Electronic Circuit Theory at the Military Academy in Brno from 1951 to 1972 and at the Faculty of Electrical Engineering of the Technical University of Brno from 1972 to 1984. His field of professional interest was the analysis of linearized circuits, in particular with the aid of computer. Currently he collaborates on the design of universal RC networks containing modern active elements.

Kamil Vrba received the M.E. degree in electrical engineering in 1972 and the Ph.D. degree in 1997, both from Technical University Brno. He joined the Institute of Telecommunications at the Faculty of Electrical Engineering and Computer Science of the TU in Brno and since 1997 is in a Full Professor position. His research work is concentrated to problems aimed to accuracy of analog circuits.

Vaclav Zeman was graduated at the Technical University of Brno. In 1993 he entered the Department of Telecommunication at the Technical University of Brno as an assistant lecturer. Since 1993 he has started his doctoral studies in the specialisation "Electronics". The domain of his interest are Higher Order Synthetic Elements and computer modelling and simulation.

MAXIMÁLIS TELJESÍTMÉNY-ÁTVITEL KIS NEMLINEARITÁSÚ ÁRAMKÖRÖKBEN

LADVÁNSZKY JÁNOS

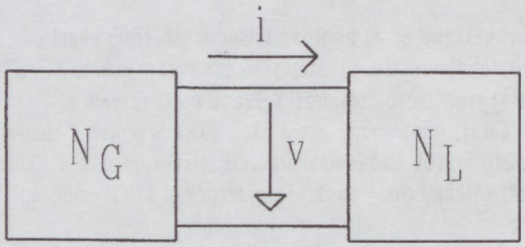
TÁVKÖZLÉSI INNOVÁCIÓS RT, TKI
1142 BUDAPEST, UNGVÁR U. 64-66.
TEL.: 251 0888, FAX: 251 9878, E-MAIL: LADVAN@TKI.HU

A maximális teljesítmény-átvitel problémáját vizsgáljuk abban az esetben, amikor a generátor belső konduktanciája harmadrendű Volterra-sorral van megadva. Bebizonyítjuk, hogy ekkor az optimális terhelés is harmadrendű Volterra sorral írható le. Zárt alakú kifejezéseket adunk meg az optimális terhelés Volterra-magfüggvényeire illetve azok frekvencia-tartománybeli megfelelőire. Eredményeink a (7.) egyenlettel leírt matematikai azonosságon alapulnak.

1. BEVEZETÉS

Adott az 1. ábrán látható N_G generátor-áramkör, amely nemlineáris áramköri elemeket és független forrásokat tartalmaz, melyek paraméterei változtathatók. Az a feladat, hogy megtaláljuk azt az N_L terhelő áramkört, amely maximális teljesítményt disszipál a változtatható paraméterek tetszőleges értéke esetén.

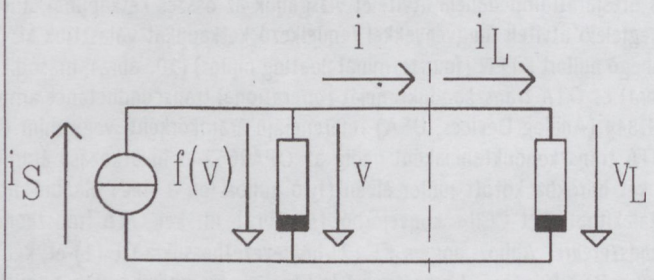
A szakirodalom a fenti feladatnak számos esetét tárgyalja, amelyek a generátorra vonatkozó feltételekben különböznek egymástól: rezisztív generátorok [1], [2], általános, nemlineáris, dinamikus generátorok [3], és olyan nemlineáris, dinamikus generátorok, amelyek a szinuszos bemenőjelre vonatkozó leírófüggvénnyel vannak jellemezve [4]. Az az ellentétes feladat, amelyben a generátor karakterisztikáját kell meghatározni a forrás karakterisztikájának ismeretében, szintén meg van oldva [5].



1. ábra. A maximális teljesítmény-átvitel problémája: adott az N_G generátor-áramkör, keresett az az N_L terhelő áramkör, amely a lehető legnagyobb teljesítményt nyeli el

Keverők és teljesítményerősítők esetén, amelyek szinuszos jelek összegével vannak vezérelve, a kimenő teljesítmény maximálásának feladata gyakran felmerül. Azonban ennek a feladatnak a generátor előzőekben megadott modellje segítségével történő tárgyalása szükségtelenül bonyolult. Sok alkalmazásban a gerjesztőjelek tartománya rögzített, ezért a vizsgált áramkört kis nemlinearitású modellel lehet jellemezni, és a Volterra-sorok alkalmazása előnyöket ígér.

Ebben a cikkben egykapus forrást tételezünk fel, melyet csonkított Volterra-sorral jellemzünk (2. ábra). Tetszőleges hullámformájú gerjesztést engedünk meg. A maximális teljesítmény-átvitel problémáját Rohrer-nek a lineáris áramkörökre vonatkozó módszerének [6], [7] általánosításával oldjuk meg. Zárt kifejezéseket adunk meg a maximális teljesítményt elnyelő terhelés karakterisztikájára a 4. fejezetben.



2. ábra. A generátor Norton helyettesítő áramköre, a terheléssel párhuzamosan kapcsolva

2. JELÖLÉSEK ÉS FELTÉTELEZÉSEK

Norton helyettesítő áramkörrel modellezhető generátort tételezünk fel, amelyet a következő összefüggéssel lehet leírni:

$$i(t) = i_S(t) - f[v(t)] \qquad (1.)$$

ahol $i(t)$ a kapuáram, $v(t)$ a kapufeszültség, és $i_S(t)$ a forrásáram hullámformáját, t pedig az időt jelöli. A generátor nemlinearitását az $f(.)$ idő-invariáns operátor jelöli. A feszültség és az áram hullámformáját négyzetesen integrálhatónak tételezzük fel a $-\infty < t < \infty$ intervallumban. Az ϵ nettó energia maximumát határozzuk meg. A nettó energiát a következő egyenlettel definiáljuk [7]:

$$\epsilon = \int_{-\infty}^{\infty} v(t)i(t)dt \qquad (2.)$$

és a jobb oldalon álló kifejezésre új jelölést vezetünk be:

$$\int_{-\infty}^{\infty} v(t)i(t)dt = < v, i > \qquad (3.)$$

Az integrálnak véges értéke van a Schwartz egyenlőtlenség következtében [7]. A Norton helyettesítő áramkör és a teljesítmény-maximum létezésének feltételei az irodalomban megtalálhatók [2], [3].

A generátort gyengén nemlineárisnak tételezzük fel abban az értelemben, hogy az f operátort csonkított Volterra-sorral lehet kifejezni [8]:

$$f[v(t)] = \sum_{N=1}^{N} f_n[v(t)] \quad (4.)$$

$$f_n[v(t)] =$$

$$= \int_{-\infty}^{\infty} \dots \int_{-\infty}^{\infty} h_n(\tau_1, \dots \tau_n) \prod_{k=1}^{n} [v(t-\tau_k) d\tau_k] \quad (5.)$$

A $h_n(t_1, \dots t_n)$ magfüggvényre a h_n rövidített jelölést vezetjük be:

$$f_n = h_n * \begin{pmatrix} 1 & \dots & n \\ v, & \dots & v \end{pmatrix} \quad (6.)$$

ahol * a konvolúciót jelöli. Vizsgálatainkban a következő azonosságnak alapvetően fontos szerepe van:

$$< \alpha, h_n * (v_1, \dots v_k, \dots v_n) >= \quad (7.)$$

$$= \left\langle v_{k,k} h_n * \begin{pmatrix} 1 & & k & & n \\ v_1, & \dots & \alpha, & \dots & v_n \end{pmatrix} \right\rangle$$

ahol $a(t)$ négyzetesen integrálható, és a bal oldali index előjelcserét jelöl az argumentumban:

$$_k h_n = h_n(\tau_1 \dots - \tau_k \dots \tau_n) \quad (8.)$$

A (7) azonosság csak elsőrendű magfüggvényre van bebizonyítva [7]. Magasabbrendű magfüggvényre a bizonyítás hasonlóan végezhető el.

3. MAXIMÁLIS TELJESÍTMÉNYÁTVITEL LINEÁRIS ÁRAMKÖRÖKBEN

A legújabb tudományos közlemények, amelyek lineáris áramkörökben tárgyalják a maximális teljesítmény-átvitelt szinuszosan gerjesztett áramkörökben, a [9] referenciában vannak felsorolva. Sajnos az ott idézett közlemények nem említik a [6], [7] cikkeket, melyek nem szinuszos gerjesztésekkel is foglalkoznak. A [6], [7] referenciák néhány lényeges mondanivalóját ebben a fejezetben foglaljuk össze.

Tekintsük a 2. ábrán látható egy kapus forrást, amely a tetszőleges $i_S(t)$ hullámalakú áramforrásból és a következő egyenlettel leírható, passzív egykapuból van felépítve:

$$f(v) = h_1 * v \quad (9.)$$

Az a feladat, hogy találjuk meg annak a terhelésnek a h_{L1} magfüggvényét, amely a legnagyobb

$$\epsilon =< v_L, i_L > \quad (10.)$$

nettó energiát nyeli el, ahol $v_L(t)$ és $i_L(t)$ a terhelés áram- és feszültség-hullámformája:

$$i_L = h_{L1} * v_L \quad (11.)$$

és az ábrából $i_L = i$, $v_L = v$. A maximális energiát és a hozzá tartozó hullámformákat nulla indexszel jelöljük:

$$\epsilon_0 =< v_{L0}, i_{L0} > \quad (12.)$$

Az optimális terhelést a feszültség variálásával keressük meg:

$$v = v_0 + \alpha \quad (13.)$$

A globális maximum feltétele a következő:

$$\epsilon_0 - \epsilon \geq 0 \quad (14.)$$

azaz

$$< v_0, i_0 > - < v_0 + a, i >\geq 0 \quad (15.)$$

tetszőleges α esetén. Rendezéssel kapjuk, hogy

$$< v_0, i_0 - i > - < \alpha, i >\geq 0 \quad (16.)$$

A generátor karakterisztikájának az (1.), (9.) egyenlettel megadott alakját alkalmazva azt kapjuk, hogy

$$i_0 - i = h_1 * (v_0 + \alpha) - h_1 * v_0 = h_1 * \alpha \quad (17.)$$

Behelyettesítve a (9.), (1.) és (17.) egyenleteket a (16.) egyenletbe, a következő adódik:

$$< v_0, h_1 * \alpha > - < \alpha, i_S - h_1 * (v_0 + \alpha) >\geq 0 \quad (18.)$$

A (18.) egyenlőtlenség akkor és csak akkor áll fenn tetszőleges α esetén, ha

$$< \alpha_1 h_1 - i_S + h_1 * v_0 >\geq 0 \quad (19.)$$

és

$$< \alpha, h_1 * \alpha >\geq 0 \quad (20.)$$

Az áramkört leíró egyenlet az optimumnak megfelelő v_0 feszültségnél a következő:

$$h_{L1} * v_0 - i_S + h_1 * v_0 = 0 \quad (21.)$$

Ezért a (19.) egyenlőtlenség biztosan teljesül, ha

$$h_{L1} =_1 h_1 \quad (22.)$$

A (20.) egyenlőtlenséget energia-elnyelési feltételnek nevezzük. A (22.) egyenlőtlenség kétoldalú Laplace transzformáltja a jól ismert komplex frekvenciatartománybeli teljesítmény-illesztési feltételt adja meg:

$$Y_L(s) = Y(-s) \quad (23.)$$

ahol Y_L, Y és s rendre a terhelő és a generátor-admittanciát és a komplex frekvenciát jelöli.

Általában a (23.) egyenlettel megadott terhelő admittanciát nem lehet realizálni, de realizálható egykapuk admittanciájával közelíteni lehet a $j\omega$ tengely valamely véges intervallumában. Ezzel a problémakörrel a pozitív reális függvénnyel történő interpoláció néven találkozunk a szakirodalomban.

4. ILLESZTÉS KIS NELINEARITÁSÚ ÁRAMKÖRÖKBEN

Most a 2. ábrán látható felépítésű, tetszőleges $i_s(t)$ hullámalakú áramforrásból és az alábbi karakterisztikájú passzív, nemlineáris egykapuból álló generátort vizsgáljuk:

$$f(v) = h_1 * v + h_2 * (v, v) + h_3 * (v, v, v) \quad (24.)$$

A feladat a maximális $\epsilon =< v_L, i_L >$ energiát elnyelő terhelés h_{L1}, h_{L2}, h_{L3} magfüggvényeinek megadása, ahol

$$i_L = h_{L1} * v_L + h_{L2} * (v_L, v_L) + \\ + h_{L3} * (v_L, v_L, v_L) \quad (25.)$$

és $v_L = v$, $i_L = i$. A problémát a lineáris áramkörök esetére elvégzett számítás lépéseinek erre az esetre történő általánosításával oldjuk meg.

A maximális energiát és a hozzá tartozó mennyiségeket nulla indexszel jelöljük. A globális maximum feltételét most is a következőképen adhatjuk meg:

$$\epsilon_0 - \epsilon \geq 0 \quad (26.)$$

azaz

$$< v_0, i_0 - i > - < \alpha, i > \geq 0 \qquad (27.)$$

A (27.) egyenlet első tagjában látható $i_0 - i$ most a következőképpen fejezhető ki:

$$\begin{aligned} i_0 - i = {} & h_1 * \alpha + \\ & + h_2 * [(v_0, \alpha) + (\alpha, v_0) + (\alpha, \alpha)] + \\ & + h_3 * [(v_0, v_0, \alpha) + (v_0, \alpha, v_0) + (\alpha, v_0, v_0)] + \\ & + h_3 * [(v_0, \alpha, \alpha) + (\alpha, v_0, \alpha) + (\alpha, \alpha, v_0)] + \\ & + h_3 * (\alpha, \alpha, \alpha) \end{aligned} \qquad (28.)$$

Behelyettesítve a (27.) egyenletbe az (1.) egyenletet, a következőt kapjuk:

$$< v_0, i_0 - i > - < \alpha, i_S - f(v) > \geq 0 \qquad (29.)$$

ahol $i_0 - i$ a (28.) egyenlettel, $f(v)$ pedig a (24.) egyenlettel van megadva. A behelyettesítés után az első tagra a (7.) azonosságot és a (8.) jelölést alkalmazva, a következő egyenletet kapjuk:

$$\begin{aligned} \epsilon_0 - \epsilon = {} & - < \alpha, i_S > + \\ & + < \alpha, ({}_1h_1 + h_1) * v_0 > + \\ & + < \alpha, ({}_1h_2 +_2 h_2 + h_2) * (v_0, v_0) > + \\ & + < \alpha, ({}_1h_3 +_2 h_3 +_3 h_3 + h_3) * (v_0, v_0, v_0) > + \\ & + < \alpha, h_1 * \alpha > + \\ & + < \alpha, ({}_1h_2 + h_2) * (v_0, \alpha) > + \\ & + < \alpha, ({}_1h_3 + h_3) * (v_0, v_0, \alpha) + ({}_2h_3 + h_3) * (v_0, v_0, \alpha) + \\ & + ({}_3h_3 + h_3) * (v_0, \alpha, v_0) > + \\ & + < \alpha, h_2 * (\alpha, \alpha) > + \\ & + < \alpha, ({}_1h_3 + h_3) * (v_0, \alpha, \alpha) + h_3 * (\alpha, v_0, \alpha) + \\ & + h_3 * (\alpha, \alpha, v_0) > + \\ & + < \alpha, h_3 * (\alpha, \alpha, \alpha) > \geq 0 \end{aligned} \qquad (30.)$$

A (30.) egyenlet a négyzetesen integrálható $\alpha(t)$ függvények $\{\alpha(t)\}$ tartományában áll fenn. Ezt a tartományt olyan résztartományokra bontjuk fel, amelyek azonos alakú, de különböző nagyságú hullámokból állnak:

$$\{\alpha_0(t)\} = \{\alpha(t) | \alpha(t) = x\alpha_0(t)\} \qquad (31.)$$

ahol $\alpha_0(t)$ a tartományt generáló függvény, x tetszőleges, véges valós szám. A (30.) egyenlőtlenségnek minden $\alpha_0(t)$ és x esetén teljesülnie kell. Ezért a (30.) egyenlőtlenséget a következő alakba lehet átírni:

$$\epsilon_0 - \epsilon = a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 \geq 0 \qquad (32.)$$

ahol

$$\begin{aligned} a_1 = {} & - < \alpha, i_S > + \\ & < \alpha, ({}_1h_1 + h_1) * v_0 > + \\ & < \alpha, ({}_1h_2 +_2 h_2 + h_2) * (v_0, v_0) > + \\ & < \alpha, ({}_1h_3 +_2 h_3 +_3 h_3 + h_3) * (v_0, v_0, v_0) > \end{aligned} \qquad (33.)$$

és a (30.) egyenlőtlenség alapján az a_2, a_3 és a_4 együtthatók is felírhatók. A (32.) egyenlőtlenségnek minden x értékre teljesülnie kell. Ez $|x| << 1$ esetén csak úgy állhat fenn, ha

$$a_1 = 0 \qquad (34.)$$

azaz (33.) alapján

$$\begin{aligned} & - < \alpha, i_S > + \\ & < \alpha, ({}_1h_1 + h_1) * v_0 > + \\ & < \alpha, ({}_1h_2 +_2 h_2 + h_2) * (v_0, v_0) > + \\ & < \alpha, ({}_1h_3 +_2 h_3 +_3 h_3 + h_3) * (v_0, v_0, v_0) > = 0 \end{aligned} \qquad (35.)$$

A (34.) egyenletből következik, hogy a (32.) egyenlőtlenség a következőképpen módosul:

$$\epsilon_0 - \epsilon = a_2 x^2 + a_3 x^3 + a_4 x^4 \geq 0 \qquad (36.)$$

Ez utóbbit átalakítva

$$a_4 x^2 \left[\left(x + \frac{a_3}{2a_4} \right)^2 + \frac{4a_2 a_4 - a_3^2}{4a_4^2} \right] \geq 0 \qquad (37.)$$

mely akkor és csak akkor áll fenn x minden értéke esetén, ha

$$a_4 \geq 0 \qquad (38.)$$

és

$$4a_2 a_4 - a_3^2 \geq 0 \qquad (39.)$$

A (38.) egyenlőtlenség a következő alakban is felírható:

$$< \alpha, h_3 * (\alpha, \alpha, \alpha) > \geq 0 \qquad (40.)$$

Ez a [6], [7] referenciákban említett „energia-elnyelési kritérium"-nak a vizsgált esetre történő általánosítása. A 2. ábrán látható áramkört leíró egyenlet:

$$\begin{aligned} & -i_S + (h_{L1} + h_1) * v_0 + \\ & (h_{L2} + h_2) * (v_0, v_0) + \\ & (h_{L3} + h_3) * (v_0, v_0, v_0) = 0 \end{aligned} \qquad (41.)$$

A (35.) és a (41.) egyenlet összehasonlításával a [6], [7]-ben említett „adjungált illesztési kritérium" általánosítását kapjuk meg:

$$h_{L1} =_1 h_1 \qquad (42.)$$

$$h_{L2} =_1 h_2 +_2 h_2 \qquad (43.)$$

$$h_{L3} =_1 h_3 +_2 h_3 +_3 h_3 \qquad (44.)$$

A három utóbbi egyenlet Laplace-transzformáltjával a komplex frekvenciatartománybeli illesztési kritériumokat kapjuk meg:

$$H_{L1} =_1 H_1 \qquad (45.)$$

$$H_{L2} =_1 H_2 +_2 H_2 \qquad (46.)$$

$$H_{L3} =_1 H_3 +_2 H_3 +_3 H_3 \qquad (47.)$$

ahol a következő jelölést vezettük be:

$$H_n(s_1, \ldots s_n) =$$

$$= \int_{-\infty}^{\infty} \ldots \int_{-\infty}^{\infty} h_n(\tau_1, \ldots \tau_n) \prod_{k=1}^{n} (e^{-s_k t_k} d\tau_k) \qquad (48.)$$

Magasabb rendű tagokra kiterjesztve a (24.) egyenletet:

$$f(v) = \sum_{k=1}^{n} h_k * \begin{pmatrix} 1 & \ldots & k \\ v, & \ldots & v \end{pmatrix} \qquad (49.)$$

bármeny pozitív n-re, és a fenti lépéseket megismételhetjük. A (32.) egyenlőtlenséget általánosítva, a globális energia-maximum feltétele a következő:

$$\epsilon_0 - \epsilon = \sum_{k=1}^{n+1} a_k x^k \geq 0 \qquad (50.)$$

Az energia-maximum szükséges feltételei az együtthatókkal kifejezve a következők:

$$a_1 = 0 \qquad (51.)$$

$$a_{n+1} \geq 0 \qquad (52.)$$

biztosítva, hogy n páratlan legyen. Az (51.) egyenlet az adjungált illesztési feltétel tetszőleges, páratlan N-re történő általánosításához vezet:

$$h_{Lk} = \sum_{m=1}^{k} {}_m h_k \qquad (53.)$$

ahol $k = 1, 2, \ldots n$. Az (53.) egyenletet a szimmetrizált magfüggvény bevezetésével a következőképpen egyszerűsíthetjük:

$$\overline{h_{Lk}} = k({}_1\overline{h_k}) \qquad (54.)$$

ahol

$$\overline{h_k} = \frac{1}{k!} \sum h_k(\tau_1, \ldots \tau_k) \qquad (55.)$$

és az összegzés $\tau_1 \ldots \tau_k$ minden permutációjára kiterjed.

Az (53.) és (54.) egyenlet mindkét oldalát Laplace-transzformálva, a komplex frekvencia-tartománybeli illesztési feltételeket kapjuk meg:

$$H_{Lk} = \sum_{m=1}^{k} {}_m H_k \qquad (56.)$$

$$\overline{H_{Lk}} = k({}_1\overline{H_k}) \qquad (57.)$$

A maximum (35.), (38.) és (39.) egyenlettel megadott feltételei szükséges és elégséges feltételek. Azonban az (51.), (52) szerinti feltételek szükséges, de nem elégséges feltételek. Ezért az (53.), (54.), vagy az (56.), (57.) egyenletek csak akkor alkalmazhatók, ha valahogyan már meggyőződtünk arról, hogy a maximum létezik.

Ha a 2. ábra szerinti forrásáramkör rezisztív és

$$f(v) = Kv^n \qquad (58.)$$

ahol $K > 0$ és n páratlan, pozitív egész szám, akkor létezik az optimális terhelés [1]. Az optimális terhelés $i_L = nKv_L^n$ karakterisztikának és a (54.), (57.) egyenletnek az összehasonlítása mutatja, hogy eredményeink a rezisztív hálózatokra vonatkozó eredmények általánosításai.

A generátor kauzalitásából az következik, hogy

$$h_n(\tau_1, \ldots \tau_n) = 0 \quad \tau_k < 0, k = 1, \ldots n \qquad (59.)$$

Az (53.) és (59.) egyenletek a következőt eredményezik:

$$h_{Ln} = 0, \ \tau_k > 0 \qquad (60.)$$

Következésképpen minden realizálható optimális terhelő áramkör, amely Volterra sorral írható le, rezisztív kell legyen. A (42.)-(44.), (45.)-(47.), (53.)-(54.) és (56.), (57.) egyenletek nem kauzális, ezért nem realizálható egykapukat írnak le. A realizáció feladata ezeket kauzális egykapukkal megközelíteni a $j\omega$ tengely egy szakaszán.

A maximális energiát elnyelő terhelés karakterisztikájának zárt alakban történő felírása nagy gyakorlati jelentőségű. Nemlineáris generátor esetén a maximális energiát elnyelő terhelés numerikusan csak olyan áramkörtervező program alkalmazásával kereshető meg, amely egyaránt rendelkezik nemlineáris analízis és optimalizálási lehetőséggel, és ezt a kettőt egyidejűleg is lehet alkalmazni. Gyakorlati tapasztalataink szerint azonban ez sem mindig vezet célra. Ugyanis a nemlineáris analízis és az optimalizálás (az ehhez szükséges deriváltak előállítása) egyaránt közelítésen alapszik, és ennek a két közelítésnek az egyidejű alkalmazása számos numerikus probléma forrása.

5. KÖVETKEZTETÉSEK ÉS MEGJEGYZÉSEK

Zárt alakú kifejezéseket származtattunk, melyek Volterra-sorral jellemezhető nemlineáris generátorból maximális energiát abszorbeáló, optimális terhelés karakterisztikáját írják le. Az eredményeket az idő- és a komplex frekvenciatartományban adtuk meg. Az energia-maximum létezésének feltételeit is tanulmányoztuk: szükséges és elégséges feltételeket adtunk meg a harmadrendű, és szükséges feltételeket az N-edrendű Volterra-sorral jellemzett generátorok esetére (N páratlan).

Megjegyezzük, hogy a periodikus jelek nem integrálhatók négyzetesen a kétszeresen végtelen időintervallumban. Ezt a problémát a periodikus gerjesztőjelnek véges, de elegendően hosszú darabjának a figyelembe vételével oldhatjuk fel, az átlagteljesítmény és a véges időintervallumra vonatkozó nettó energia kapcsolatának felhasználásával. A vizsgált esetben ezért a „maximális teljesítmény-átvitel" kifejezést is használhatjuk.

HIVATKOZÁSOK

[1] J. L. Wyatt, L. O. Chua: „Nonlinear resistive maximum power theorem, with solar cell application", IEEE Trans. on CAS, Nov. 1983, pp. 824-828

[2] J. Ladvánszky: „On the extension of the nonlinear resistive maximum power theorem I", Proc. of the ISCAS'86, San José, California, May 5-7 1986, pp. 257-259

[3] J. L. Wyatt: „Nonlinear dynamic maximum power theorem, with numerical method", Internal report, Massachusetts Institute of Technology, LIDS-P-1331, 1983

[4] J. Ladvánszky: „Maximum power theorem – a describing function approach", Proc. of the European Conference on Circuit Theory and Design, Paris, France, Sept. 1-4, 1987, pp. 35-40

[5] J. Ladvánszky: „On the extension of the nonlinear resistive maximum power theorem II", Proceedings of the 8th International Colloquium on Microwave Communications, Budapest, Hungary, Aug. 25-28, 1986, pp. 251-252

[6] R. A. Rohrer: „The scattering matrix normalized to complex n-port load networks", IEEE Transactions on Circuit Theory, June 1965, pp. 223-230

[7] R. A. Rohrer: „Optimal matching: A new approach to the matching problem for real time-invariant one-port networks", IEEE Transactions on Circuit Theory, June 1968, pp. 118-124

[8] L. O. Chua, C. Y. Ng: „Frequency domain analysis of nonlinear systems: General theory", Electronic Circuits and Systems, July 1979, pp. 165-185

[9] P. M. Lin: „Competitive power extraction from linear n-ports", IEEE Transactions on Circuits and Systems, February 1985, pp. 185-191

POWER MATCHING IN WEAKLY NON-LINEAR CIRCUITS

J. LADVÁNSZKY

INNOVATION COMPANY FOR TELECOMMUNICATIONS, TKI
H-1142 BUDAPEST, UNGVÁR U. 64-66.
TEL.: 251 0888, FAX: 251 9878, E-MAIL: LADVAN@TKI.HU

The maximum power transfer problem is investigated in the case when the source conductance is characterised by third order Volterra series. Power matching is one of the key problems in electrical engineering. The problem of power matching has arisen in the investigation of telephone lines. That times the "conjugate matching condition" was revealed: In a simple one-port source-load circuit, the load impedance has to be equal to the conjugate of the source impedance for maximum power transfer from the source to the load, at a single frequency. This problem, among several other ones, generated the need for fixed topology equivalents of complicated linear networks for solving analysis problems. The problem of maximum power transfer led also to an alternative definition of the scattering matrix as a useful tool in maximising power efficiency of linear, time invariant, multiport loads. The scattering matrix soon became indispensable in the extension of the maximum power transfer problem for a finite frequency band and its application, the solution of the broadband matching problem. This step was achieved by extending the definition of the scattering matrix for the case of complex normalising impedance at a single frequency, and later on, for the whole complex frequency plane. Since then, several independent solutions to the gain-bandwidth problem are known, and applied in the broadband amplifier and filter design.

The non-linear version of the maximum power transfer problem is first solved in general in the case of the solar cell. The solar cell can be modelled at DC by a circuit whose topology is the same as that of a Norton-like source. However, the extension of the idea of the circuit equivalents to non-linear circuits is much more complicated than that for linear circuits and a general solution does not exist. This latter problem emerged in the inverse maximum power transfer problem when one has to determine the source that delivers maximum power to a given load. Up to this point of our consideration, the non-linear source-load circuit models did not contain memory.

Today the most general, known solution of the maximum power problem is related to non-linear sources with memory. Solutions for some practically important cases of the latter problem are also known, they are the case of severely non-linear, tuned sources and the weakly non-linear sources discussed in this paper.

In addition to all these, several cases of linear, time-invariant, multiport sources are also discussed in the literature. Also, some non-linear versions of the maximum power transfer problem are discussed in terms of wave variables.

We prove that if the source is weakly non-linear, then the load absorbing maximum power is also weakly non-linear: The optimum load can also be described by truncated Volterra series. Closed form expressions are obtained for the load absorbing maximum energy from the non-linear source at arbitrary current and voltage waveforms. Results are given both in the time and the complex frequency domain. Conditions for the energy maximum are also studied: necessary and sufficient conditions for the third order and necessary conditions for the N-th order Volterra sources are given (provided that N is odd).

We would like to emphasise the practical importance of the closed form description of the load that absorbs maximum power from a weakly non-linear source. Without this knowledge the same problem could be treated by circuit analysis programs that are suitable for non-linear analysis and optimisation simultaneously. In such situations, both the analysis and the optimisation are based on approximations (finite number of harmonics and the approximation of derivatives). These two approximations may lead to serious numerical problems that do not exist when the closed form expressions for the optimum load are applied.

All the theoretical solutions of the maximum power problem of sources with memory result in load circuits that are non-causal therefore non-realisable. The way to the realisable solution in the case of linear circuits is known in the literature as interpolation with positive real functions and matrices.

Ladvánszky János a Távközlési Innovációs Rt. tudományos tanácsadója. Okleveles villamosmérnök (1978), a műszaki tudomány kandidátusa (1988), egyetemi doktor (1990). Szakmai érdeklődési köre az elektronikus eszközök áramköri modellezése, a mikrohullámú S-paraméter mérés, az áramkörelmélet, mikrohullámú, majd mikrohullámú-optikai áramkörök tervezésének problémái, köztük a zajcsökkentés és más témakörök. Számos szakmai szervezet, köztük a Híradástechnikai Tudományos Egyesület és a Magyar Tudományos Akadémia Távközlési Rendszerek Bizottságának tagja, huzamosan a Híradástechnika c. lap szerkesztője.

WWW ALAPÚ INFORMÁCIÓS RENDSZER

BODOR ANDRÁS LAJOS és SZABAD TAMÁS

E-MAIL: BANDITA@SCH.BME.HU; E-MAIL: SZABADT@SCH.BME.HU
TEL: (06-1) 463-2815
BUDAPESTI MŰSZAKI EGYETEM
VILLAMOSMÉRNÖKI ÉS INFORMATIKAI KAR, ELMÉLETI VILLAMOSSÁGTAN TANSZÉK MŰSZAKI INFORMATIKA SZAK, 5. ÉVF.
1111 BUDAPEST, EGRY J. U. 18.

Ebben a cikkben egy Internet alapokon működő információs rendszert fogunk bemutatni. Először áttekintjük, hogy milyen feladatokat old meg és milyen hardver-szoftver háttér szükséges a működtetéséhez, majd részletesen ismertetjük az Oracle WebServer felépítését, működését és konfigurálását, amit korábban használtunk. A cikkben kitérünk arra, hogy milyen módszerrel titkosítjuk a világhálózaton áthaladó adatokat, illetve arra, hogy milyen rendszerbe beépített biztonsági korlátokat valósítottunk meg. Egy rövid fejezetben ismertetjük az információs rendszer szolgáltatásait.

1. BEVEZETÉS

1.1. Motiváció

Ma már rengeteg információt kell az egyetemeken, főiskolákon dolgozó előadóknak, oktatóknak, tanároknak, laborvezetőknek valamint a hallgatóknak ismerni, feldolgozni, rendszerezni. A helyzetet tovább nehezíti a levelezős és esti tagozatos hallgatók ügyeinek intézése, az adminisztrációs feladatok elvégzése. Ez régebben sok-sok papírmunkával és idővel járt. Egy ideje már számítógépes feldolgozás segíti a különböző emberek munkáját. A tárgyak, a vizsgák, az oktatók, a hallgatók adatainak és jegyeinek nyilvántartása olyan mennyiségű információt jelentenek, amit már érdemes adatbázisban tárolni. Sok munkát, időt és papírt lehet megtakarítani, ha mindezeket az adatokat egy számítógépes rendszerbe tápláljuk be, és azután a rendszerre bízzuk ezek lekezelését.

1.2. Megoldandó feladatok

Az általunk ismertetendő WWW alapú információs rendszer célja a felsőoktatási intézményekben előforduló információ begyűjtésével, feldolgozásával, továbbításával és rendszerezésével járó feladatok megoldása, megkönnyítése. Tulajdonképpen az adminisztrációs ügyek megoldására szolgáló hardver-szoftver együttesről van szó. Képzeljük csak el, mennyi minden egyszerűsödik le a rendszer használatával. A hallgatók akár otthonról tudnak új információkat megtudni, tárgyakat felvenni, vizsgára jelentkezni stb. Az előadóknak nem kell nagy mennyiségű irattal foglalkozniuk, egy számítógép előtt ülve szinte minden adat egy pillanat alatt rendelkezésükre áll, amire szükségük van. Különösen a keresés, visszakeresés műveletek elvégzése gyorsul fel. Persze ahhoz, hogy a rendszer tökéletesen működjön, biztosítani kell a géppark megfelelő karbantartását, hiba esetén megtenni a hiba elhárítását szolgáló intézkedéseket.

1.3. A rendszer áttekintése

Az Internet alapú rendszer előnye, hogy gyakorlatilag a világ bármely pontjáról elérhető, platformfüggetlen és csupán egy internetes csatlakozásra és egy böngésző programra van szükség a használatához, ez utóbbiak pedig ingyen letölthetők.

A kommunikáció úgy zajlik, hogy a rendszer tárolt eljárásokat futtat le az adatbázisban. A tárolt eljárások választását több szempont is indokolja, mégpedig: a tárolt eljárások gyorsan lefutnak és az adatok helyben vannak, a fejlesztéshez használatos PL/SQL nyelv rugalmassága, nincsenek integritási problémák, valamint könnyű telepíthetőség (egy ugyanolyan típusú adatbázisba).

A tárolt eljárások, ill. függvények ún. csomagokba (package) vannak szervezve, ami azt jelenti, hogy az összetartozó információkat kezelő és funkcionalitásában hasonló eljárások és függvények deklarációja és implementációja egy csomagban van. Ez megkönnyíti a csoportos fejlesztést és az utólagos módosításokat. Ugyanis egyszerre csak egy ember tudja módosítani egy csomag tartalmát, a többiek által beírt változtatások felülíródnak. Az pedig nyilvánvaló, hogy az eljárások csoportosítása kisebb egységekre növeli az átláthatóságot.

Egy igazán komplex szoftver esetén, de még egy kevésbé bonyolult szoftvernél is nagyon nehéz a teljes rendszer áttekintése. A hallgatói információs rendszer is már eléri azt a bonyolultsági fokot, ahol már nem lehetséges az egész rendszer átlátása. Szükséges volt tehát a megoldandó feladatok alapján a rendszert kisebb egységekre, modulokra osztani. A teljes hallgatói információs rendszer két fő részből áll, ezek a hallgatói modul és a tanszéki modul.

A rendszer kifejlesztésében még két hallgató vett részt, Bak Attila és Gál Richárd. A megjelenítés tervezését két weblaptervező végezte el a mi igényeink alapján.

1.3.1. Infrastruktúra

A rendszer megvalósításához szükséges infrastruktúra tartalmaz egy adatbázisszervert, egy vagy több webszervert és egy hálózatot a felhasználók gépeivel. Az adatbázisszerver és a webszerver (ha csak egy van) lehet egy gépen is, de ajánlott külön számítógépeket alkalmazni. A felhasználói hálózat felépítésére csupán az a megkötés, hogy biztosítsa a TCP/IP (Transmission Control Protocol/Internet Protocol) használatát.

1.3.2. Szoftver háttér

A WWW alapú információs rendszer számítógép hálózatokon működik a TCP/IP felhasználásával. Működtetéséhez kell egy adatbázis-kezelő program, egy webszerver és egy internetböngésző program. Ha a titkosítást is igénybe akarjuk venni, akkor szükségünk lesz még egy biztonságos kapcsolatot nyújtó titkosító szerverre is.

Ha a webszerver képes a tárolt eljárásokat automatikusan meghívni a nevük és paraméterlistájuk alapján, akkor nincsen szükség más szoftverre. Ha viszont nem az Oracle webszerverét alkalmazzuk, akkor ezt egy, pl. CGI (Common Gateway Interface) nyelven megírt programmal kell megoldani, ami fogadja a böngésző program hívását, elvégzi a csatlakozást az adatbázishoz, átadja a paramétereket, ott lefuttatja a kívánt tárolt eljárást, majd visszaadja az eredményt a böngésző programnak. A fejlesztés során mi elkészítettük ezt a CGI-programot. A webszerver és a CGI összekonfigurálását lásd a 2.4. alfejezetben.

1.3.4. Többnyelvűség

Többnyelvűnek nevezzük azt a szoftvert, ahol egy újabb nyelv bevitele, ill. egy nyelv kivétele nem jár a megírt programkód módosításával. Célszerűen tehát adatbázisban, vagy erőforrás állományokban kell a pusztán nyelvi, szöveges információkat elhelyezni.

A rendszer fejlesztése alatt felmerült, hogy különböző nyelven kellene megjeleníteni az információkat. Mivel a nyelvfüggő információk nagy része a HTML oldalakon van, ezért sok helyen elegendő volt a HTML oldalakat sokszorosítani és átírni a kívánt nyelvre. A hibaüzenetek és a felhasználónak szóló üzenetek tárolásánál az első fajta megoldás volt a célravezető, tehát az adatbázisban helyeztük el a különböző nyelvű szövegeket. Az üzeneteket egy-egy azonosítóval láttuk el és az adott nyelv kódjával letároltuk egy táblában. A visszakeresés így nagyon egyszerű, egy adott üzenet lekérdezése adott nyelven egyetlen lekérdező utasítással elvégezhető. Meg kell azonban jegyezni, hogy az adatbázisban eltárolt adatok csak azon a nyelven jeleníthetők meg, ahogyan azok tárolásra kerültek.

A rendszerbe való belépés előtt a felhasználó kiválaszthatja az általa preferált nyelvet, és attól fogva az oldalak az adott nyelven fognak megjelenni. Ennek megvalósítására az adatbázisban hoztunk létre egy külön táblát, ami a felhasználóval kapcsolatos információkat tárolja. Amikor egy új HTML oldalt kell megjeleníteni, a megfelelő tárolt eljárás az egyedi felhasználói azonosító által kiválasztott adatokat veszi ki az adatbázisból, ahol többek között el van tárolva a kiválasztott nyelv is. Ezáltal lehetővé válik, hogy a következő oldal, csupán egyszeri kezdeti beavatkozással, automatikusan a kiválasztott nyelven jelenjen meg.

2. A RENDSZER FELÉPÍTÉSE

2.1. Bevezetés

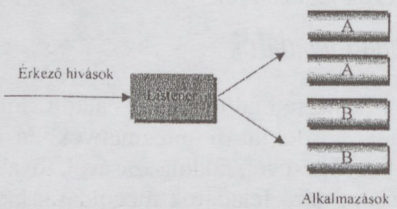
A rendszerünk egy Oracle adatbázis szerverben lett implementálva. Szót ejtünk az Interneten érkező kéréseket kiszolgáló webszerverekről, a Netscape Fasttrack Serverről és főleg az Oracle WebServerről, amellyel mi is behatóbban foglalkoztunk. A következőkben tehát leírjuk, hogyan teljesíti a webszerver a kliensek kéréseit az adatbázissal kapcsolatban. Előre is elnézést kell kérnünk, ha néha megtartottuk az angol nyelvű terminológiát, de az angol kifejezések jelenleg jobban elterjedtek, és sok esetben még nincs rájuk megfelelő magyar szó.

2.2. Az Oracle WebServer

Az Oracle WebServer egy Hypertext Transfer Protocolt (HTTP) használó Internet szerver, amely egyrészt független adatbázis-hozzáférést, másrészt hatékony fejlesztői környezetet nyújt. Ha a WebServer egy Uniform Resource Locator (URL) hívást kap egy – vagy a World Wide Weben vagy a lokális hálózaton elhelyezkedő – böngészőtől, akkor szükség szerint az adatbázishoz vagy az operációs rendszer fájlrendszeréhez nyúl a kérés teljesítéséhez. A fájlrendszeren található adatok vagy CGI-scriptek, melyek nem férnek adatbázishoz statikus weboldalak, míg az adatbázis segítségével generált oldalak dinamikusan felépülő „élő" weboldalak felépítésére alkalmasak.

A Web Listener a WebServer azon része, ami a webböngészőtől az URL-t megkapja, majd a megfelelő kimenetet visszaküldi. Amikor a Web Listenerhez az URL beérkezik, az eldönti, hogy szükség van-e a kérés teljesítéséhez valamilyen WebServer szolgáltatás igénybe vételére. A szolgáltatás igénybe vétele történhet a Web Request Brokeren (a továbbiakban WRB, részletesebben ld. az ezzel foglalkozó fejezetet) keresztül, a Common Gateway Interface (a továbbiakban CGI) felületén keresztül, esetleg a gép fájlrendszerén – amelyen a Web Listener található – keresztül. Amennyiben a WRB hozzáférés igénye felmerül, a Listener továbbadja a kérést a WRB Dispatchernek feldolgozásra, majd tovább folytatja eredeti feladatát, vagyis figyel a beérkező HTTP kérésekre.

A WRB Dispatcher – amiről később még bővebben lesz szó – olyan kérésekkel foglalkozik, melyek a WRB executable engine-en keresztül folynak le. Minden WRB végrehajtó példány (WRBX) kapcsolódik egy végfelhasználói alkalmazáshoz a WRB API (Application Programming Interface)-n keresztül. Ezeket az alkalmazásokat WRB cartridge-oknak nevezzük. A WRB API struktúrájából kifolyólag alkalmas külső, saját tervezésű cartridge-ok kéréseinek kiszolgálására (1. ábra).



1. ábra. A Listener feladata a WebServerben

2.2.1. A Web Listener

Az Oracle Web Listener egy olyan HTTP eszköz, amely a webböngészők hipermédia dokumentumok iránti kéréseinek kiszolgálására használatos. Most a Web Listener főbb jellemzőiről fogunk néhány szót ejteni.

Hálózati kommunikációban a Web Listener egy adott IP cím/port konfigurációban fogadja a böngészők kéréseit. Fizikailag ugyanazon a gépen egyszerre több Web Listener folyamat is futhat. A port egy szám, amit a TCP protokoll használ egy kommunikációs csatorna azonosítására, amely egy programmal van összeköttetésben. Például a login program szokás szerint a 49-es porton, a Domain Name Service az 53-as porton fogadja a hívásokat. Az Oracle Web Listenernél elterjedt szokás szerint egy átlagos kapcsolatot a 90-es porton, míg egy biztonságos kapcsolatot a 443-as porton kezdenek meg felépíteni. Az 1-1024-ig terjedő portokra csak root joggal futtatott programok, míg 1024-től 65535-ig terjedő portokra bármilyen programok kapcsolódhatnak.

Természetesen az IP cím egyedi azonosító, mellyel pontosan egy gépet címezhetünk meg az Interneten, de egy gép akár több IP címmel is rendelkezhet. Egy gép így különböző célokra különböző IP címeket használhat. Például egy gép egyik IP címével mondjuk egy e-mail routing szerverként működhet, egy másik címen pedig DNS (Domain Name Server)-ként szolgál. Azt, hogy az egyedi karakterlánc, mellyel egy gépet a hálózaton megcímeztünk valójában milyen IP címen van, azt egy ún. Domain Name Service tartja fenn. Ez egy adatbázis, mely a gépnevekhez IP címeket rendel. Az ehhez való hozzáférés a DNS-en keresztül lehetséges.

A kliensek számára elérhető fájlokat az Oracle Web Listener egy úgynevezett virtuális fájlrendszerben kezeli. Ez a virtuális fájlrendszer összerendeli a webszerver gép valós fájlrendszer egy elérési útját a hívott URL-lel. Ezen kívül a Web Listener kihasználja a gép operációs rendszerének fájl-memória összerendelési képességét. Így amikor egy kliens lekér egy fájlt, a Web Listener virtuális címterülete a fájl tartalmára mutat. Ezzel gyorsabbá lehet tenni a hozzáférést, és lehetővé teszi több kliens számára a fájlnak ugyanazt a másolatát használni, így a Listener takarékoskodni tud saját memória erőforrásával.

Normális esetben, mikor a Web Listener megnyit egy lekért fájlt, az a memóriában marad, egészen addig, amíg az összes kliens, ami használta a fájlt befejezi vele kapcsolatos tevékenységét. Ekkor a Web Listener bezárja a fájlt, majd felszabadítja az általa lefoglalt memóriaterületet. A Web Listener számunkra is lehetővé teszi a fájlok cache-elését. Egy ilyen fájl megnyitása után az egész Web Listener folyamat befejezéséig a memóriában marad. Ezzel optimalizálni lehet a fájlhozzáférési időket.

A Web Listener lehetővé teszi ezeken túl még virtuális fájlok vagy könyvtárak biztonságosabbá tételének érdekében a belépők autentikálását és/vagy korlátozását. Ha egy fájl vagy könyvtár autentikálással van védve, akkor a kliensnek szolgáltatnia kell egy érvényes felhasználónevet a hozzá tartozó jelszóval. Lehetőség van felhasználói csoportok kialakítására, sőt csoportok összefogására is, ezeket „realm"-nek nevezik. Ezt a felhasználó, csoport vagy „realm" felhasználót aztán hozzárendelhetjük bizonyos virtuális fájlrendszerekhez, vagy könyvtárakhoz. A Web Listener kétfajta autentikációs sémával rendelkezik: „basic" és „digest". A különbség a két autentikációs metódus között csupán annyi, hogy digest módban a kliens és szerver közötti utat a jelszó titkosítva teszi meg (a titkosítást digestnek nevezik). Néhány régebbi webböngésző nem támogatja még az ilyen digest autentikációs módot, de amikor csak lehetséges, saját érdekünkben ajánlott ennek a metódusnak a használata. A korlátozó sémával védett fájlokhoz vagy könyvtárakhoz a Web Listeneren keresztül csak bizonyos engedélyezett gépek vagy gépcsoportok férhetnek hozzá. Korlátozó sémából is kétfajta van, az IP alapú korlátozás és a Domain alapú korlátozás. Az IP alapú korlátozás csak bizonyos IP címmel rendelkező gépek hozzáférését engedélyezi, míg a Domain alapú korlátozással, DNS alapján, gépeket, illetve domainen belüli gépcsoportokat engedélyezhetünk.

Az Oracle Web Listener egy dokumentum különböző formátumú példányait is képes nyilvántartani, és a kliens által kívánt formátumot a rendelkezésére bocsátani. Például, ha egy kliens egy dokumentumot magyar nyelven kíván lekérni, akkor a Listener ellenőrzi, hogy tárol-e belőle ilyen példányt. Amennyiben igen, akkor a Listener visszaadja a kívánt dokumentumot, ellenkező esetben pedig az alapbeállításnak megfelelő nyelvű példányt. Hasonló módon a kliens Multipurpose Internet Mail Extension (MIME) típusban is kérheti a dokumentumot, és amennyiben a gépen megtalálható a keresett verzió, a Web Listener visszaadja azt, ellenkező esetben pedig a legkisebb méretű verziót.

A Web Listener képes tömörítő programok által kódolt dokumentumok kezelésére is. Például, ha egy kliens ki tud egy „gzip"-pel tömörített dokumentumot csomagolni, akkor a Web Listener az eredeti dokumentum helyett annak tömörített változatát bocsátja rendelkezésére, és így lecsökkenti az átviteli időt. A fájlformátumok azonosítását egyébként a Web Listener is a kiterjesztés alapján végzi.

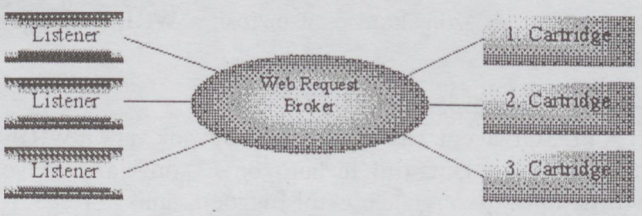
A Web Listeneren keresztül lehetővé válik a dinamikus dokumentum-generálás. Ez több módon lehetséges. Az egyik mód az általunk felhasznált Web Request Brokeren keresztül a PL/SQL Agent igénybe vételével egy adatbázishoz való kapcsolódás, és az ottani tárolt eljárások futtatása, a másik lehetséges mód a Common Gateway Interface-en keresztül a fájlrendszeren elhelyezkedő programok futtatása [3].

2.2.2. A Web Request Broker

Az Oracle Web Listener képes egy olyan interfészt biztosítani, mint az Oracle Web Request Broker, amelynek segítségével a kliensek programokat futtathatnak a szerver gépen, és így az adatokhoz sokkal hatékonyabban férnek hozzá, mint CGI-n keresztül. Hogy ez lehetővé váljon, a Web Listener a hozzá beérkező ilyen kérést a WRB Dispatchernek adja tovább, amely kiválasztja, hogy az aktuális kérést a futó processzei közül melyikhez rendelje. Ebben a részben ezt a mechanizmust fogjuk megvizsgálni.

A Web Request Broker az Oracle WebServer központi része. Aszinkron módon teljesíti a hozzá beérkező kéréseket egy API (Application Programming Interface) segítségével, amellyel lehetővé válik az ún. WRB Cartridge-ok elérése. Olyan architektúrát nyújt ezzel, amellyel szerver oldali webalkalmazásokat lehet futtatni a WRB-t tartalmazó HTTP szerveren.

A Web Request Broker hasonló lehetőségekkel rendelkezik, mint a CGI-scriptek. A WRB API-n keresztül hozzá lehet férni kliens által küldött CGI adatokhoz, de a WRB alkalmazások, amelyeket WRB Cartridge-oknak nevezünk, kihasználják a WRB több folyamatos (multi process) architektúráját, így ezek használatával a CGI-nél jobb eredményeket érhetünk el (2. ábra).



2. ábra. WRB a WebServer központi része

Ha egy Web Listener egy olyan URL kérést kap, mellyel a WRB-t címezték, átadja a kérést a WRB Dispatchernek. A Dispatcher eldönti, hogy a kérést melyik cartridge tudná

teljesíteni, majd átadja annak. Ennek eredményeképpen a Listener csak fogadja és ellenőrzi a beérkező URL-eket, majd minden kérést ezután egy a háttérben futó folyamat teljesít. A következő típusú WRB cartridge-ok léteznek:

- A PL/SQL Agent: Ez a cartridge hajtja végre az adatbázisban a PL/SQL utasításokat. Összehasonlítva a Java Cartridge-vel, jobb az adatbázis-elérési képessége, de nincs meg ugyanaz az erős funkcionalitása.
- A Java Cartridge: Ezzel a szerveren lévő java programokat lehet végrehajtani dinamikus weboldalak generálásához. Ezt a cartridge-ot használva lehet Javan belül PL/SQL utasításokat végrehajtani.
- LiveHtml: Ennek segítségével a weboldalainkra irányíthatjuk bármilyen program kimenetét, melyet az operációs rendszer végre tud hajtani.
- Saját cartridge: Mivel a WRB API-t használ, mi is írhatunk saját cartridge-ot. A WRB Cartridge-ok fejlesztési nyelve a C. A jövőben a tervek szerint más nyelveken is lehet majd WRB API alá fejleszteni.
- Egyéb cartridge: Ismét csak az API révén bármilyen harmadik fél által írott cartridge-ot felhasználhatunk.

A WRB architektúra a következő elemekből épül fel:

- WRB Dispatcher,
- WRB Cartridge-ok,
- WRB Application Engine,
- WRB végrehajtó példányok (WRBXs).

A WRB Cartridge-ről már volt szó, osztott könyvtárként van implementálva, és WRB API-t használ a kliensek igényeinek kielégítésére.

A WRB Dispatcher a Web Listener és a WRB cartridge-ok közötti kapcsolatot biztosító program. Amikor a Web Listener megkap egy HTTP kérést egy WRB cartridge-nak címezve, továbbadja azt a WRB Dispatchernek. A Dispatcher az URL-ben hivatkozott út és kiterjesztés alapján eldönti, hogy melyik cartridge-nak kell tovább küldeni a kérést. Azt, hogy melyik elérési út melyik cartridge-vel van kapcsolatban, az a webszerver konfigurálása során dől el, amelyről a később még részletesen szólunk.

Ez után a WRB Dispatcher kiválaszt a cartridge-on belül egy WRBX-et, hogy teljesítse a kérést. A cartridge-oknak különböző számú WRBX példánya lehet, amelyek az aktuális igény szerint születnek és terminálódnak. Egy minimum számú WRBX példány azonban állandóan fut, így a legtöbb kérés kielégítéséhez nem szükséges új folyamat indítása. A WRBX két fő részből áll: a WRB Application Engine egy másolatából és egy WRB Cartridge osztott könyvtárából. A WRB Application Engine egy futtatható program, amelyben a WRB API implementálva van. Biztosítja a kapcsolatot a WRB cartridge-ok és a WRB Dispatcher között, és szolgáltatásokat biztosít a WRB cartridge-ok számára [4].

2.2.3. A PL/SQL Agent

A PL/SQL agent, vagy másképpen ügynök vagy a WRB-n vagy CGI-n keresztül hívható be a könyvtár-, illetve MIME típus-összerendelésektől függően, amit a WebServer adminisztrátora állít be. Ha egy CGI-t hívunk meg, az URL-ben „owa"-nak kell állnia, ha a WRB-hez kapcsolódunk, akkor a beállított összerendelések elégségesek, hogy specifikálják a PL/SQL ügynököt. A PL/SQL ügynök feladata, hogy végrehajtsa a PL/SQL kódot, majd a kapott eredményt HTML formában visszaadja a Web Listenernek, ami továbbítja azt a kliens felé.

A PL/SQL eljárások az adatbázisban tárolódnak, melyeket a PL/SQL ügynök hív meg az adatbázisnak megadott utasításokkal, utána végrehajtja a kódot, majd a kimenetet és az esetleges üzeneteket visszaadja a PL/SQL ügynöknek.

Mivel a PL/SQL az adatbázisban hajtódik végre, a PL/SQL ügynöknek akár CGI-n akár a WRB-n keresztül kapcsolódnia kell az Oracle adatbázishoz. Amennyiben WRB-t használ az ügynök, akkor a WRBX példány a következő két lépésben kapcsolódik az adatbázishoz:

- A kapcsolat felépítése. A WRBX ezt létrehozása pillanatában megteszi.
- Belépés az adatbázisba. Ez azért külön lépés, mert a WRBX példány ezt addig nem teszi meg, amíg egy kérés nem érkezik. Minden adatbázisba érkező kérés így külön munkafázissal (session) fog rendelkezni. Ha a kérést teljesítette, akkor a WRBX kilép az adatbázisból, de a kapcsolatot fenntartja.

Egy általunk is tapasztalt következménye ennek az architektúrának, hogy ha az adatbázis vagy a gép, amelyen az adatbázis elhelyezkedik, valamilyen oknál fogva leáll, akkor az Oracle WebServer azon Listenerje, amelyik ehhez az adatbázishoz kapcsolódott, menthetetlenül lefagy. A listener szolgáltatást sem leállítani, sem újraindítani nem lehet. Az adatbázis újraindítása után, még ha a webszervert is megállítjuk és újraindítjuk, akkor sem lehet a listener folyamatba életet lehelni, ezen csak a webszerver gép újraindítása segít. A tanulság az, hogy hacsak lehetséges, állítsuk le a Listenert az adatbázis leállítása előtt.

Visszatérve a WRB-n keresztüli hívásra, mivel az első lépés jóval több időt vesz igénybe, ezt a technológiát használva jóval gyorsabban visszakaphatjuk egy kérés eredményét a WebServertől, pedig közben úgy tűnik, minden kérés egymástól függetlenül építi fel a kapcsolatot az adatbázissal. Ha a CGI-n keresztül kerül meghívásra a PL/SQL ügynök, minden egyes kérés teljesítésekor az egész procedúrán végig kell menni, ami alaposan meglassítja a válaszidőt.

Az URL-lel, amellyel a PL/SQL ügynök meghívásra került, kijelölünk egy DAD-t (Database Access Descriptor az Oracle WebServer 3-nál, 2-es verzióban ezt még DCD-nek hívták, Database Connection Descriptornak). Ez egy olyan, az operációs rendszeren lévő fájl, amit a WebServer tart karban és az adatbázissal való kapcsolat-felépítéshez szükséges információkat tartalmazza. Ilyenek például a felhasználó neve, jelszava, az adatbázis azonosítója a lokális gépen, stb. A DAD alapján kapja meg a PL/SQL ügynök az adatbázis aktuális sémájában végrehajtható művelethez szükséges jogosultságot.

Az eddigiekben bemutattuk, hogyan kezelődik le egy kliens böngészőjétől érkezett kérés az Oracle WebServerben. Ezek után néhány szót ejtünk még az Oracle támogatásáról a webes felületek készítésében PL/SQL ügynökön keresztül, majd ismertetjük az általunk megvalósított rendszer felállításakor végzett lépéseket, a szerzett tapasztalatokat.

2.2.4. A PL/SQL WebToolkit

Hogy könnyebbé tegye webes alkalmazások készítését

az Oracle WebServer speciális csomagokat biztosított, melyeket használva generálhatunk Oracle adatbázisban tárolt adatokra épülő dinamikus a weboldalakat. Ezeket gyűjtőnéven PL/SQL WebToolkitnek nevezik. E csomagoknak a felhasználásával saját eljárásaink is egyszerűen jeleníthetnek meg adatokat a Weben. Az egyetlen feltétel, hogy a mi tárolt eljárásaink ugyanabban a sémában legyenek az adatbázisban, mint amelyben a PL/SQL WebToolkit csomagjai, így ugyanis eljárásaink belsejéből közvetlenül tudunk rájuk hivatkozni. Ezt a technikát használva tehát az adatbázisban lesznek tárolva a weboldalaink, ugyanott, ahol az eljárásaink is futnak. Ez a rendszer gyorsabb, biztonságosabb és hordozhatóbb annál a módszernél, ha a „minden legyen a kliensnél" elvet követjük. Ezt a rendszert kibővítve mi még egy külön makrózó eljárást használtunk fel, így egyszerűbb lett a tárolt eljárások írása, és a HTML oldalak és a tárolt eljárások szétválasztása. Ezenkívül lehetővé válik a HTML szabvány fejlesztésével az oldalak újratervezése a kód módosítása nélkül.

Ha nincsenek meg a PL/SQL WebToolkit működéséhez szükséges csomagok az adatbázisban, akkor a WebServer DAD adminisztrációs oldalán beállíthatjuk, hogy fel akarjuk installálni őket, így a szükséges csomagok bekerülnek az adatbázisba.

A PL/SQL WebToolkit működésének áttekintése

A működés központjában a HTP és a HTF nevű csomagok állnak. Minden HTP csomagban szereplő HTML tagot generáló eljárásnak megfeleltethető, egy a HTF csomagban szereplő függvény ugyanolyan névvel és paramétersorral. A különbség az, hogy a függvény visszaadja a kimenetét arra a pontra, ahonnan az meg lett hívva, így könnyen beágyazható más eljárásokba vagy függvényekbe. A kiindulási értékkel szereplő paraméterek opcionálisak [5].

Hypertext eljárások (HTP csomag)

Egy hypertext eljárás egy olyan sort generál egy HTML dokumentumban, amely a nevében benne van. Például a htp.anchor eljárás egy link tagot generál. A HTP eljárásai a következő kategóriák alapján csoportosíthatók.

- kiíratő eljárások,
- HEAD taggal kapcsolatos eljárások,
- általános BODY tagok,
- listázó tagok,
- karakterformázó tagok,
- általános megjelenítést formázó tagok,
- formokkal kapcsolatos tagok,
- táblázattal kapcsolatos tagok.

Hypertext függvények (HTF csomag)

A hypertext függvény azzal a HTML taggal tér vissza, ami maga a függvény neve. Magában egy HTF függvénynek a meghívása mégsem elegendő, mivel a HTML tag még nem kerül vissza a PL/SQL ügynökhöz. Egy HTF függvény kimenetét még a HTP csomag print eljárásának kell továbbadni, hogy valóban egy HTML dokumentum részévé váljon. Minden hypertext függvénynek van egy megfelelő hypertext eljárás párja ugyanazzal a névvel, paramétersorral és funkcióval. A HTF csomag függvényei általában csak akkor használhatók, ha valamilyen hívásba kell őket ágyazni.

OWA eszközök (OWA_UTIL csomag)

Ebben a csomagban jól felhasználható eljárások és függvények vannak implementálva. A csomag a következő részekből áll:

- HTML eszközök: felhasználhatók az aláírás (signature) tag HTML oldalra való kiíratásától kezdve CGI környezeti változók értékének a visszavételén át URL átirányításokig.
- Dinamikus SQL eszközök: segítségükkel a weboldalon dinamikus SQL kódgenerálásra van lehetőség.
- Dátum eszközök: könnyebben kezelhetővé teszi a dátum formátumot, amelyek a HTML nyelvben sztringek, viszont az ORACLE adatbázisban külön adattípusként vannak kezelve.

2.3. A PL/SQL nyelv

A PL/SQL nyelv az SQL nyelv kibővített változata, lehetőség nyílik vele alkalmazások fejlesztésére. Az SQL nyelvet standard programozási eszközökkel bővítették ki, többek között:

- moduláris struktúra,
- folyamat-szabályozó utasítások és ciklusok,
- változók, konstansok és típusok,
- strukturált adatok,
- testre szabható hibakezelés.

A PL/SQL nyelv alapvető tulajdonsága, hogy a programkód közvetlenül az adatbázisban tárolódik [1]. Ezzel lehetővé válik több felhasználó számára ugyanazon eljárások és függvények használata. Amint egy adott kódrészlet bekerül a memóriába, akárhány felhasználó dolgozhat ugyanazon a példányon párhuzamosan (bár úgy viselkedik a program, mintha minden felhasználó külön példánnyal dolgozna). Ezen kívül a PL/SQL segítségével „triggereket" definiálhatunk az adatbázisban, amelyek olyan programok, melyeket az adatbázisban bekövetkezetett események válthatnak ki.

A programokban nem lehetnek utalások olyan objektumokra, melyek még nem léteznek, ezért az SQL nyelv egy részét kihagyták a PL/SQL-ből. Ilyen például a DDL (Data Definition Language) utasítások, mint például a CREATE TABLE, vagyis amelyekkel objektumokat hozhatunk létre. Ennek ellenére használhatunk bizonyos típusú futási idő alatt fordítódó kódot a DBMS_SQL csomagban lévő eljárások felhasználásával.

Ha tárolt eljárásokat akarunk létrehozni, akkor akárcsak más adatbázis objektumok esetében, a CREATE parancsot kell használnunk. Létrehozhatunk eljárásokat, függvényeket, illetve csomagokat. Egy csomag tetszőleges számú függvény és eljárás gyűjteménye külön deklarációs és definíciós résszel. Az általunk készített rendszer is ilyen tárolt eljárásokban található. Futtatásuk 2.2. fejezetben van bővebben leírva.

Az adatok lekérdezését sok helyen kurzorral oldottuk meg. Nem érdektelen tehát néhány szót szólni a PL/SQL nyelvben felhasználható kurzorokról.

Az Oracle munkaterületeket használ az SQL utasítások végrehajtásához és a feldolgozáshoz szükséges információk tárolásához. Egy PL/SQL struktúra, amit kurzornak nevezünk, teszi lehetővé, hogy megnevezzünk egy munkaterületet és elérjük a benne tárolt információkat. Kétféle kurzor létezik: implicit és explicit. A PL/SQL implicit mó-

don minden adatmanipulációs utasításhoz hozzárendel egy kurzort, beleértve azt a lekérdezést is, ami csak egy sort ad eredményül. Azokhoz a lekérdezésekhez, amik több sorral térnek vissza, explicit kurzort lehet deklarálni, amivel soronként dolgozhatjuk fel az adatokat. Pl.

```
DECLARE
  CURSOR c1 IS
    SELECT empno, ename, job FROM emp
    WHERE deptno = 20;
```

Egy PL/SQL program úgy működik, hogy megnyitja a kurzort, feldolgozza a sorokat, amiket a lekérdezés visszaadott, majd lezárja a kurzort. Egy többsoros lekérdezés sorainak halmazát eredményhalmaznak nevezzük. Ennek a mérete azoknak a soroknak a száma, amik teljesítik a keresési feltételeket.

Végezetül néhány szó az eljárásokra adható jogokról. Ahhoz, hogy a tárolt eljárásainkat futtathassa egy felhasználó, rendelkeznie kell a futtatási (EXECUTE) joggal. Ezután az eljárás már azokkal a jogokkal rendelkezik, amilyennel létre lett hozva, nem pedig az aktuális futtató jogával. Így nem kell olyan jogokat a felhasználóhoz hozzárendelni, amelyek az eljárás hatáskörén kívül esnek. Ennek akkor van jelentősége, ha az eljárás más eljárásokat vagy függvényeket hív meg, amikre az adott felhasználónak nincs futtatási joga. Hogy bármely felhasználó számára futtathatóvá tegyünk egy eljárást, az EXECUTE jogot biztosítani kell a PUBLIC nevű felhasználó számára az adott eljárásra.

2.4. A rendszer konfigurálása, indítása

Ebben a részben a rendszer indításának körülményeiről, a kezdetekben szükséges teendőkről lesz szó. A konfiguráláskor szükségünk van egy futó Oracle adatbázis szerverre (7-es vagy 8-as verzió), egy Oracle WebServerre (2-es vagy 3-as verzió), vagy egy másik webszerverre és az általunk megírt CGI-programra, egy érvényes felhasználó/jelszó kombinációra és az adatbázisban a felhasználóhoz tartozó futtatható tárolt eljárásokra. Az Oracle WebServeren történő beállítások elvégzéséhez adminisztrátori jogkörrel kell rendelkezni. A titkosítás működéséhez fel kell még használnunk egy Netscape Fasttrack Servert is, mivel a PL/SQL ügynök a 3-as Oracle WebServerben nem támogatja az SSL titkosítást az Oracle Listeneren keresztül. Ha Oracle WebServert használunk, a konfigurálása során a következő lépéseket kell elvégeznünk:

- DAD (vagy DCD) állomány létrehozása, ebből a WebServer tudni fogja az adatbázis helyét, illetve az adatbázisba belépő felhasználó nevét, jelszavát és jogosultságát.
- A PL/SQL ügynök létrehozása, mely a már létező DAD (vagy DCD) állomány alapján fog a WRB-n keresztül az adatbázishoz csatlakozni.
- A WRB konfigurálása: a virtuális könyvtár-összerendelés elvégzése, vagyis a létrehozott PL/SQL ügynökhöz tartozó URL megadása.
- A Web Listener konfigurálása.
- Az SSL alapú titkosítás használatához, az Oracle WebServert futtató gépre még egy Netscape Fasttrack Servert is kell installálnunk. A titkosító szerver konfigurálása után az Oracle WebServeren a „Register External Listener" opció alatt a Netscape szerver listenerét kell felhasználni. Ezzel a módszerrel csak a Web Listenert cseréltük le, így a WRB és az ügynök munkájában nem történik változás. Ha a Netscape szerveren bekapcsoljuk a titkosítást, a dokumentumaink 40 bites szimmetrikus titkosító algoritmussal lesznek kódolva. Hogy a titkosítás pontosan hogyan működik arra a cikkben még bővebben kitérünk.

Ha a CGI-programot akarjuk használni az egyébként drága Oracle WebServer helyett, akkor célszerű a Netscape Fasttrack Servert installálni, ami nem csak a titkosítást látja el, hanem webszerverként is működik. A Netscape webszerveren be kell kapcsolni a titkosítást, és azt, hogy a CGI-programokat melyik könyvtárban keresse. Ezek után a tárolt eljárások futtatására vonatkozó kérések teljesítését a CGI-program végzi, míg az adatok titkosítását a böngésző program és a webszerver között a Netscape Fasttrack Server.

3. A RENDSZER RÖVID BEMUTATÁSA ILLUSZTRÁCIÓKKAL

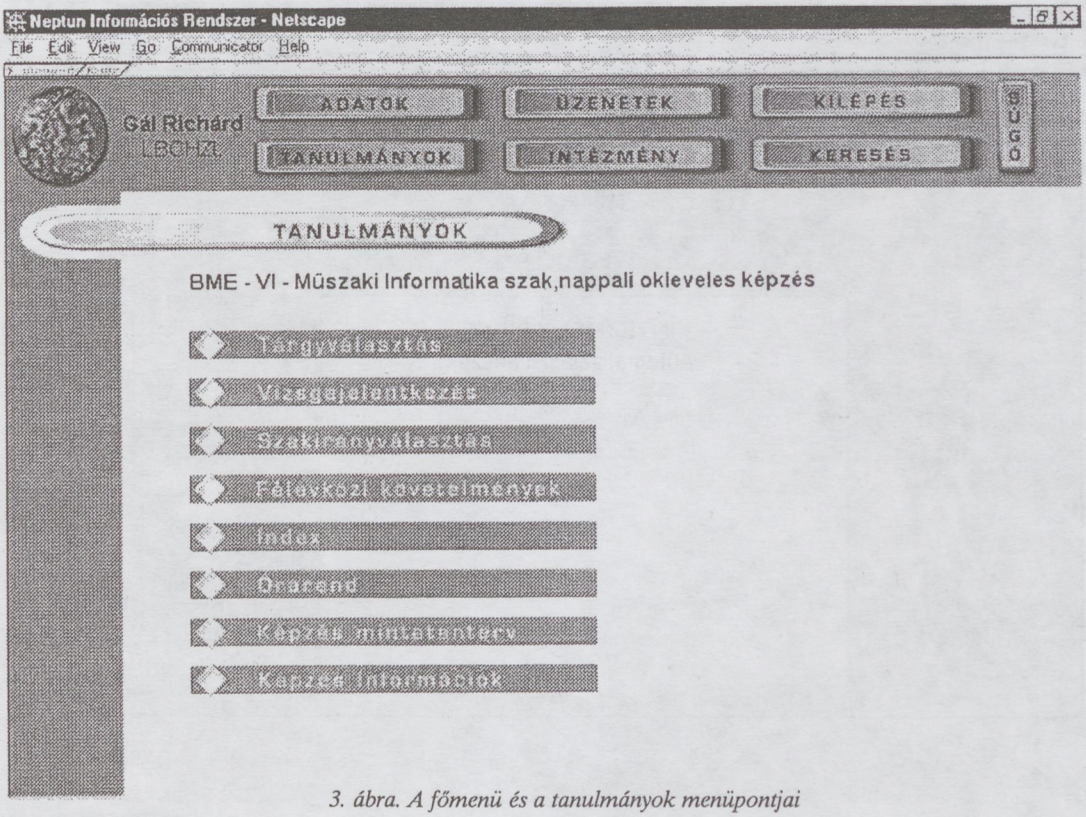
A WWW alapú információs rendszert csak az arra jogosult felhasználók használhatják, azaz olyan felhasználók, akik regisztrálva vannak a rendszerben. A felhasználóknak a szolgáltatások igénybe vételéhez be kell lépniük a rendszerbe. Ehhez meg kell adniuk az egyedi azonosítójukat és a jelszavukat.

A rendszer két részből áll: hallgatói modul és tanszéki modul. A hallgatói modult csak az intézmény hallgatói, a tanszéki modult csak az intézmény oktatói és a tanszéki adminisztrátorok vehetik igénybe.

3.1. A hallgatói modul ismertetése

A hallgatói modul funkciói az információ megszerzésére és az adminisztrációs feladatok elintézésére irányulnak. A főmenüből elérhető funkciók a következők:

- ADATOK: A felhasználó saját személyes adatait, címeit, előző képesítéseit nézheti meg itt, és lehetőség nyílik a jelszavának megváltoztatására is.
- TANULMÁNYOK: A rendszer legfontosabb szolgáltatásait ezzel a menüponttal érhetjük el. Részletesebb ismertetés a következő bekezdésben.
- ÜZENETEK: A dékáni hivatal által küldött üzeneteket tudjuk itt megtekinteni.
- INTÉZMÉNY: Az intézménnyel kapcsolatos általános információkat nézhetjük meg e menüpont alatt.
- KILÉPÉS: Kilépés a rendszerből.
- KERESÉS: Bizonyos regisztrált felhasználók adatait lehet megkeresni ezzel a menüponttal a következő szempontok alapján: név, cím, e-mail cím, telefonszám ill. egyedi azonosító.
- SÚGÓ: A rendszer használatával kapcsolatban kaphatunk itt felvilágosítást.



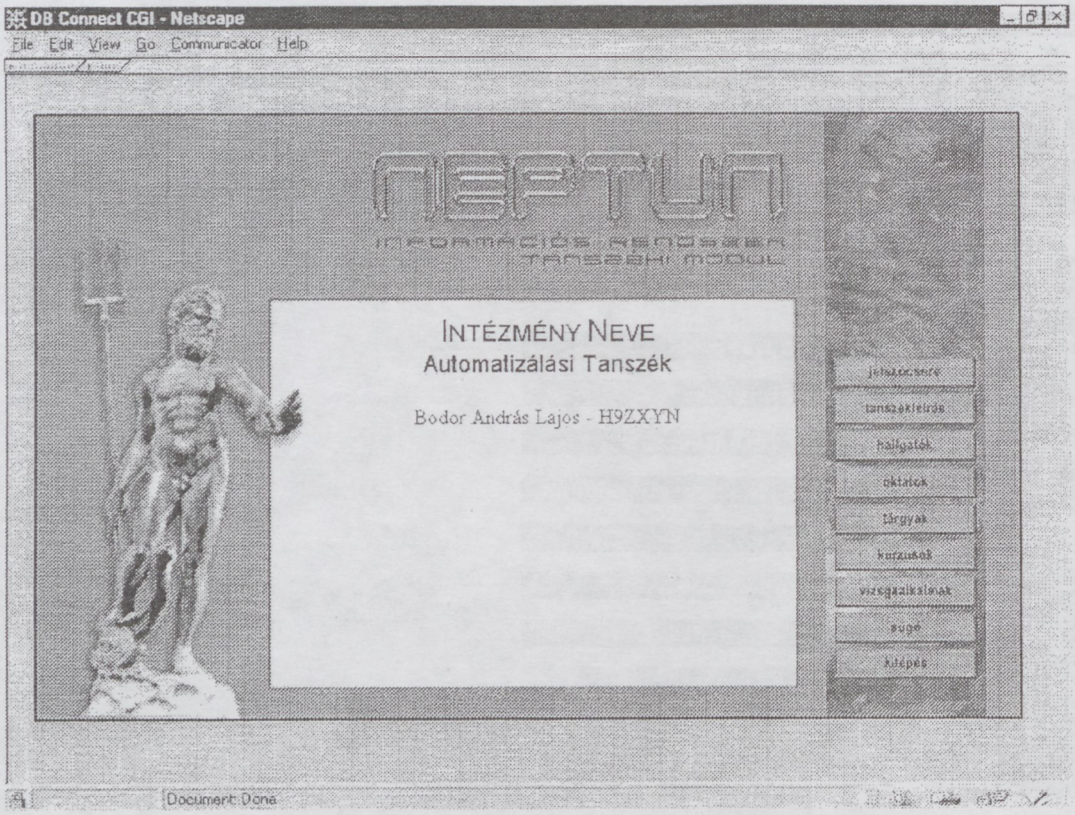
3. ábra. A főmenü és a tanulmányok menüpontjai

A TANULMÁNYOK menüponton keresztül tudunk új tárgyakat felvenni, vizsgákra jelentkezni, szakot és szakirányt választani. Továbbá megtekinthetjük a tantárgyak félévközi követelményeit, az indexbejegyzéseket, az aktuális félévben érvényes órarendünket, a képzés mintatantervét, valamint a képzésre vonatkozó egyéb információkat (3. ábra). Külön kiemelnénk, hogy a hallgatói pénzügyek elintézésére is van lehetőség. Minden a hallgató által a programból végezhető pénzügyi művelet az oktatási intézmény gyűjtőszámlán keresztül megy végbe. Azaz minden befizetett összeg a gyűjtőszámlára kerül. A hallgatók által elvégezhető pénzügy műveletek a következők: IV díj befizetése, tandíj fizetése, különeljárási díj fizetése, szolgáltatások térítése, pénzvisszautalás, tandíjbefizetők felvétele és elvégzett műveletek megtekintése.

3.2. A tanszéki modul ismertetése

A tanszéki modul szolgáltatásait úgy alakítottuk ki, hogy az megfeleljen a napi gyakorlatban elvégzendő tipikus feladatoknak. Ezek az alábbi menüpontokban foglalhatók össze (4. ábra):

- JELSZÓCSERE: A rendszerben használt jelszavunkat tudjuk itt megváltoztatni.
- TANSZÉKLEÍRÁS: A tanszék nevét, elérhetőségeit tekinthetjük meg ezzel a menüponttal. Az adminisztrátorok ezeket az adatokat módosítani is tudják.
- HALLGATÓK: Azoknak a hallgatóknak a névsorát láthatjuk itt, akik a tanszék által indított tárgyat vettek fel. A névsort különböző szempontok szerint lehet megjeleníteni: ábécérend, képzés és szakirányok alapján.
- OKTATÓK: Az oktató kiválasztása oldalon az oktató választhat a tanszéki oktatók közül. Egy adott oktatóról a következő információkat kérheti le megtekintésre: személyes adatok, oktatott kurzusok és a tartott vizsgaalkalmak.
- TÁRGYAK: A tanszéken meghirdetett tárgyak alapadatait tudjuk itt megtekinteni, valamint meg tudjuk változtatni egy-egy hallgató adott tárgyhoz rendelt kurzusát, és a tárgy kurzusairól kaphatunk részletes információkat. Egy-egy kurzusról a következő adatokat láthatjuk: kód, félév, típus, nyelv, oktatók neve, hallgatók neve, létszám.
- KURZUSOK: A kurzusokat ki tudjuk választani tárgyak és oktatók szerint. A kurzusokra vonatkozólag információkat gyűjthetünk be, úgymint jellemző adatok, az órák időpontjai és helyei, a kurzus oktatói és hallgatói, segédanyagok. A kurzusok menüponttal a következő feladatokat tudjuk elintézni: évközi feladatok kiírása, jegyek beírása, bejegyzések megtétele, valamint segédanyagok megadása az adott kurzushoz.
- VIZSGAALKALMAK: Egy vizsgaalkalmat tárgy, kurzus, vagy oktató csoportosítás alapján kiválasztva először megnézhetjük a vizsga jellemző adatait, pl. dátum, időpont, terem, maximális létszám, a vizsga típusa, stb. Lehetőségünk van továbbá egy kurzushoz új vizsgaalkalom kiírására, a vizsga jegyének beírására, a vizsgaalkalomra jelentkezett hallgatók névsorának és a vizsgáztató tanárok nevének megtekintésére.
- SÚGÓ: A rendszer használatával kapcsolatban kaphatunk itt felvilágosítást.



4. ábra. A tanszéki modul menüpontjai

4. BIZTONSÁGTECHNIKAI MEGFONTOLÁSOK

4.1. Bevezetés

Olyan sok személyes információval dolgozó rendszer esetén, mint amilyen a miénk, nem szükséges kihangsúlyozni, hogy igen is szükség van a világhálózaton áthaladó adatok védelmére, azaz a tikosításra. Ebben a fejezetben az alkalmazott megoldást fogjuk megismertetni az olvasóval.

4.2. Az igényelt biztonság

Szolgáltatásunkkal a felsőoktatásban dolgozókat és tanulókat céloztuk meg, és nem csak a számítástechnika iránt érdeklődőket. Rendszerünkben egy esetleges betörő nem tud túlságosan nagy kárt előidézni. Mégis, az alapvető magánszféra védelme mellett teljes biztonságot akartunk felhasználóinknak teremteni. Próbáltunk egy informatív, könnyen kezelhető rendszert konstruálni, melyet korrekt biztonsági korlátok is jellemeznek.

4.2.1. Megvalósított biztonsági korlátok

- Túl sok ideig egy helyben tartózkodó felhasználó

Bárkivel előfordulhat, hogy miután elvégezte az általa kívánt műveletet, elfelejt kijelentkezni, kilépni a programból. Programunkban a biztonság garantálásának a feltétele, hogy használat után kilépjünk a rendszerből. Így törlődnek azok az információk, amelyekkel esetleg más vissza tudna élni. Ugyanis minden felhasználóhoz tartozik két egyedi azonosító, amely csak arra a felhasználóra jellemző. Minden egyes művelet előtt ellenőrizzük, hogy az adott azonosítókhoz tartozik-e belépett felhasználó. Egy felhasználó természetesen több ilyen azonosítópárral is rendelkezhet. A rendszerből való kilépés után ezek az azonosítók érvénytelenítődnek, azaz használhatatlanná válnak.

- Időszaknak nem megfelelő hívások

Sokszor előfordulhat, hogy olyankor próbál meg valaki vizsgára, szakirányra jelentkezni, vagy tárgyat felvenni, amikor nincs erre lehetőség. Az adatbázis struktúrájából kifolyólag ezek a védelmek egyszerű mezőellenőrzés feladatra redukálódtak. Tehát mindig el van tárolva adatbázisban a megfelelő dátum, ameddig a műveletet el lehet, ill. kell végezni. A program a művelet elvégzése előtt mindig ellenőrzi az akcióhoz eltárolt időpontokat, azaz összehasonlítja azt az aktuálissal. A konkrét művelet elvégzésére csak akkor kerül sor, ha az aktuális dátum az időkorlát vizsgálaton átesett.

- Átszerkesztett hívások eljárásainkra

Sok ügyes kíváncsiskodó felhasználó figyeli meg az egyes weboldalak forrását. Nos, a miénket lehívva linkek tömkelegével találja magát szemben. Biztosak vagyunk benne, hogy sokan ki fogják próbálni, hogy az egyes linkek önmagukban működőképesek-e. A válasz természetesen igen, kérdés inkább az, hogy egy linket kicsit átalakítva, más nevében is működnek-e.

Sokakban fel fog merülni a gondolat, hogy mást is fel lehet-e esetleg íratni egy vizsgára, a nevében szakirányra jelentkezni stb. Ennek elkerülésére külön ellenőrzéseket vezettünk be. Mint már említettük, minden műveletre jellemző két azonosító és egy felhasználó. Ezek összetartozását folyamatosan ellenőrizzük. Kilépés után pedig érvénytelenítjük az azonosítókat. Így, ha kiléptünk, és valaki más próbál meg a mi nevünkben valamilyen műveletet elvégezni, hibajelzést fog kapni (még ha ismeri felhasznált azonosítóinkat is).

4.3. A rendszerben alkalmazott titkosítás

A beépített vizsgálatok mellett az adatok hálózaton történő áthaladásra is gondoltunk és a manapság legelterjedtebb webes biztonságtechnikai megoldást választottuk, az SSL alapú titkosítást. A Netscape fejlesztette ki, de a Microsoftnak is van egy hasonló, a PCT (Private Communication Technology). A protokoll dolga, hogy a kliens és a szerver között létrehozzon egy közös kulcselemet, majd a forgalmat ezzel a kulccsal titkosítsa. A felhasználó számára ez úgy jelentkezik, hogy ha a böngészőjével SSL-re alkalmas oldalhoz kapcsolódik, akkor a böngésző egy ikon (általában lakat vagy kulcs) aktiválásával jelzi, hogy a kapcsolat titkosítva van.

Az SSL a TCP/IP szerinti szállítási réteg szintjén működik, így az applikációk számára átlátszó. Mivel ez a réteg kapcsolat-orientált, így a két fél a kezdeti fázisban egyezteti képességeit. Ennek alapján az SSL az RSA módszert használja kulcsegyeztetésre, majd valamilyen szimmetrikus kulcsú algoritmussal folyik a titkosítás. Az RSA helyett akár más módszer is használható, a protokoll nagyon rugalmasan kezeli a kriptográfiai alapeszközöket [6].

5. KÖVETKEZTETÉSEK

5.1. Megjegyzések a rendszerrel kapcsolatban

A bankok Magyarországon még nem fogadják el a HTTPS által nyújtott 40 bites titkosítást. Habár az említett titkosítást az internetes fizetéseknél elfogadják szerte a világon, pl. az amerikai vasúttársaság honlapján a jegyrendelés az SSL titkosítással történik. Tény, hogy napjainkban ez a legelterjedtebb és legelfogadottabb rendszer az internetes társadalom egyre bővülő körében.

A rendszer megjelenése különböző felbontásokban eltérő, mert mi 800x600-as felbontásra optimalizáltuk. Kisebb felbontásban egyszerre kevesebbet lehet látni a képernyőn, ekkor többet kell görgetni a megjelenő ablakon. Ide tartozik még az is, hogy a régebbi böngészőprogramok nem mindegyike támogatja a JavaScripteket, amiket a HTML oldalakon felhasználtunk [2].

5.2. Összefoglalás

Munkánk során elkészült egy többnyelvű, felsőoktatási intézményben használható hallgatói információs rendszer, mely a kor igényeinek megfelelően lett kialakítva egy már létező, kliens alapú hallgatói rendszer struktúrája alapján. Képes kezelni a hagyományos és a kredit rendszerű képzést is.

Rendszerünk előnyei a következők:

- Könnyű hozzáférhetőség a világ bármely részéről.
- Csak egy webböngésző kell telepíteni.
- 4 különböző nyelven áll rendelkezésre.
- Több platformos: Windows NT, Sun Solaris, Linux.
- Egyszerűen kezelhető, könnyen elsajátítható.

A WWW alapú információs rendszer jelenleg öt helyen működik az országban. Üzembe helyeztük már a Közgazdasági Egyetemen, a Külkereskedelmi Főiskolán, a szolnoki Kereskedelmi és Gazdasági Főiskolán, a Miskolci Egyetem Dunaújvárosi Főiskolai Karán és a Veszprémi Egyetemen.

Ebben a cikkben a már működő rendszer bemutatására törekedtünk. Az első fejezetben röviden felvázoltuk, mi vezérelt minket e cél megvalósítására, és egy kis betekintést nyerhettünk a megvalósítás körülményeibe. A következő fejezetben a felhasznált termékekről és az eszközökről esett bővebben szó, majd a rendszer rövid bemutatása következett. Külön fejezetben tértünk ki az ilyen rendszereknél elmaradhatatlan biztonsági problémákra is. Legvégül értékeltük rendszerünket mind pozitív, mind negatív vonatkozásai alapján. Reméljük, sikerült betekintést nyújtani a rendszer elkészítésének körülményeibe, és ismertetni mindazon szempontokat, amiket egy hasonló rendszer elkészítésénél figyelembe kell venni.

IRODALOMJEGYZÉK

[1] C.J.Date: A Guide to the SQL Standard, Second Edition, Addison-Wesley, 1989

[2] Nagy Péter: JavaScript, Kalibán Bt. és Kiskapu Kft., Budapest, 1997.

[3] Oracle WebServer Documentation: Introduction to the Oracle WebServer, Release 2.1, forrás: Internet

[4] Oracle WebServer Documentation: Introduction to the Web Request Broker, Release 2.1, forrás: Internet

[5] Oracle WebServer Documentation: The PL/SQL WebToolkit, forrás: Internet

[6] Adam Shostack: An Overview of SSL (version 2), May, 1995

INFORMATION SYSTEM BASED ON WWW

In this paper we will introduce an information system based on the Internet technology. First, we consider the tasks to solve and what are the necessary hardware and software components to the carry these out. After that, we investigate the structure, the operation and the configuration of the Oracle WebServer, which we used to apply. We touch upon the method of ciphering our data in the World Wide Web and the security solutions used in the system. In a short section we present the services of the information system.

INTERNETES INFORMÁCIÓS RENDSZEREK BIZTONSÁGI KÉRDÉSEI

BAK ATTILA, GÁL RICHÁRD

E-MAIL: BAKI@SCH.BME.HU; E-MAIL: GALR@SCH.BME.HU
TEL: (06-1) 463-2815
BUDAPESTI MŰSZAKI EGYETEM
VILLAMOSMÉRNÖKI ÉS INFORMATIKAI KAR, ELMÉLETI VILLAMOSSÁGTAN TANSZÉK MŰSZAKI INFORMATIKA SZAK, 5. ÉVF.
1111 BUDAPEST, EGRY J. U. 18.

A cikkben először egy kriptográfiai áttekintés következik, amelyben néhány fogalom magyarázata után szó lesz az információs rendszerek elleni támadások fajtáiról. Bemutatjuk a nyilvános kulcsú titkosítás módszerét és megvalósítását RSA algoritmussal. A nyilvános kulcsú titkosítás ismeretében több ezen alapuló kriptográfiai protokoll ismertetése következik, amelyeket szükségesnek ítéltünk a webes alkalmazások alatt is gyakran használt SSL protokoll működésének megértéséhez.

1. BEVEZETÉS

Az utóbbi években gyors fejlődésnek indult hálózati technológiák között kiemelt jelentőségűvé váltak a számítógép hálózatok, és az általuk nyújtotta lehetőségek. Az internet, mint a világot átfogó számítógép hálózat az elektronikus kereskedelem (e-commerce) alapjául szolgálhat, ha bizonyos architektúrális és biztonsági követelményeknek megfelelve üzemeltetjük.

Az internetes alkalmazások biztonságos működéséhez kétféle dolognak kell teljesülni: biztosítani kell a hozzáférési biztonságot és a tranzakciók biztonságosságát. A hozzáférési biztonság a szolgáltatást nyújtó fél azon képességét jelenti, hogy biztosítani tudja hálózati erőforrásainak (számítógépek, memóriák, diszkek stb.) illetéktelen behatolóktól való védelmét. A tranzakció biztonság vagy kommunikációs biztonság megléte lehetővé teszi két objektumnak, hogy internetes tranzakcióikat titkosítva és hitelesítve lefolytathassák. Az internetes és webes elektronikus kereskedelem és információs szolgáltatásokhoz nélkülözhetetlen a tranzakciók biztonságának megléte, amelyet pl. a webes alkalmazásokban gyakran használt SSL protokoll biztosíthat. Ebben a cikkben a tranzakció biztonságot vizsgáljuk, és feltételezzük, hogy a szolgáltató fél részéről biztosítja a hozzáférési biztonságot.

2. INFORMÁCIÓVÉDELEM

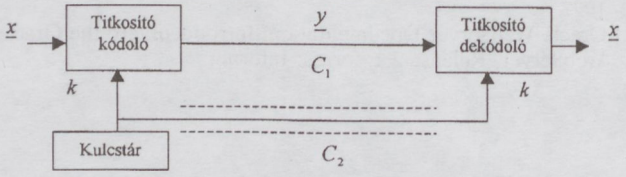
A kommunikáció titkosságának és védettségének biztosításával a kriptológia tudománya foglalkozik, amelynek két ága a kriptográfia és a kriptoanalízis. A kriptográfia a kommunikációban résztvevő adatok titkosságának, védettségének és hitelességének biztosítására alkalmas algoritmikus módszerekkel dolgozik. A kriptoanalízis a titkosított információ megfejtésére tartalmaz eljárásokat.

A kriptográfiával kapcsolatos kutatások a 70-es évek közepétől egyre növekvő ütemben folynak. Ennek fő oka az, hogy a privát szektorban egyre nő az igény az algoritmikus adatvédelem iránt, mivel napjainkban – különösen a fejlett hírközléssel rendelkező országokban – érzékeny információk nagy mennyiségben kerülnek átvitelre nyilvános távközlési csatornákon, vagy tárolódnak fizikailag átlagosan védett memóriákban. Gondoljunk például az internetes vásárlási lehetőségekre, iskolákban, kórházakban, ill. egyéb intézményekben használt információs rendszerekre, ahol pénzügyi információk, egészségügyi, életrajzi, személyi adatok átvitele történik, amelyek jogtalan megszerzése súlyos anyagi és erkölcsi károk okozására adhat lehetőséget.

Fontos azonban megjegyezni, hogy az információk védelmére alkalmazott algoritmikus módszerek csak a megfelelő fizikai, ill. ügyviteli eljárások alkalmazásával együtt biztosíthatják hatékonyan a valós rendszerekben az információvédelmet.

3. ALAPFOGALMAK

A digitális információforrás kimenő adatfolyamát nyílt üzenetnek (plain text) nevezzük, amelynek egy blokkját jelölje . A titkosítás művelete alatt a titkosító kódoló ebből az egy-egy értelmű invertálható leképezéssel az titkosított üzenetet (ciphertext) készíti, vagyis az $\underline{y} = E_k(\underline{x})$ transzformációt végzi, ahol k a titkosítás kulcsa. A D_k dekódoló transzformáció – az E_k inverze – az $\underline{x} = D_k(\underline{y})$ művelettel adja vissza $\underline{x}$-et. Ha a kódolás és a dekódolás azonos kulcsot használ, akkor konvencionális vagy szimmetrikus kriptográfiáról beszélünk. Ennek blokkvázlata az 1. ábrán látható.



1. ábra. konvencionális titkosító blokkvázlata

A rejtett üzenet a C_1 nyilvános csatornán (public channel) kerül a dekódoló oldalra, azonban a kulcsot szigorúan védeni kell, hiszen ennek megszerzése a dekódolás lehetőségét jelenti. Ezért konvencionális titkosító esetén a kulcsot a C_2 titkos csatornán (secret channel) továbbítjuk a dekódolónak.

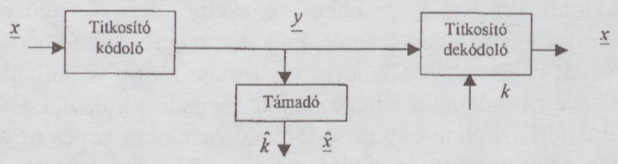
Létezik még az ún. nyilvános kulcsú kriptográfia, amely olyan algoritmust használ, amelynél két kulcs létezik. Az egyikkel titkosítani, a másikkal dekódolni lehet az adott üzenetet. Ez lehetővé teszi, hogy az egyik kulcsot nyilvá-

nossá tesszük (nyilvános kulcs), a másikat védjük (titkos kulcs). Tipikusan a címzett nyilvános kulcsával titkosítjuk az üzenetet, és azt a címzett titkos kulcsa tudja csak dekódolni. A nyilvános kulcsú titkosítás módszereit egyéb kriptográfiai protokollok is alkalmazzák – pl. digitális aláírás, autentikáció stb. – amelyekről még később lesz szó.

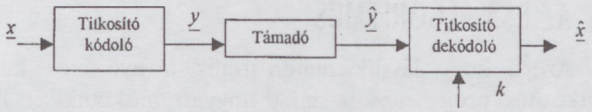
4. AZ INFORMÁCIÓS RENDSZEREK ELLENI TÁMADÁSOK FAJTÁI

Az interneten megvalósuló kommunikációk a TCP/IP (Transmission Control Protocol/Internet Protocol) protokollt használják hálózati protokollként. A TCP/IP kapcsolatorientáltan biztosítja az adatok helyes célba érését, miközben forgalom irányító (routing) funkciót is ellát, azaz az adatok a célba érésig több különböző számítógépen és hálózaton mennek keresztül. Éppen ezen utóbbi momentum teszi lehetővé, hogy egy harmadik személy – a támadó – jogtalanul hozzáférjen a kommunikáló felek között áramló információhoz. A támadóval szembeni alapvető feltételezés az, hogy az aktuális titkosító kulcs kivételével a kódolás, dekódolás alkalmazott algoritmusát teljes részletességgel ismeri [1]. Ennek alapján aktív és passzív algoritmikus típusú támadási módszereket különböztet meg a szakirodalom, amelyek a nyilvános csatorna ellen történnek.

- Passzív támadás: a támadó a nyilvános csatornán folyó kommunikáció adatainak birtokába jut. A megszerzett rejtjelezett információból próbál következtetni a titkos kulcsra. A passzív típusú támadásokat lehallgatásnak (eavesdropping) is nevezik, ilyenkor ugyanis az információ érintetlen marad, de a támadó érzékeny adatok birtokába juthat. A passzív támadásokat (2. ábra) a következő kategóriákba szokás sorolni [1]:
  - Rejtett szövegű támadás: támadás azonos kulccsal kódolt rejtett üzenetek birtokában.
  - Ismert nyílt szövegű támadás: támadás nyílt és rejtett üzenet párok birtokában.
  - Választható nyílt szövegű támadás: a támadó szabadon választhatja meg azt a nyílt üzenetet, amelynek rejtett párját látni szeretné.
- Aktív támadás: a támadó a csatornából üzeneteket von ki, cserél ki, vagy számára kedvezően módosít (üzenetmódosítás). Másik fajtája a megszemélyesítés, amikor a támadó megpróbálja egy legális felhasználó szerepét eljátszani, hogy ezzel valamelyik másik legális rendszerbeli objektumtól információt szerezzen. A 3. ábra szemlélteti az aktív támadás elvi vázlatát.



2. ábra. Passzív típusú támadás elvi vázlata



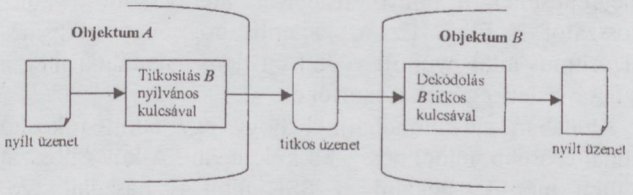
3. ábra. Aktív típusú támadás elvi vázlata

Néhány fogalom magyarázatára szükség van a továbbiakhoz. Ezek a következők. Egy üzenet titkossága (privacy) azt jelenti, hogy csak a kommunikáló felek számára elérhető annak nyílt tartalma. Megkülönböztetjük az üzenet hitelességét (authenticity), amely garantálja, hogy olyan személy küldte, aki a kulcs legális birtokosa. Vagyis a titkosság az üzenet tartalmával, a hitelesség az üzenet küldőjével van szoros kapcsolatban. Egy titkosító algoritmus sikeres feltöréséről beszélünk, ha a támadó „gyorsan" meg tudja állapítani az üzenet nyílt tartalmát az alkalmazott titkosító kulcstól függetlenül. A „gyorsan" olyan időtartamot jelent, amelyen belül a támadó sikeresen felhasználhatja céljaira a megszerzett információt.

A titkosítási algoritmusok a passzív támadások megakadályozását célozzák. Az aktív támadásokat algoritmikus módszerekkel megelőzni nem lehet, de az aktív támadás tényét különböző kriptográfiai protokollok alkalmazásával észlelni lehet. Mielőtt azonban rátérnénk a különböző kriptográfiai protokollok ismertetésére, röviden ismertetjük a nyilvános kulcsú titkosítás módszerét.

5. NYILVÁNOS KULCSÚ TITKOSÍTÁS

A nyilvános kulcsú titkosítás leggyakrabban használt implementációi az RSA algoritmust használják. A következőkben is azt a megközelítést alkalmazzuk. A módszer lényege, hogy nyilvános kulcsú titkosítást használó objektumok mind rendelkeznek egy nyilvános és egy titkos kulccsal (kulcspár). A nyilvános kulcs azt jelenti, hogy ahhoz bárki hozzáférhet, a titkos kulcsát viszont minden objektum védi mások elől. Az adott objektum nyilvános kulcsával titkosított információt csak az ő saját titkos kulcsával lehet dekódolni. Ahhoz tehát, hogy az A objektum B-nek küldhessen titkosított üzenetet, ismernie kell B nyilvános kulcsát, amely mint említettük szabadon hozzáférhető, hiszen azt B publikálja. Mivel azonban egyedül B-nek áll rendelkezésére a saját titkos kulcsa, ami dekódolja az üzenetet, csak B jut hozzá a nyílt üzenethez (4. ábra).



4. ábra. A nyilvános kulcsú titkosítás elvi vázlata

A nyilvános kulcs publikálása azt jelenti, hogy miután B legenerálta a kulcspárját, a nyilvános kulcsot egy nyilvános kulcstárban helyezi el, ahonnét bármelyik objektum kiolvashatja annak az objektumnak a nyilvános kulcsát, akinek rejtett üzenetet kíván küldeni. Vagyis a kommunikációt megelőzően nem kell titkos kulcscserét végezni, de adódik az a feladat, hogy a nyilvános kulcs hitelességét ellenőrizni kell. Erről a kriptográfiai protokolloknál lesz szó.

6. AZ RSA ALGORITMUS

Azért, hogy lássuk miben rejlik a nyilvános kulcsú titkosítás ereje, nézzük meg hogyan működik az RSA algoritmus [1].

- Válasszunk véletlenszerűen két nagy prímszámot: p_1 és p_2.
- Számítsuk ki az $m = p_1 p_2$ és $\phi(m) = (p_1 - 1)(p_2 - 1)$ paramétereket, valamint válasszunk véletlenszerűen egy e egész számot, amelyre $1 \leq e \leq \phi(m)$, hogy $(\phi(m), e) = 1$ legyen. A (a,b) a és b legnagyobb közös osztóját jelöli.
- Számítsuk ki e inverzét modulo $\phi(m)$: $e^{-1}(\mathrm{mod}\phi(m))$.
- Ezek után legyen a nyilvános kulcs m és e, azaz $k^p = [m, e]$, a titkos kulcs pedig d, p_1 és p_2, vagyis $k^s = [d, p_1, p_2]$.
- A titkosító kódolás az $1 \leq x \leq m$ nyílt üzenetre egy $1 \leq y < m$ rejtett üzenetet ad, ahol

$$y = x^e (\mathrm{mod}\ m)\ ,$$

míg a dekódolás az

$$x = y^d (\mathrm{mod}\ m)$$

inverz művelet.

Az x és y skalár jelölések azt jelzik, hogy nemnegatív egész számként végezzük velük a mod m műveletet.

A módszer lényege az, hogy a nyilvános adatok birtokában az inverz számítása igen számításigényes feladat. Ha a p_1 és p_2 prímeket elegendően nagyra választjuk akkor napjainkban gyakorlatilag megoldhatatlan feladat. A titkos kulcs megléte azonban egyszerűvé teszi az inverz számítását.

Az algoritmus hátránya viszont az, hogy a konvencionális titkosításhoz képest a nyilvános kulcsú titkosítás számításigényesebb művelet, ezért nagy mennyiségű adat titkosítására nem biztos, hogy jó választás. Az viszont kivitelezhető, hogy nyilvános kulcsú titkosítással küldjünk szimmetrikus kulcsot, amellyel később valamilyen konvencionális titkosító módszerrel végezzük a kommunikációt. Pontosan ez az, amit a későbbiekben ismertetendő SSL protokoll csinál.

7. A TITKOSÍTÁSI MÓDSZEREK EREJE

Egy titkosító algoritmus ereje kapcsolatban van a kulcs megfejtésének a bonyolultságával, ami viszont a kulcs hosszától is függ. Ez azt jelenti, hogy egy titkosítási algoritmus által nyújtott védettség nem haladhatja meg a kulcsa védettségének a mértékét.

Általában azt mondhatjuk, hogy egy adott titkosító annál erősebb, minél hosszabb kulcsa van. A kulcs hosszát bitben mérjük. Például az SSL által is használt 128-bites kulccsal dolgozó RC4 szimmetrikus titkosító sokkal erősebb védettséget nyújt, mint a 40-bites kulccsal működő RC4 titkosító.

Természetesen a különböző algoritmust használó titkosítóknak különböző hosszú kulcsok szükségesek ugyanahhoz az erősség eléréséhez. Mivel pl. az RSA titkosítók az adott bithosszon elérhető kombinációk közül csak egy szűkebb részhalmazt használhatnak kulcsként, ezért azoknak ugyanolyan titkosítási erősséghez hosszabb kulcsok kellenek, mint a szimmetrikus titkosítóknak, amelyek minden kombinációt használhatnak kulcsként adott bithosszon. Ez magyarázza, hogy miért van az, hogy RSA titkosító esetében miért kell napjainkban 512 bites kulcs ahhoz, hogy azt kriptográfiailag erősnek nevezhessük. Ezzel szemben egy 64 bites kulccsal működő szimmetrikus kódoló már kb. ugyanilyen erősnek mondható.

Itt kell megemlíteni, hogy a titkosítók katonai vonatkozásai miatt az Egyesült Államok kormánya erősen korlátozza a kriptográfiai szoftverek exportálását, például azon szimmetrikus titkosítókét, amelyek kulcsa 40 bitnél hosszabb.

8. KRIPTOGRÁFIAI PROTOKOLLOK

A kriptográfiai protokollok olyan szabályok összességét jelentik, amelyek elemenként használják a titkosító transzformációkat, és biztosítják, hogy ezen transzformációk az adott titkosító rendszerben nyújtsák az adott alkalmazásban megkívánt titkosságot vagy hitelességet. Például a transzformáció használja a kulcsot, de nem biztosítja a kulcs védett odajuttatását a dekódolóhoz. Ekkor egy kulcskiosztó protokollra van szükség, amely elvégzi ezt e feladatot. Általában azt lehet mondani, hogy az aktív támadások felfedésére alkalmasak ezen protokollok, hiszen azok ellen a titkosító transzformáció nem véd. Jellemző kriptográfiai protokollok pl. kulcskiosztás, üzenethitelesítés, partnerhitelesítés, digitális aláírás. A következőkben néhány, a nyilvános kulcsú titkosításon alapuló kriptográfiai protokollt tekintünk át.

8.1. Kulcskiosztás

A kulcskiosztás nyilvános kulcsú titkosításon alapuló változatát mutatjuk be ebben a szakaszban. Ilyenkor a szétosztott kulcsokkal aztán konvencionális titkosítást alkalmazva folyhat a kommunikáció.

Tegyük fel, hogy A és B akarnak titkosított párbeszédet folytatni, amihez szükségük van egy ún. kapcsolat kulcsra (session key), ami a konvencionális kódoló kulcsa lesz. Természetesen nem akarják, hogy ezen kulcs bárki más kezébe kerüljön, ezért a következő képen járnak el: A generál egy rn_A véletlen számot, amelyet B nyilvános kulcsával kódolva elküld B-nek. B is generál egy rn_B véletlen számot, amelyet A nyilvános kulcsával kódolva küld el A-nak. Ekkor A-nak is és B-nek is rendelkezésére állnak az rn_A és rn_B számok, amelyekből mindketten előállítják a $sk = f(rn_A, rn_B)$ kapcsolat kulcsot.

Megfordulhat a fejünkben, hogy miért nem elég ha csak A generál véletlen számot, majd B nyilvános kulcsával kódolva elküldi azt B-nek, hiszen azt úgyis csak B képes dekódolni. Ez igaz is, de ebben az esetben egy támadó generálva egy véletlen számot, majd azt megfelelően kódolva A-nak és B-nek is elküldve, saját magán átfolyó kommunikációt kezdeményezhet az általa megadott kulccsal. Esetünkben azonban egy ilyen támadó már nem képes az sk kapcsolat kulcsot előállítani.

További feladat a nyilvános kulcstár algoritmikus védelme, nehogy a támadó a kulcsok valamelyike helyére a sajátját helyezze, hiszen ekkor másnak szánt üzenetet tud dekódolni, tekintve, hogy azt az ő kulcsával kódolták. A megoldás az lehet, ha a kulcs mellé egy megbízható központ (Certificate Authority) digitális aláírását is elhelyezzük.

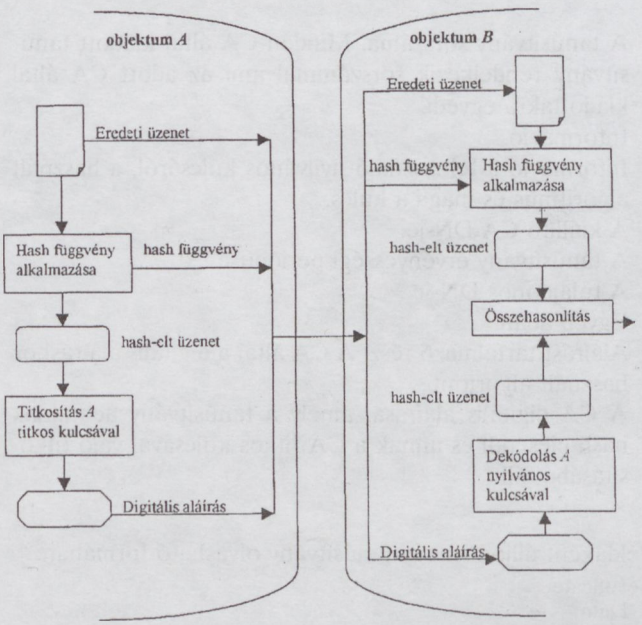
8.2. Digitális aláírás

Ebben a szakaszban azt tekintjük át, hogy a nyilvános kulcsú titkosítást hogyan lehet felhasználni az üzenetmódosítás, mint aktív támadási módszer detektálására.

Az üzenetmódosítás detektálásának (és egyéb hitelesítési technikáknak) a hátterében egy olyan matematikai függvény áll, amelyet egyirányú hash függvénynek (one-way hash) vagy message digest-nek neveznek. Ezen függvény a következő fontos tulajdonságokkal rendelkezik:

- A hash függvény értéke egyértelműen rendelhető a hash-elt adathoz, azaz minden inputhoz egyedi a függvény értéke. Bármilyen változtatás az input adatban más függvényértéket eredményez.
- A függvény egyirányúsága azt jelenti, hogy a hash-elt függvényértékből gyakorlatilag nem állíthatók vissza az input adatok.

A nyilvános kulcsú titkosításnál lehetőség van arra, hogy a titkos kulccsal kódoljuk le az információt, és az így titkosított adatot a nyilvános kulccsal dekódoljuk. Erre az ad lehetőséget, hogy az alkalmazott kódoló és dekódoló transzformáció kommutatív műveletek, azaz a kétszeres kódolás eredménye független a kulcsválasztás sorrendjétől. Ezt a feltételt teljesíti az RSA algoritmusban használt modulo hatványozás. Igaz ugyan, hogy a titkos kulccsal titkosítani és a nyilvános kulccsal dekódolni nem praktikus, hiszen akkor mindenki tudja azt dekódolni. A módszer viszont alkalmas digitális aláírás készítésére. Ennek működését illusztrálja az 5. ábra.



5. ábra. Digitális aláírás alkalmazása üzenetmódosítás detektálására

Ahogy az 5. ábrán is látszik, a vevőhöz (B) három féle adatot továbbítunk: az eredeti üzenetet, a hash függvényt és a digitális aláírást, ami valójában a hash-elt üzenet az A titkos kulcsával kódolva. A vevő objektum alkalmazza a hash függvényt a kapott eredeti üzenetre aminek eredményeként előáll a hash-elt üzenet. Dekódolva a kapott digitális aláírást szintén megkapja a hash-elt üzenetet, amelyet biztosan azzal a titkos kulccsal készítettek, amelynek nyilvános párja nála van. Ha a két hash-elt üzenet megegyezik, akkor B biztos lehet benne, hogy az üzenet integritása nem sérült az átvitel során. Azt azonban még ellenőrizni kell, hogy az általunk A nyilvános kulcsának hitt kulcs valóban A-hoz tartozik. Ezen probléma megoldása a partnerhitelesítés (authentication) feladata.

8.3. Partnerhitelesítés

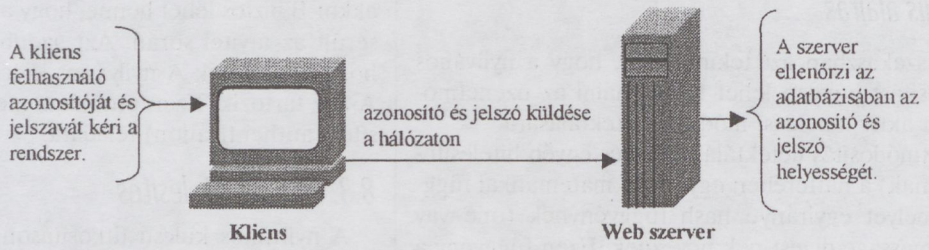
A nyilvános kulcsú titkosításon alapuló partnerhitelesítés eszköze a tanúsítvány (Certificate). A tanúsítvány – ebben a szóhasználatban – egy elektronikus dokumentum, amely azonosítja az adott kommunikációban résztvevő objektumot, és hozzá rendel egy nyilvános kulcsot. A partnerhitelesítéssel a megszemélyesítés jellegű aktív támadások detektálására nyílik mód.

Mint bármilyen egyéb hétköznapjainkban használt tanúsítvány esetén, itt is szükség van egy „intézményre", aki jogosult a tanúsítvány kiadására. Ezt a szerepet a CA-k (Certificate Authority) töltik be. A CA lehet független szervezet, vagy üzemeltethetnek cégek saját tanúsítvány kiosztó szervert (ilyen pl. a Netscape Certificate Server). A CA által kiosztott tanúsítvány egy nyilvános kulcsot rendel a tanúsítvány birtokosához, így megakadályozza a hamis nyilvános kulccsal történő megszemélyesítést. Csak ezen nyilvános kulcs tud együttműködni a tanúsítvány birtokosának titkos kulcsával. A tanúsítvány tartalmazza még az azonosított objektum nevét, egy az érvényesség hosszát jelentő időkorlátot, a kiadó CA nevét, egy sorszámot és egyéb információkat. A legfontosabb azonban, hogy a tanúsítvány mindig tartalmazza a CA digitális aláírását.

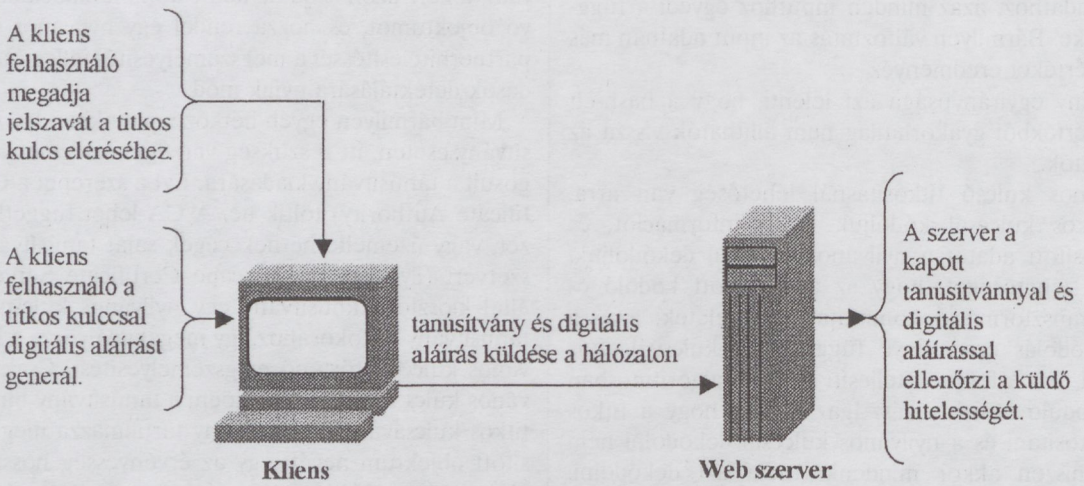
A hálózati interakciók tipikusan egy kliens, pl. web böngésző és egy szerver, pl. web szerver között folynak. Megkülönböztetünk tehát kliens hitelesítést és szerver hitelesítést. Az előbbi a klienst azonosítja a szerver felé, a második pedig fordítva. A partnerhitelesítés fajtái:

- Jelszó alapú partnerhitelesítés: ezt szinte minden szerver szoftver biztosítja. Ilyenkor a kliens felhasználójának érvényes azonosítót és jelszót kell megadnia, amelyet a szerverhez elküldve az ellenőriz (6. ábra). A szerver az azonosítókat és jelszavakat adatbázisban tárolja és innen végzi az ellenőrzést.
- Tanúsítvány alapú partnerhitelesítés: a 7. ábra alapján mutatjuk be partnerhitelesítést tanúsítvány alapján.

A kliens szoftver egy adatbázist tart fenn a titkos kulcsoknak. Ezen adatbázisból a felhasználó csak a megfelelő jelszó ellenében veheti ki a titkos kulcsát. A kliens szoftver ezen titkos kulccsal készít digitális aláírást egy véletlenül generált adathoz. A véletlen adat és a hozzá tartozó digitális aláírás igazolja a titkos kulcs érvényességét, hiszen a digitális aláírást csak a megfelelő nyilvános kulccsal lehet majd verifikálni. A kliens ezután elküldi a tanúsítványt és a digitálisan aláírt véletlen adatot a szervernek, amely alapján az meggyőződik a kliens hitelességéről. A tanúsítvány alapú partnerhitelesítést általában véve szívesebben alkalmazzák, mint a jelszó alapút, mert nemcsak azon alapszik, hogy mit tud a felhasználó (jelszó), hanem azon is amivel rendelkezik (tanúsítvány). Fontos azonban kiemelni, hogy ez csak akkor igaz, ha illetéktelen személy nem fér hozzá a felhasználó erőforrásaihoz (számítógép) és jelszavához, és a titkos kulcsokat tartalmazó adatbázis jelszóval védett. Az SSL protokoll is ezt a partnerhitelesítést használja.



6. ábra. Jelszó alapú partnerhitelesítés



7. ábra. Tanúsítvány alapú partnerhitelesítés

Többféle típusú tanúsítvány létezik egy SSL kapcsolatban, ezek közül hármat emelünk ki: kliens SSL tanúsítvány, szerver SSL tanúsítvány, CA tanúsítvány. Ilyenkor a szerver hitelesítése mindig megkövetelt, míg a kliensé opcionális.

9. TANÚSÍTVÁNYOK SZERKEZETE

A tanúsítványok szerkezeti felépítése, bár a szoftvergyártótól függ, mégis leginkább az ITU X.509 v3 specifikáció szerinti. Bár a felhasználók szempontjából nem kritikus a tanúsítványok szerkezeti felépítése, rendszeradminisztrátori szempontból hasznos lehet ennek ismerete.

A tanúsítvány a tulajdonos megkülönböztető nevéhez (distinguished name – DN) rendel egy nyilvános kulcsot. A megkülönböztető név – továbbiakban DN – azonosító-érték párokat jelent, amelyek összessége egyértelműen azonosítja a tanúsítvány tulajdonosát. A rövidített tipikus azonosítók jelentése a következő: uid: felhasználói azonosító,
e: e-mail cím,
cn: a felhasználó neve,
o: intézmény, cég stb. neve,
c: ország.

Például:

uid=gr, e=galr@evt.bme.hu, cn=Gal Richard,
o=Budapesti Muszaki Egyetem, c=HU

Egy tipikus tanúsítvány a következő részekből áll:

- Adatokat tartalmazó rész:
  A tanúsítvány által támogatott X.509 szabvány verziószáma.
  A tanúsítvány sorszáma. Minden CA által kiadott tanúsítvány rendelkezik sorszámmal ami az adott CA által kiadottakra egyedi.
  Információ.
  Információ a felhasználó nyilvános kulcsáról, a használt algoritmus és maga a kulcs.
  A kiállító CA DN-je.
  A tanúsítvány érvényességi periódusa.
  A tulajdonos DN-je.
  Egyéb adatok.
- Aláírást tartalmazó rész: A CA által a digitális aláíráshoz használt algoritmus.
  A CA digitális aláírása, amely a tanúsítvány adatainak hash-eléséből és annak a CA titkos kulcsával való titkosításából áll.

Példaként álljon itt egy tanúsítvány olvasható formában:

```
Certificate:
    Data:
    Version: v3 (0x2)
    Serial Number: 33 (0x21)
    Signature Algorithm: PKCS # 1 MD5 With RSA Encryption
    Issuer: CN=WWWNeptun, OU=I.D., O=SDA Ltd., C=HU
    Validity:
    Not Before: Tue Mar 09 12:43:18 1999
    Not After: Sun Sep 05 13:43:18 1999
    Subject: CN=gr, OU=EVT, O=BME, L=Budapest,
    ST=Budapest, C=HU
    Subject Public Key Info:
    Algorithm: PKCS # 1 RSA Encryption
    Public Key:
    Modulus:
    00:ec:57:53:86:55:cb:d8:40:e3:4c:a7:04:6d:34:ee:bd:f5:
```

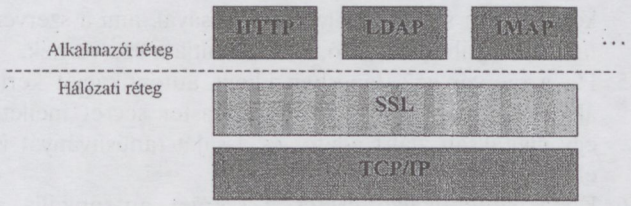
71:0c:17:61:8b:df:be:1f:a0:84:c9:53:14:e3:03:b6:9a:7f:
cb:a3:6a:41:2a:c5:cb:c2:2e:e3:c9:66:57:83:79:f3:b3:da:
79:69:17:e0:12:6c:9d:a1:2e:23:ef
Public Exponent: 3 (0x3)
Extensions:
Identifier: Certificate Type
Critical: no
Certified Usage:
SSL Client
SSL Server
Identifier: Authority Key Identifier
Critical: no
Key Identifier:
bc:d6:72:4c:a5:5c:4a:8e:39:6e:0e:e9:f5:52:2a:09:f2:76:
b7:ae
Signature:
Algorithm: PKCS # 1 MD5 With RSA Encryption
Signature:
1e:f5:56:15:5b:25:b7:cb:77:12:a9:ba:1e:f6:3d:a9:f8:7f:d6:25:a0:
19:52:31:58:d4:64:4a:3e:24:0e:79:eb:ff:7f:df:64:aa:ea:f8:aa:7c:
4d:04:bf:e4:df:1c:91:fd:9c:6e:f8:7b:94:27:64:2a:30:0d:75:9e:4e:
53

Ugyanezen tanúsítvány a szerver számára kódolt formában:

——BEGIN CERTIFICATE——
MIIBxDCCAW6gAwIBAgIBITANBgkqhkiG9w0BAQQFADBD
MQswCQYDVQQ
GEwJIVTER
MA8GA1UEChMIU0RBIEx0ZC4xDTALBgNVBAsTBEkuRC4x
EjAQBgNVBAMT
CVdXV05l
cHR1bjAeFw05OTAzMDkxMTQzMThaFw05OTA5MDUxMTQz
MThaMFwxCzAJ
BgNVBAYT
AkhVMREwDwYDVQQIEwhCdWRhcGVzdDERMA8GA1UEBx
MIQnVkYXBlc3
QxDDAKBgNV
BAoTA0JNRTEMMAoGA1UECxMDRVZUMQswCQYDVQQ
DEwJncjBaMA0GC
SqGSIb3DQEB
AQUAA0kAMEYCQQDsV1OGVcvYQONMpwRtNO699XEMF
2GL374foITJUxTj
A7aaf8uj
akEqxcvCLuPJZleDefOz2nlpF+ASbJ2hLiPvAgE
DozYwNDARBglghkgBhvhCAQEE
BAMCAMAwHwYDVR0jBBgwFoAUvNZyTKVcSo45bg7p
9VIqCfJ2t64wDQYJKo
ZIhvcN
AQEEBQADQQAe9VYVWyW3y3cSqboe9j2p+H/WJa
AZUjFY1GRKPiQOeev/f99k
qur4
qnxNBL/k3xyR/Zxu+HuUJ2QqMA11nk5T
——END CERTIFICATE——

10. AZ SSL PROTOKOLL

Az interneten folyó adatforgalom forrástól célig történő átviteléért és a forgalomirányításért a TCP/IP hálózati protokoll felelős. Az alkalmazói protokollok, mint HTTP, LDAP vagy IMAP a TCP/IP-re, mint hálózati rétegre épülve futnak, vagyis használják a TCP/IP által nyújtott szolgáltatásokat. Az SSL (Secure Sockets Layer) protokoll a fent említett hálózati és alkalmazói protokollok közé ékelődve fut, azaz pl. www alapú átvitel esetén a TCP/IP és a HTTP között (8. ábra).



8. ábra. Az SSL protokoll helye a protokoll hierarchiában

Ha a szerverben az SSL használata engedélyezve van, akkor az SSL protokoll a TCP/IP szolgáltatásait igénybe véve biztosítja a kliens-szerver partnerhitelesítést, és mindkét irányban a titkosított kapcsolatot. Az SSL protokoll által megvalósított funkciók:

- SSL szerver hitelesítés: lehetővé teszi a felhasználónak, hogy megbizonyosodjon a szerver kilétéről. A kliens ilyenkor nyilvános kulcsú titkosításon alapuló partnerhitelesítési protokollal ellenőrzi a szerver tanúsítványát.
- SSL kliens hitelesítés: lehetővé teszi a szervernek felhasználónak, hogy megbizonyosodjon a szerver kilétéről. A használt technika ugyan az mint a szerver hitelesítésnél.
- Titkosított SSL kapcsolat: biztosítja a kommunikáció titkosságát, valamint detektálja, ha üzenetmódosítás történt az átvitel során.

Az SSL protokoll két alréteget tartalmaz: az SSL record protokoll-t és az SSL handshake protokoll-t. Az SSL record protokoll definiálja az átvitel során használt adatformátumot, míg az SSL handshake protokoll tartalmaz egy sereg üzenetet, amelyeket a kliens és a szerver közötti kapcsolatlétesítésnél használ. Az SSL record protokoll-t itt nem részletezzük, azonban az SSL handshake protokoll-t érdemes átnézni.

10.1. SSL handshake protokoll

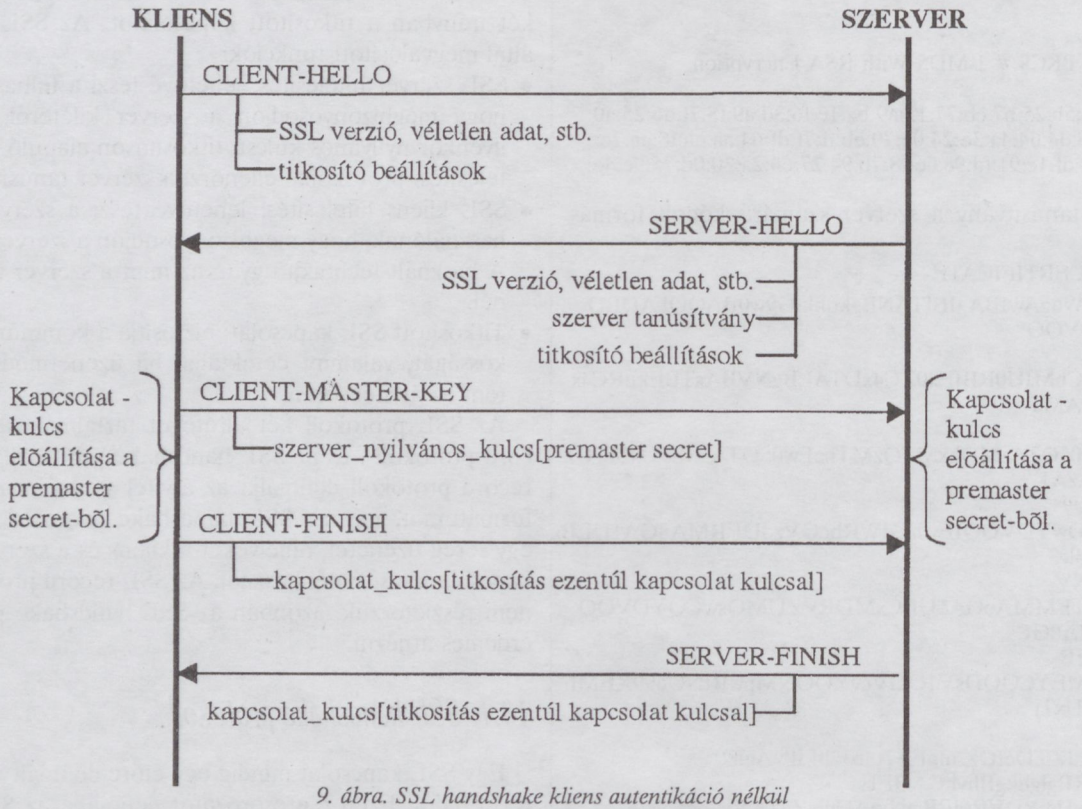
Egy SSL kapcsolat mindig egy előre definiált üzenetcseréjével indul. Ezen cseresorozatot definiálja az SSL handshake protokoll. Eközben a szerver hitelesíti magát a kliens felé nyilvános kulcsú technikát alkalmazva, majd a szerver és a kliens végrehajtják a szimmetrikus titkosításhoz és üzenetmódosítás-detektáláshoz szükséges kulcscserét. Lehetősége van a szervernek van a kliens autentikációját is kérni. A handshake közben a következő lépések történnek [5]:

1. A kliens elküldi a szervernek a saját SSL verziójának a számát, a titkosítóra vonatkozó beállításokat, véletlen adatot stb.
2. A szerver elküldi a kliensnek a saját SSL verziójának a számát, a titkosítóra vonatkozó beállításokat, véletlen adatot stb. Elküldi még a saját tanúsítványát, és ha szükséges, akkor kliens hitelesítést kér.
3. A kliens meggyőződik a szerver hitelességéről. Ha nem találja hitelesnek, akkor tájékoztatja a felhasználót, hogy a kapcsolatlétesítés SSL szinten nem sikerült. Sikeres autentikáció esetén folytatódik a handshake a 4. lépéssel.
4. Az eddigi procedúra alatt a kliens rendelkezésére állt adatokból egy ún. premaster secret-et állít elő, és tit-

kosítja azt a szerver nyilvános kulcsával, ami a szerver tanúsítványából elérhető, és továbbítja a szervernek.

5. Ha a szerver a 2. lépésben kliens autentikációt kért, akkor a kliens a titkosított premaster secret mellett egy digitálisan aláírt adatot és a saját tanúsítványát is elküldi a szervernek.
6. Kliens autentikáció esetés a szerver autentikálja a klienst. Titkos kulcsával dekódolja a premaster secret-et és abból egy ún. master secret-et generál. Ezt a generálást a kliens is elvégzi.
7. A szerver és a kliens a master secret-ből állítja elő a szimmetrikus titkosításhoz szükséges ún. kapcsolat kulcsot (session key).
8. A kliens üzenetben értesíti a szervert, hogy ezek után minden információt ezzel a kapcsolat kulccsal titkosítva továbbít felé, majd részéről lezárja a handshake procedúrát.
9. A szerver is jelzi a kliensnek, hogy a kapcsolat kulcsot használva kommunikál vele, majd ő is lezárja a handshaket.

A folyamatot a 9. ábrán szemléltetjük.



9. ábra. SSL handshake kliens autentikáció nélkül

10.2. Az SSL által használt titkosító kódolók

Az SSL protokoll több különböző titkosító algoritmust (cipher) támogat a partnerhitelesítéshez, a kapcsolat kulcsok cseréjéhez és a titkosított adatátvitelhez. A kliensek és a szerverek egyenként lehet, hogy különböző titkosító rendszereket támogatnak pl. a használt SSL protokoll verziószámától , vagy az adott cég ide vonatkozó szabályaitól vagy a szoftvert exportáló ország korlátozásaitól függően. Éppen ezért az előbb ismertetett handshake folyamatban a kliens és a szerver szoftverek megegyeznek abban, hogy mely titkosító algoritmusokat használják a különböző kriptográfiai protokollokban, ill. a titkosított adatátvitelre. Itt olyan algoritmusok jönnek szóba, mint DES, DSA, KEA, MD5, RC2, RC4, RSA, RSA key exchange, SHA-1, SKIPJACK, Triple-DES stb.

11. ÖSSZEFOGLALÁS

Amikor egy WWW alapú szolgáltatást nyújtó rendszert üzemeltetünk, és a működés közben érzékeny adatok továbbítása történik, hamar szembesülünk a kommunikáció titkosításának a problémájával. A megoldás lehet az ilyen alkalmazásoknál gyakran használt SSL protokoll használata. Ha ezt a megoldást választjuk, akkor olyan szerver és kliens szoftvereket kell használnunk, amelyek képesek az SSL protokollal együtt működni. Tipikusan a web szerver és web böngésző szoftverek ilyen irányú megválasztása célszerű. A manapság elterjedt Netscape és Internet Explorer böngészők teljesítik ezen kritériumot. A web szerverek közül ilyen pl. a Netscape FastTrack, ill. Apache web szerverek. Ha saját CA-t üzemeltetünk, akkor szükség van egy tanúsítvány kiadására alkalmas szoftverre is. Ilyen pl. a Netscape Certificate Server, vagy a mod_ssl nevű modul Apache web szerver alá.

A már említett export korlátozások miatt számunkra a legerősebb kódoló a 40 bites kulcsot használó RC4 kódoló. Megbecsülték, hogy egy pentium alapú PC-vel a 40 bites kulcs megfejthető pár hónap alatt.

Az SSL protokoll böngésző és webszerver közötti webes HTTP kommunikáció titkosítására való használata nem zárja ki a hagyományos, nem titkosított HTTP kommunikáció egyidejű meglétét. Titkosított átvitelhez az URL-ben nem http-t, hanem https-t kell írni a megfelelő portszámmal (alapértelmezés szerint az SSL a 443-as portot használja).

IRODALOM

[1] Györfi László, Vajda István: A hibajavító kódolás és a nyilvános kulcsú titkosítás elemei, Műegyetemi Kiadó 1996.
[2] Ralf S. Engelschall: mod_ssl The Apache Interface to SSLeay
[3] Adam Shostack: An Overview of SSL (version 2), May, 1995
[4] Introduction to SSL, Online documentation, http://developer.netscape.com
[5] SSL 3.0 Specification, http://home.netscape.com
[6] W. Diffie, M. E. Hellman: Privacy and authentication: An introduction to cryptography, Proc. IEEE, vol.67, 1979
[7] J. L. Massey: Introduction to Contemporary Cryptology, Proc. IEEE, vol. 76, 1988.

SECURITY ASPECTS OF INTERNET BASED OF INFORMATION SYSTEMS

A. BAK, R. GÁL

TECHNICAL UNIVERSITY OF BUDAPEST

Internet security actually consists of two distinct services – access security and transaction security. Access security refers to a corporation's ability to protect its computers, memory, disk, printers and other computing equipment from unauthorized use. Transaction security or communications security refers to the ability of two entities on the internet to conduct a transaction privately with authentication and digital signatures if required. Electronic commerce on internet and the web fundamentally depends on transaction security. SSL is a mechanism for transaction security on the World Wide Web. This article considers transaction security and assumes that problem of access security is already solved in the system.

A secure transaction of information messages possesses the following characteristics: Confidentiality: others cannot eavesdrop on an exchange; Integrity: the messages received are identical to the messages sent; Authenticity: you are assured of the persons with whom you are making an exchange; Non-Repudiability: none of the involved parties can deny that the exchange took place.

In this article we first intend to make an introduction into cryptography, where after the explanation of some main concepts we describe the types of attacks against information systems and briefly review the technique of public key cryptography with RSA algorithm. Having given an insight into public key cryptography we explain some cryptoprotocols which we claim to be necessary to understand the SSL mechanism widely used in WWW applications.

Bodor András a gimnáziumi évek alatt angol és német nyelvből tett középfokú "C" típusú nyelvvizsgát. Ezután a Budapesti Műszaki Egyetem Villamosmérnöki és Informatikai karának műszaki informatika szakára jelentkezett a német nyelvű mérnökképzésre, ahol az első 4 szemeszterben az előadások német nyelven zajlottak, majd az ötödik szemesztert a Karlsruhei Műszaki Egyetemen végezhette. Hazatérése után kezdett el adatvédelmi, adatbiztonsági problémákkal és az elektronikus kereskedelemmel foglalkozni. E témában német nyelven előadást tartott a 97-es Balatonfüredi, majd a 98-as Müncheni Frühlings-akademián. A 1998-ban megrendezett Műegyetemi TDK-n WWW alapú Információs rendszerek c. dolgozattal jutalomdíjban részesült. Részt vett a 99-es Műegyetemi Végzős Konferencián. Egyetemi tanulmányai befejezése után doktoranduszként szeretne tovább tevékenykedni.

Szabad Tamás középiskolai tanulmányaimat a székesfehérvári Gróf Széchenyi István Műszaki Középiskolában végezte számítástechnikai és informatika szakon. A középiskola negyedik osztályában angolból középfokú állami nyelvvizsgát tett. Ezután felvételt nyert a Budapesti Műszaki Egyetem Villamosmérnöki és Informatikai Karának műszaki informatika szakára. 1997 szeptemberében a középfokú nyelvvizsgával egyenértékű nyelvi szigorlatot tett francia nyelvből az egyetemen. 1997 nyarától dolgozik a wavelet transzformáció felhasználásán a jelfeldolgozás területén. Egyik társszerzője volt a Híradástechnika c. folyóiratban tavaly megjelent "Compressing Still Imges Using Wavelet Transform" című lektorált cikknek. Jelenleg ötödéves hallgató, multimédia és kommunikációs hálózatok szakirányra jár. Diplomamunkáját a "Wavelet transzformáció alkalmazása a hangfeldolgozásban" címmel készíti. A BME Elméleti Villamosságtan Tanszékén 1998 nyarától vesz részt a Neptun Hallgatói Információs Rendszer WWW alapú fejlesztésében.

Gál Richárd az egri Szilágyi Erzsébet Gimnáziumba járt speciális angol és matematika szakra. A gimnáziumban angol nyelvből felsőfokú állami nyelvvizsgát tett. Az Országos Középiskolai Tanulmányi Verseny országos döntőjében angol nyelvből hetedik helyezést ért el. 1994-ben felvételt nyert a Budapesti Műszaki Egyetem Villamosmérnöki és Informatikai karának műszaki informatika szakára, ahol multimédia és kommunikációs hálózatok szakirányra jár. A BME Elméleti Villamosságtan Tanszékén részt vesz a Neptun Hallgatói Információs Rendszer WWW alapú fejlesztésében. Diplomamunkáját wavelet transzformáció alapú képtömörítés témában írja. Ezen témában már több TDK, OTDK konferencián is részt vett, valamint társszerzője volt a Híradástechnika folyóiratban megjelent, lektorált "Compressing Still Images Using Wavelet Transform" cínű cikknek. 1999 júniusában államvizsgázik. Ezt követően tervei között szerepel a Budapesti Műszaki Egyetemen egy Ph.D. kurzus elvégzése és a Ph.D. cím megszerzése. Ezen kurzuson az elektronikus kereskedelem és authorizációs központok távközlési és informatikai alkalmazásainak kutatásával szeretne foglalkozni.

XIVth International Conference on Microwave Ferrites Microwave Ferrite Technology in Hungary

ANNA SZTANISZLAV
Chairperson of the XIVth ICMF

The Innovation Company for Telecommunication organised in Eger the XIVth International Conference on Microwave Ferrites (ICMF) between 11-15 October 1998.

The ICMF is a traditional meeting held regularly of the scientists who are interested in physics and microwave behaviour of gyromagnetics, electrodynamics of the microwave magnetic structures, microwave ferrite devices, technology, measurement and application of microwave magnetic materials and superconductors.

A new conference was called to life 28 years ago to counter the seclusion of scientists from the East, to enhance the possibilities of scientists from the East European countries. Those scientists were eager to obtain information their own fields, wanted to learn about the new trends of the sciences, to join into the bloodstream circulation of the world, they decided to bring to life a new regular forum for the Eastern European scientists.

The industrial application of ferrite materials started during the first half of 50's and the first description of synthetic garnet materials were published from 60's. This field of science seemed to be very prosperous one. Research Institutes and Departments of Universities were established for investigation, development and new applications of the ferrite and garnet materials. This movement was the motivation to establish the ICMF in 1970 and by the creation of this forum a bridge was built for the Eastern European specialists to the scientific world.

This is the only conference in the whole world so far which has been managing the microwave ferrite and garnet materials and their applications separately from the other ferrite materials and applications. Following the political and economical changes, realising the necessity of renewal the organisers opened the conference to all scientists of the world from the middle of 80's and continuously put new colours the palette of the conference. New topics were included in the conference programme such as superconductors for microwave application and absorbers as well.

However all of these efforts were proved to be insufficient to keep the interest focused for the ICMF. It seemed that the interest in the basic research of the microwave ferrite materials decreased as from the beginning of 80's. The previous three conferences were held by a limited – not more than max. 10 – number of the participants.

When the Innovation Company for Telecommunication was asked to organise the XIVth ICMF two years ago the company took a great risk, the expected result was more than doubtful. On the other hand it was really a great challenge for the Hungarian organisers.

The result surpassed the boldest expectations of the organisers. More than 40 participants arrived from 10 countries (Japan, USA, Iran, Russia, Romania, Bulgaria, Lithuania, Poland, Slovakia, Hungary). 46 lectures were held in 7 sections. The organisers had the possibility – in first time of the history of the ICMF – to invite lecturers and to arrange tutorial section.

Prof. Patton (USA) , whose two invited lectures could be found in this issue of the Telecommunication, is one of the most famous and well-known scientist on the field of microwave garnets. Generations of scientists have been learning their job from his publication and lectures. Prof. Fukasawa (Japan), whose invited lecture was published in the previous issue of the Telecommunication – gave a lecture about the latest technology on mobile radio communication with spread spectrum modulation. Although the topic of Prof. Fukasawa's lecture is a little bit diverting from the ferrite field but as one of the hottest points of the nowadays telecommunication is interesting for everybody who has any connection with the telecommunication.

The XIVth ICMF was sponsored by the IEEE, the Hungarian IEEE MTT/Com. Chapter, the National Committee for Technological Development (OMFB), National Foundation for Scientific Research (OTKA) and the Pharmathesis L.P. (International Business Contacts) for which the organisers are most thankful and would like to take this opportunity to extend their thankfulness.

The Conference Proceedings were published in Hungary (ISBN 963 420 568 2) and in Russia, Moscow as well.

It was a regrettable experience that although the development of the telecommunication has never been so fast and extensive than it is nowadays, nobody from some founder countries – such as Slovakia, Czech Republic –, and only one professor from Bulgaria participated on the XIVth ICMF because of the bankrupt of their institutes the ferrite activity is no more in these countries, or because the ferrite specialists changed their job.

The ferrite technology – development and production of large scale of microwave ferrite-, garnet materials and devices – survived the most critical period in the Innovation Company for Telecommunication in Hungary. New scientific results of its specialists are continuously published and large scale of ferrite devices are manufactured for domestic and export markets. Basically this was the reason to accept the honoured role of organising the conference. We sincerely hope the success of this conference will a small way contribute to the bright and fruitful future in the life of ICMF.

The XVth ICMF will be organised in Poland in 2000.

LECTURE
XIVth International Conference on Microwave Ferrites
Gyromagnetic Electronics and Electrodynamics
Eger, Hungary
October 11 - 15, 1998

MICROWAVE MAGNETIC ENVELOPE SOLITONS IN THIN FERRITE FILMS

Carl E. Patton
Department of Physics, Colorado State University
Fort Collins, Colorado

Research Funding: National Science Foundation (USA), Army Research Office (USA), Office of Naval Research (USA), NATO

Sources of Materials: Dr. J. D. Adam
Northrop Grumman Science and Technology Center

Other Collaborators:
Pavel Kabos, Hua Xia, Pavel Kolodin, Hong-Yan Zhang, Reinhold Staudinger, Boris Kalinikos, Nikolai Kovshikov, Yuri Fetisov, Byron Faber, Nathan Ickes, Ming Chen, Mincho Tsankov, Andrei Slavin, Jon Nash, Mark Ablowitz, Scott Mock, Paolo DeGasperis, Sergei Nikitov, Allan Boardman, Romolo Marcelli, Eric Wright, and Harold Ensle

XIVth International Conference on Microwave Ferrites,
Gyromagnetic Electronics, and Electrodynamics
Eger, Hungary, October 11-15, 1998

Microwave Magnetic Envelope Soliton Thin Ferrite Film Devices

Carl E. Patton, Department of Physics, Colorado State University
Fort Collins, Colorado, USA

MSW Delay Line Concept:

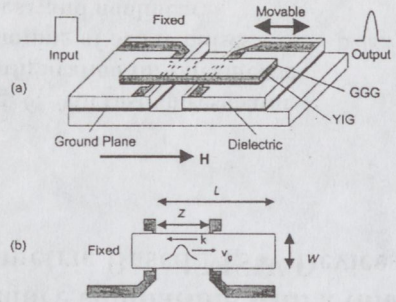


Fig. 1. Variable transducer spacing device structure for MME pulse measurements.

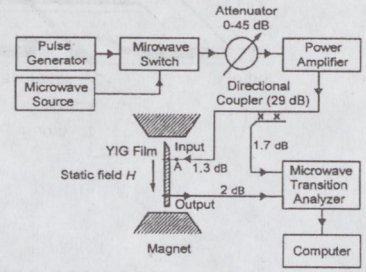


Fig. 2. Block diagram of basic MME soliton spectrometer system.

Soliton Principle:

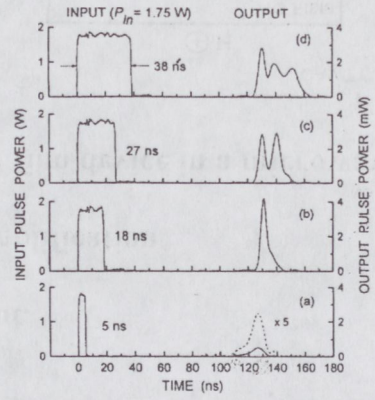


Fig. 3. Example of single and multiple soliton formation for 5 GHz magnetostatic backward volume wave (MSBVW) pulses.

Key Issues:
1. Solitons are robust, narrow, no spreading
2. YIG is a low loss material (perhaps the best)
3. Decay rate is still to high for many applications

Approaches for new YIG film MSW soliton devices:

Question: How to keep soliton pulses from decaying?

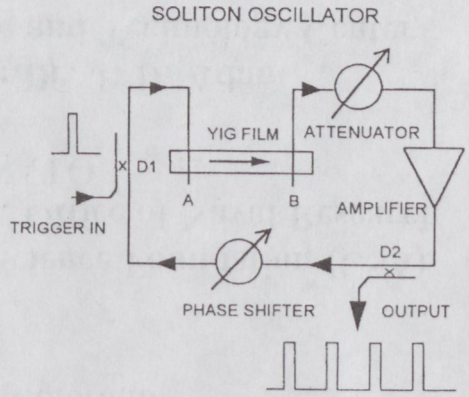


Fig. 4. Basic soliton oscillator feedback configuration.

One Answer: Feedback

Several types of MSW delay line based feedback devices developed:

I. "Active" Delay Line
II. "Interrupted" Feedback Soliton Train Generator
III. "Modulated" Feedback Soliton Oscillator

Two additional feedback applications:

IV. Feedback Controlled Bistable MSW Oscillator
V. MSW Interferometer with Bistable Power Response

Feedback is one way to maintain output.

There is a second way: Parametric Amplification

Our original idea was to put the MSW film device in a microwave cavity:

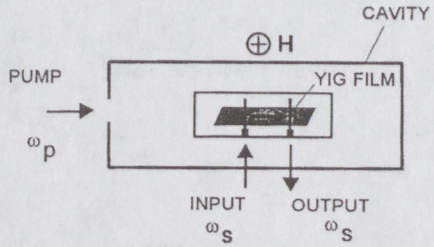


Fig. 5. Cavity arrangement for the parametric pumping of MME pulse signals in YIG films.

A second, microstrip approach was found to be easer to implement and more compatible with a thin film device concept.
Parametric Based MSW Devices:

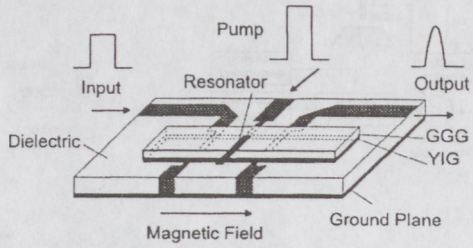


Fig. 6. Microstrip resonator configuration for parametric pumping of MSW pulses, linear and nonlinear.

VI. Soliton Parametric Amplifier
VII. Wide Resonator Gate Switch
VIII. Resonator Based Phase Detector
IX. Switch based on Soliton Dragging

Finally, we have begun to explore the use of soliton self focusing properties for microwave switching applications.

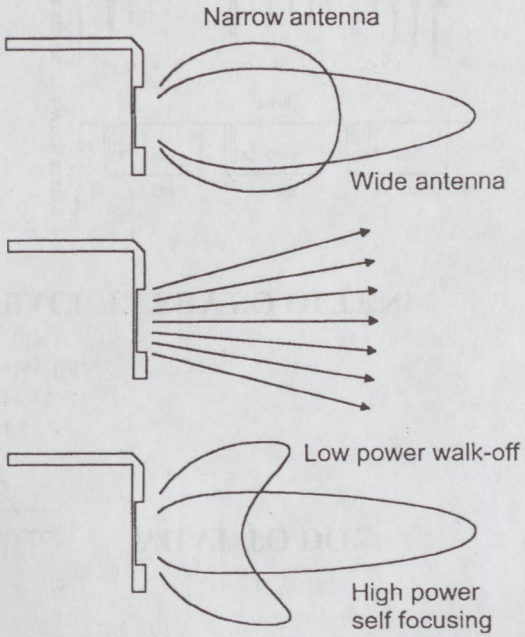


Fig. 7. Schematic power profiles for MSW signals.

(a) Radiation patterns for narrow and wide antennas.

(b) MSW signal generation (schematic)

(c) Walk-off at low power and (soliton) self focusing at high power.

An actual switch:

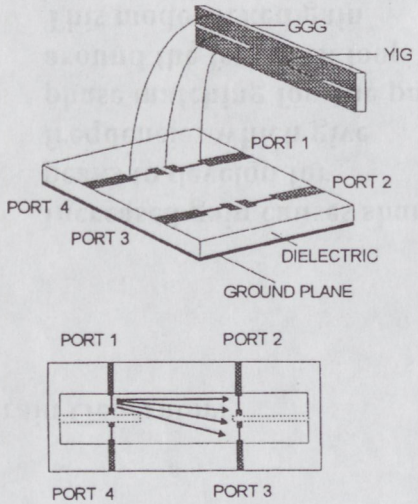


Fig. 8. Four port transducer structure for the on-on to on-off switching through the nonlinear self-focusing of MME soliton pulses.

Feedback Devices:

I. Active Delay Line.

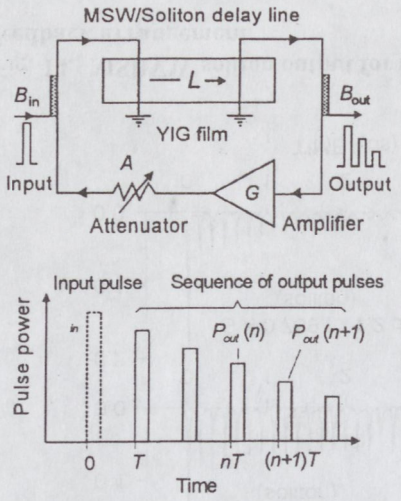
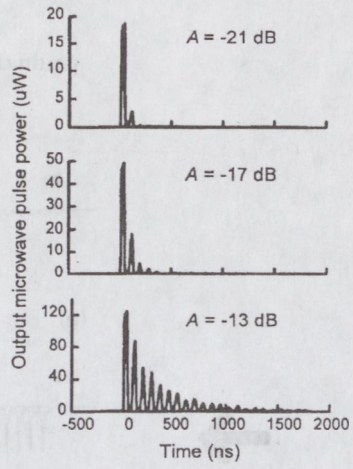


Fig. 9. Schematic of active delay line circuit and output characteristics.



200 dB/μs

100 dB/μs

40 dB/μs

Fig. 10. Typical output pulse trains for active delay line.

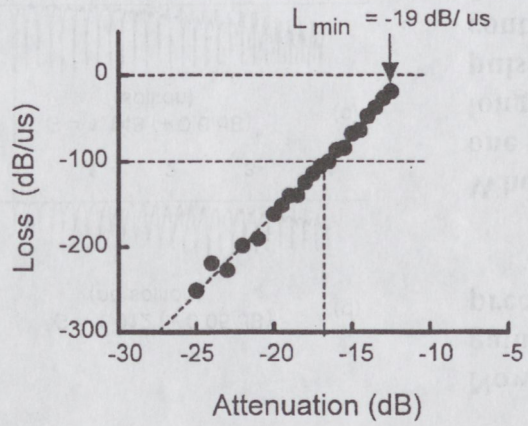


Fig. 11. Loss versus feedback attenuation for active MSSW delay line.

II. Interrupted Feedback Soliton Train Generator.

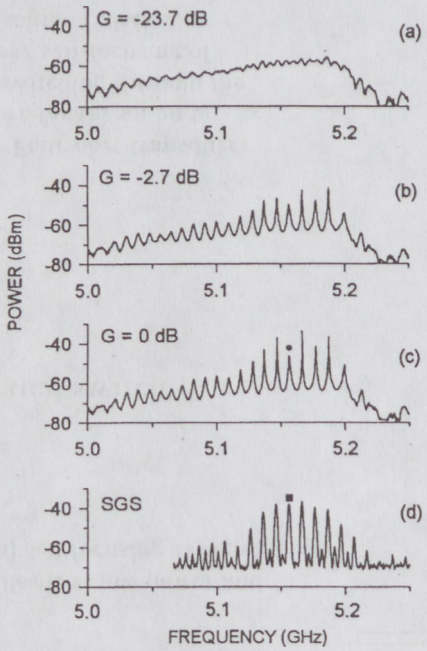


Fig. 12. Effect of feedback on power vs. frequency response for MSBVW delay line.

Increased gain causes sharp peaks to develop for frequencies which give phase matching for one pass around the feedback loop. This mode locked gain produces oscillation for loop gain factors which are below unity.

WHAT TO DO?

INTERRUPT FEEDBACK EVERY SO OFTEN!

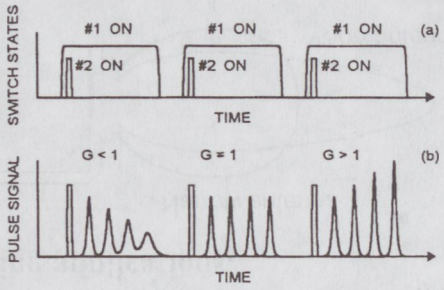


Fig. 13. Interrupted feedback scheme.

This produces a very nice result:

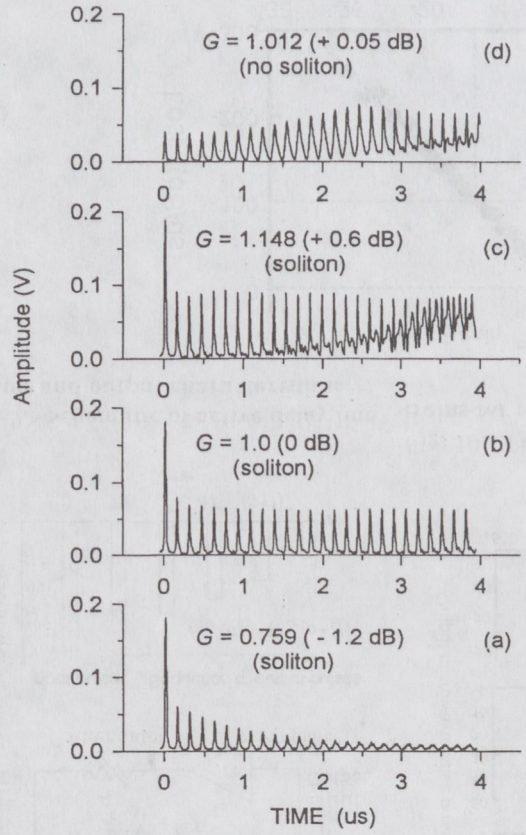


Fig. 14. MSBVW soliton output for interrupted feedback arrangement.

Now, the feedback gain may be set precisely to unity.

When this is done, one may obtain a long train of soliton pulses which can continue undistorted for up to about 40 μs.

THESE PULSES ARE MSBVW SOLITONS. THEY CONTINUE WITH NO DISTORTION UNTIL THE FEEDBACK LOOP IS SWITCHED OFF AFTER THE 40 μS.

III. Modulated Feedback Soliton Oscillator.

The mode locking shown above for the cw power vs. frequency response with feedback opens up new options.

A. There is no need to apply input pulses at all.
B. There is no need to interrupt the feedback.
C. Just <u>modulate</u> the feedback at the delay time for the MSW signal around the feedback loop!

THESE SOLITON PULSES MAY BE EXTENDED FOREVER. THE CLOCK WHICH DRIVES THE MODULATION OF THE SWITCH IN THE FEEDBACK LOOK DEFINES THE PULSE RATE (ALONG WITH THE DC MAGNETIC FIELD).

THIS CLOCK SIGNAL IS SIMPLY A VOLTAGE PULSE SIGNAL, NOT A MICROWAVE SIGNAL. THE OUTPUT CONSISTS OF MICROWAVE SOLITON PULSES.

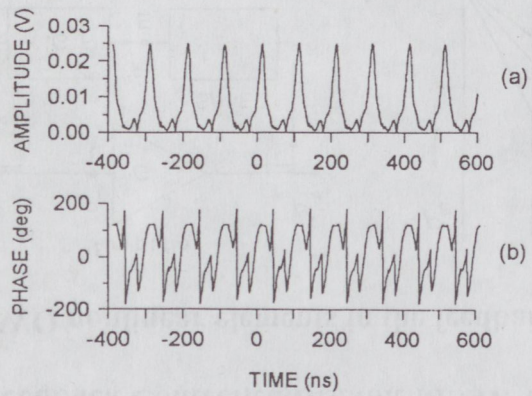


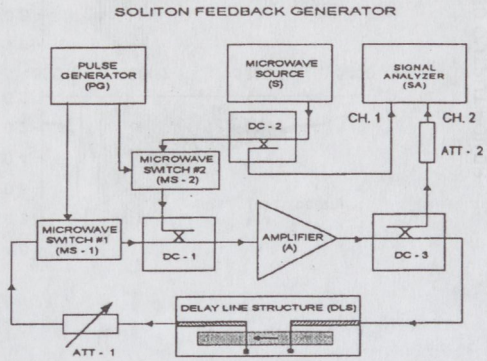
Fig. 15. Self generated MSBVW soliton pulse train obtained with modulated feedback and NO input pulse. (a) shows pulse amplitude profiles and (b) shows phase profiles.

NO DISTORTION

NO DECAY!

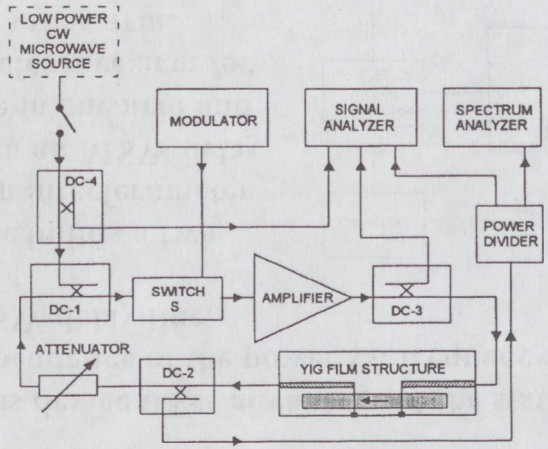
THE TWO FEEDBACK SCHEMES:

INTERRUPTED FEEDBACK -



SWITCH # 1 BREAKS THE FEEDBACK LOOP EVERY 40 μS OR SO.

MODULATED FEEDBACK SELF GENERATED SOLITONS -



NO INPUT PULSES TO FORM SOLITONS.

SWITCH S IS TIMED TO MODE LOCK TO MSW CYCLE TIME.

Two other MSW feedback devices - BISTABILITY

V. Feedback Controlled Bistable MSSW oscillator.

Use TWO nonlinear elements in the feedback loop:

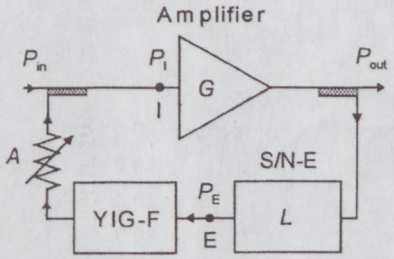


Fig. 16. MSW based MSW oscillator.

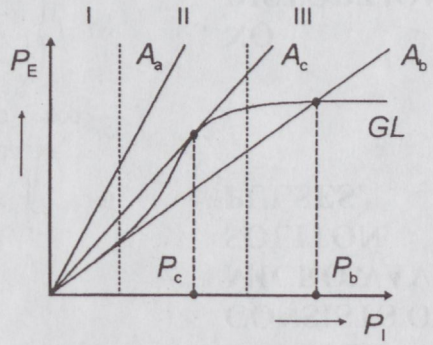


Fig. 17. Response curve analysis for bistable MSW oscillator.

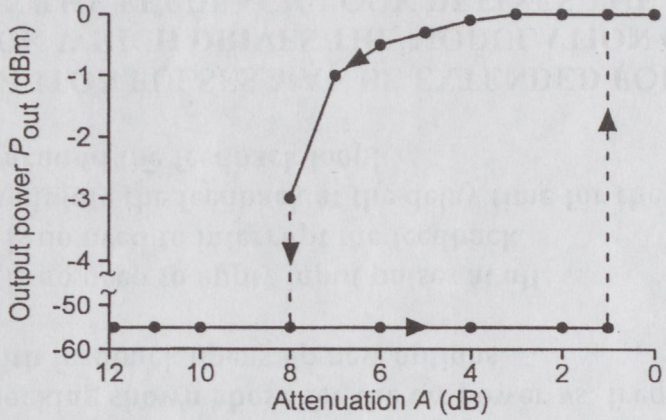


Fig. 18. Output power versus feedback attenuation level for bistable MSW oscillator.

V. MSW Interferometer with Bistable Power Response.

This device takes advantage of the static magnetic field dependence of the power vs. frequency response curve for an MSW delay line.

One builds a two arm interferometer with an MSW delay line in one arm and a reference arm for the other arm.

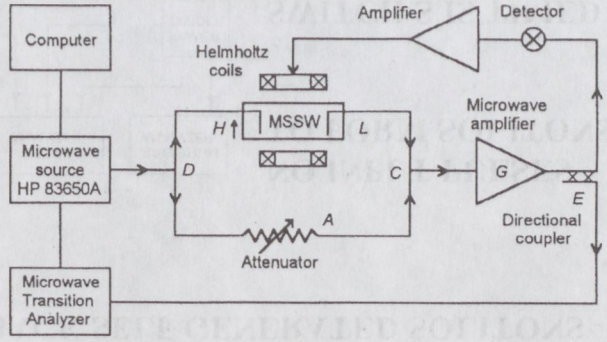


Fig. 19. MSSW Delay line interferometer with magnetic field feedback.

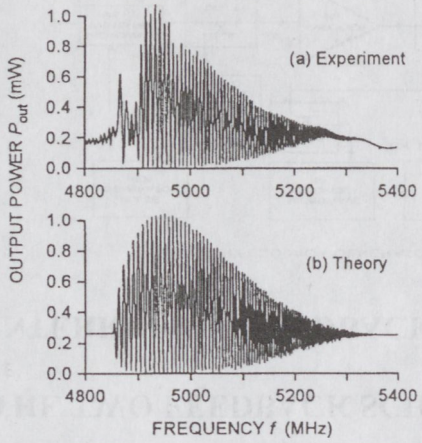


Fig. 20. Interferometer response vs. frequency with no feedback.

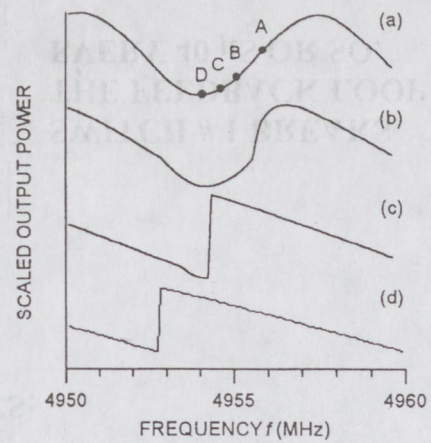


Fig. 21. Single cycle interferometer response with feedback.

A Kapsch Meridian1 intelligens technológiának köszönhetően az Ön kommunikációs rendszere együtt nő sikereivel

LOWE|GGK

Legyen szó szolgáltatásról, kereskedelemről vagy iparról, a globális elérhetőség és a zavartalan információáramlás jelentősége napról napra növekszik. Igaz ez az élőbeszédre, az adatátvitelre, az Internetes és a multimédia kapcsolatokra egyaránt.
A jelen és a jövő megoldásainak kulcsa egy teljesen digitalizált ISDN rendszer, a Meridian1: az egyszerű irodai telefóniától a videokonferencián és a távmunkán át a számítógépes és az internetes telefonálásig. A Meridian1 lépést tart cége sikereivel: moduláris felépítése korlátlan bővítést tesz lehetővé és minden további fejlesztés integrálható a már meglévő Meridian1 kommunikációs hálózatba. Nem véletlen, hogy a Meridian1 – több mint 30 millió csatlakozással – a legelterjedtebb kommunikációs rendszer a világon.
Ha szeretne többet megtudni a Meridian1-ről és ha érdeklődik az egyéni és testreszabott megoldások – tanácsadás, koncepció fejlesztés, rendszer integráció, -telepítés és -szolgáltatás – iránt, már most beszéljen a Kapsch-sal: Kapsch Telecom Kft., 1113 Budapest, Bocskai út 77-79, telefon: (1) 209-2110, fax: (1) 209-2111 vagy keresse fel internetes honlapunkat: www.kapsch.net.

KAPSCH
the communications company


MOLTELECOM

MOLTELECOM

Tevékenységi kör:

* 60 éve az olajipari távközlési rendszer üzemeltetése
* Számítástechnikai és ügyviteli adatforgalmazás, technológiai távfelügyelet illetve különdíjú telefonszolgáltatás
* Közcélú adatátviteli és béreltvonali szolgáltatások nyújtása a Hírközlési Felügyelet engedélyével
* Garantáltan jóminőségű szolgáltatás és folyamatos rendelkezésre állás, menedzselt hálózat
* A magyar államigazgatási struktúrának megfelelő, a gáz és olajvezetékek mentén telepített, főváros és megyeszékhelyek közötti zártláncú hálózat üzemeltetése
* Magasan képzett szakemberek munkájának köszönhetően, országos adatátviteli hálózat áll Ügyfeleink rendelkezésére
* A MOLTELECOM partnerei segítségével képes megvalósítani a megrendelő igényeinek megfelelő adatátviteli hálózatot

Cím: 8600, Siófok Sió u. 74. Pf:182 Tel: 06/84 505-097

MOLTELECOM

Tevékenységi kör:

* **60 éve az olajipari távközlési rendszer üzemeltetése**
* **Számítástechnikai és ügyviteli adatforgalmazás, technológiai távfelügyelet, illetve különcélú telefonszolgáltatás**
* **Közcélú adatátviteli és béreltvonali szolgáltatások nyújtása a Hírközlési Felügyelet engedélyével**
* **Garantáltan jóminőségű szolgáltatás és folyamatos rendelkezésre állás, menedzselt hálózat**
* **A magyar államigazgatási struktúrának megfelelő, a gáz és olajvezetékek mentén telepített, főváros és megyeszékhelyek közötti zártláncú hálózat üzemeltetése**
* **Magasan képzett szakemberek munkájának köszönhetően, országos adatátviteli hálózat áll Ügyfeleink rendelkezésére**
* **A MOLTELECOM partnerei segítségével képes megvalósítani a megrendelő igényeinek megfelelő adatátviteli hálózatot**

Cím: 8600, Siófok Sió u. 74. Pf:182

Tel: 06/84 505-097

TKI N

Address and contact possibilities:
TKI NETWORK LTD
H-1142 BUDAPEST
Ungvar u. 64-66, HUNGARY
Phone/Fax: (+361) 251-9078

COMPLEX ENGINEERING SERVICES FOR TELECOMMUNICATION NETWORK INSTALLATION

1. **DESIGNING**
   - network designing
   - designing microwave links
   - selecting sites
   - preparing permission plans
   - preparing installation plans
   - preparing operating and maintenance plans

2. **CO-OPERATION WITH SUPPLIER**
   - storing, asset registration
   - storing materials and equipment on site
   - domestic supplies
   - insurance administration

3. **INSTALLATION OF**
   - site survey, installing indoor and outdoor equipment and antennas
   - commissioning, tuning, equipment and link testing
   - system inspection
   - small and medium capacity digital microwave radios and multiplexes
   - SDH microwave radios and multiplexers
   - intelligent digital cross connects
   - VSAT equipment
   - UPS equipment
   - containers, towers

4. **PROGRAM MANAGEMENT**
5. **TRAINING**
6. **CARRYING OUT GUARANTEE AND MAINTENANCE TASKS**
7. **ENSURING MONITORING SYSTEM, OPERATING THE SAME**
8. **LABORATORY MEASUREMENTS**
   - type inspection in our dedicated laboratory
   - minimal tests of equipment and links
   - workshop inspection measurements of equipment
   - 24 hour climatic inspection measurements
   - measuring compliance
9. **ORGANIZING CIVIL ENGINEERING ACTIVITY, EXECUTING THE SAME**
10. **REFERENCES:**
    - Antenna Hungaria Co. LTD
    - Pannon GSM Plc.
    - MATÁV–MOTOROLA WILL
    - Hughes–Martis WILL, Czech Republic
    - ProMonte GSM, Monte Negro
    - California Microwave
    - Martis Oy
    - ELTEK AS

A Kapsch Intézményi Hálózatnak köszönhetően az információ behálózza az irodát.

LOWE | GGK

A gyors és problémamentes információtovábbítás jelentősége napról napra növekszik. Amire Önnek szüksége van, az egy, a kommunikációt leegyszerűsítő és tökéletes adatátvitelt biztosító műszaki rendszer.
A megoldás neve: Kapsch Intézményi Hálózat. A számítógépek, telefonok, nyomtatók, faxok és beszédüzenetrögzítők mind-mind ehhez az egyedi igényekre kidolgozott belső kommunikációs rendszerhez csatlakoznak.
A beszéd- és adatátvitelen kívül képek, videofelvételek és multimédia programok továbbíthatók gyorsan és pontosan: helyben, regionálisan és globálisan egyaránt. A Kapsch Intézményi Hálózatok termékcsalád a digitális irodai rendszerektől és az ISDN-től a rádióhálózatokig és adatrendszerekig terjed. A felhasznált technológiánál természetesen csak egy lehet fontosabb: az Ön cége számára kifejlesztett, testreszabott szolgáltatás.
Ha szeretne többet megtudni a Kapsch Intézményi Hálózatokról, már most beszéljen a Kapsch-sal:
Kapsch Telecom Kft.,
1113 Budapest, Bocskai út 77-79,
tel: (1) 209-2110, fax: (1) 209-2111

KAPSCH
the communications company

ERICSSON *tények*

75 000 000

Az ERICSSON mobiltelefon-rendszereit világszerte több mint **75 millió** előfizető használja.

34 000 000

Az ERICSSON új **GSM 1800**-as és GSM 900-as rendszereihez csatlakozik a világ GSM-előfizetőinek közel fele, mintegy 34 millió ember.

100 000

Az ERICSSON a világ egyik vezető távközlési cége. Ezt 100 ezer felkészült és tehetséges munkatársa **szakértelmének** köszönheti.

78 000

Az ERICSSON rendszereit használó mobiltelefon-előfizetők száma világszerte **naponta** 78 000-rel nő.

130

Az ERICSSON a világ 130 országában **elismert szállító.** Ehhez az üzleti sikerhez a maga innovatív értékeivel négy regionális szakértői központ is hozzájárul.
Ezek egyike **Magyarországon** található.

20

Az ERICSSON bevételeinek több mint 20 százalékát fordítja **kutatásra** és **fejlesztésre.** Infokommunikációs rendszereiben mindig ott van az a **többlet,** amely méltán teszi az ERICSSON-t a távközlési világpiac legjelentősebb szereplőjévé.

Nº 1.

Annak, aki az első helyen áll, nagy a felelőssége. Az ERICSSON soha nem feledkezik meg a **legfontosabbról:**

A lényeg az emberek közötti kommunikáció. A többi – technológia.

ERICSSON

Ericsson Kft., 1037 Budapest, Laborc u. 1., Tel.: 437-7100, Fax: 437-7467, http://www.ericsson.hu

One obtains a frequency sensitive bistable power response:

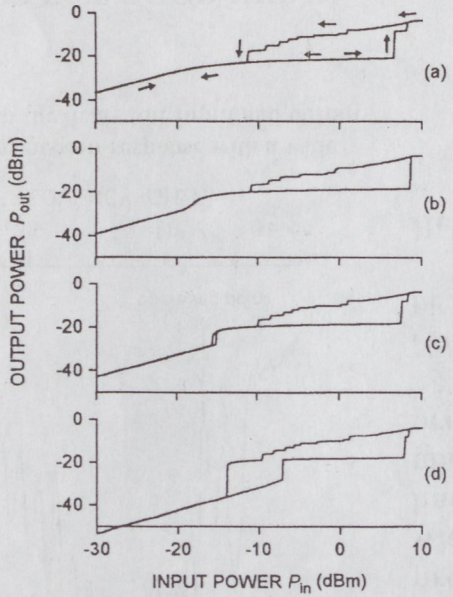
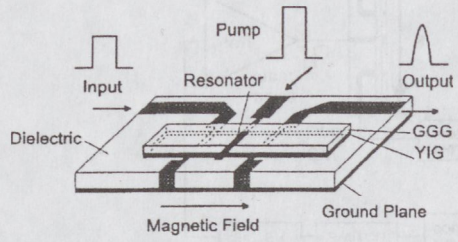


Fig. 22. Output power vs. input power bistable response curves for different frequency operating points.

Main drawback: Magnetic field feedback is response time limited by the inductance of the feedback coil. Typical response times for the bench set-up are milliseconds.

Parametric Based MSW Devices:

VI. Soliton Parametric Amplifier.



Input pulse at frequency f_s

Pump at frequency

$$f_p = 2f_s$$

Timing is critical. Pump just as the signal pulse passes the resonator.

Result is impressive:

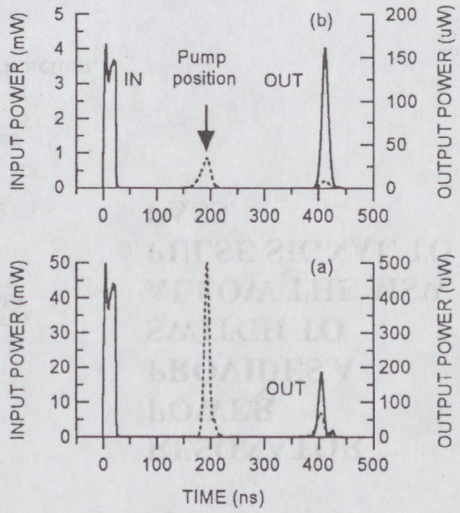
Fig. 23. Parametric pumping pulse data.

Input pulse:
4.01 GHz, 22 ns

The resonator pulse:
8.05 GHz and 5 W.

Dashed pulses at 200 ns show the MME pulse at resonator position.

Dashed pulses at 400 ns show output without pumping.



(a) 50 mW input pulse: SOLITON AMPLIFICATION
(b) 4 mW input pulse: LINEAR MSW PULSE → SOLITON

GAIN FACTORS: 22 dB (low power) 8 dB (solitons)

VII. Wide Resonator Gate Switch

Wide resonator causes an anomaly in the transmission response of the delay line:

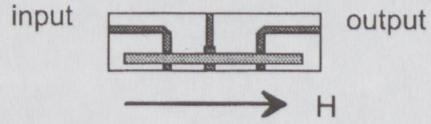


Fig. 24. Wide resonator delay line structure.

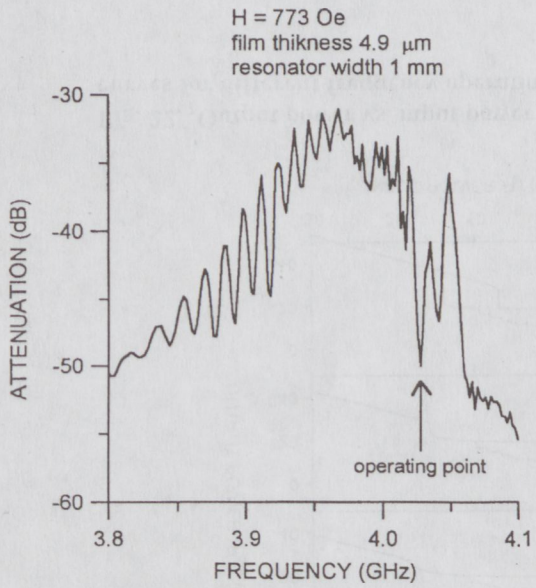


Fig. 25. MSBVW transmission response with a wide microstrip line between the delay line input and output transducers.

The sharp notch in the transmitted power is due to the discontinuity presented by the wide resonator strip line element in the middle of the propagation path.

Normally this would be BAD!

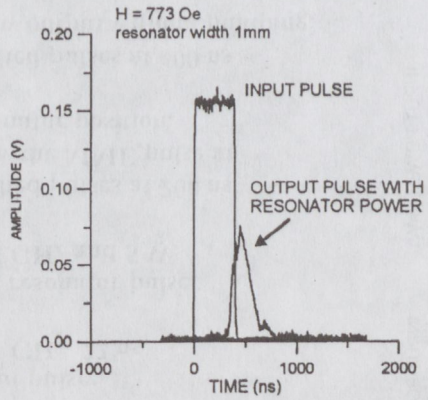
Here it is good!

WHY IS THIS EFFECT GOOD HERE?

PULSE RESONATOR POWER AT $f_p \approx 2f_s$

CHANGES THE "OFF"POWER CONDITION TO AN "ON" CONDITION.

LOOK AT THE EFFECT ON A GIVEN OUTPUT PULSE (OR LACK THEREOF):



RESONATOR POWER PROVIDES A SWITCH TO ALLOW THE MSW PULSE SIGNAL TO PASS.

Fig. 26. Wide resonator microwave switch action.

VIII. Resonator Based Phase Detector

THIS WIDE RESONATOR STRUCTURE HAS ANOTHER PROPERTY WHICH MAY BE VERY USEFUL:

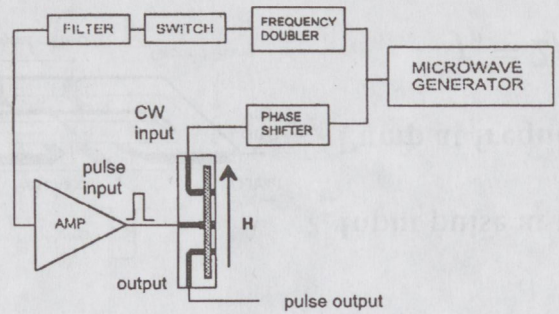


Fig. 27. Wide resonator MSW switch configuration with variable phase shift.

OUTPUT POWER PHASE RESPONSE IS EXTREMELY LARGE.

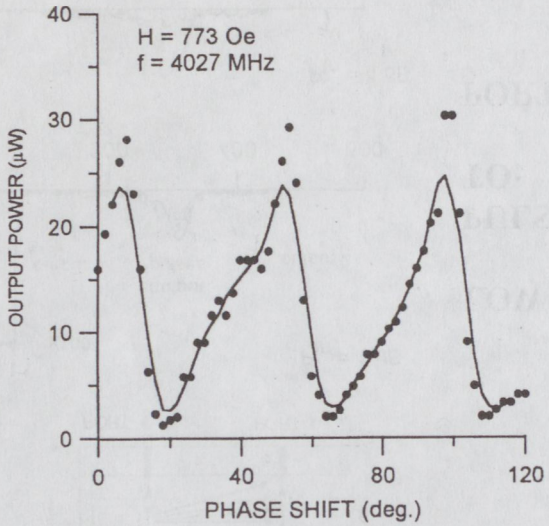


Fig. 28. Phase response of wide resonator delay line switch.

PHASE SHIFT INTRODUCED FOR INPUT CW SIGNAL:

PHASE RESPONSE PERIOD IS 45°

IF PHASE SHIFTER IS PLACED JUST BEFORE DOUBLER:

PHASE RESPONSE PERIOD IS 90°!

IX. Switch based on Soliton Dragging (Preliminary Results).

RESONATORS PRODUCE A THIRD EFFECT:

SOLITON DRAGGING

A PROPAGATED SOLITON PULSE CAN BE DELAYED BY THE APPLICATION OF PULSE MICROWAVE POWER TO THE RESONATOR.

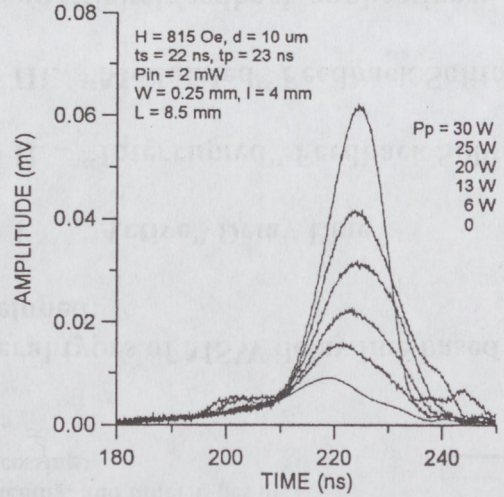


Fig. 29. Preliminary demonstration of soliton dragging.

WITH INCREASING PUMP POWER, THE SOLITON PULSE IS NOT ONLY AMPLIFIED.

IT IS ALSO DELAYED IN TIME.

IN OPTICS, THIS IS USED FOR SWITCHING ACTION.

SHOULD BE POSSIBLE FOR MICROWAVE DEVICES TOO!

X. Soliton Self Focusing Switch (some initial results).

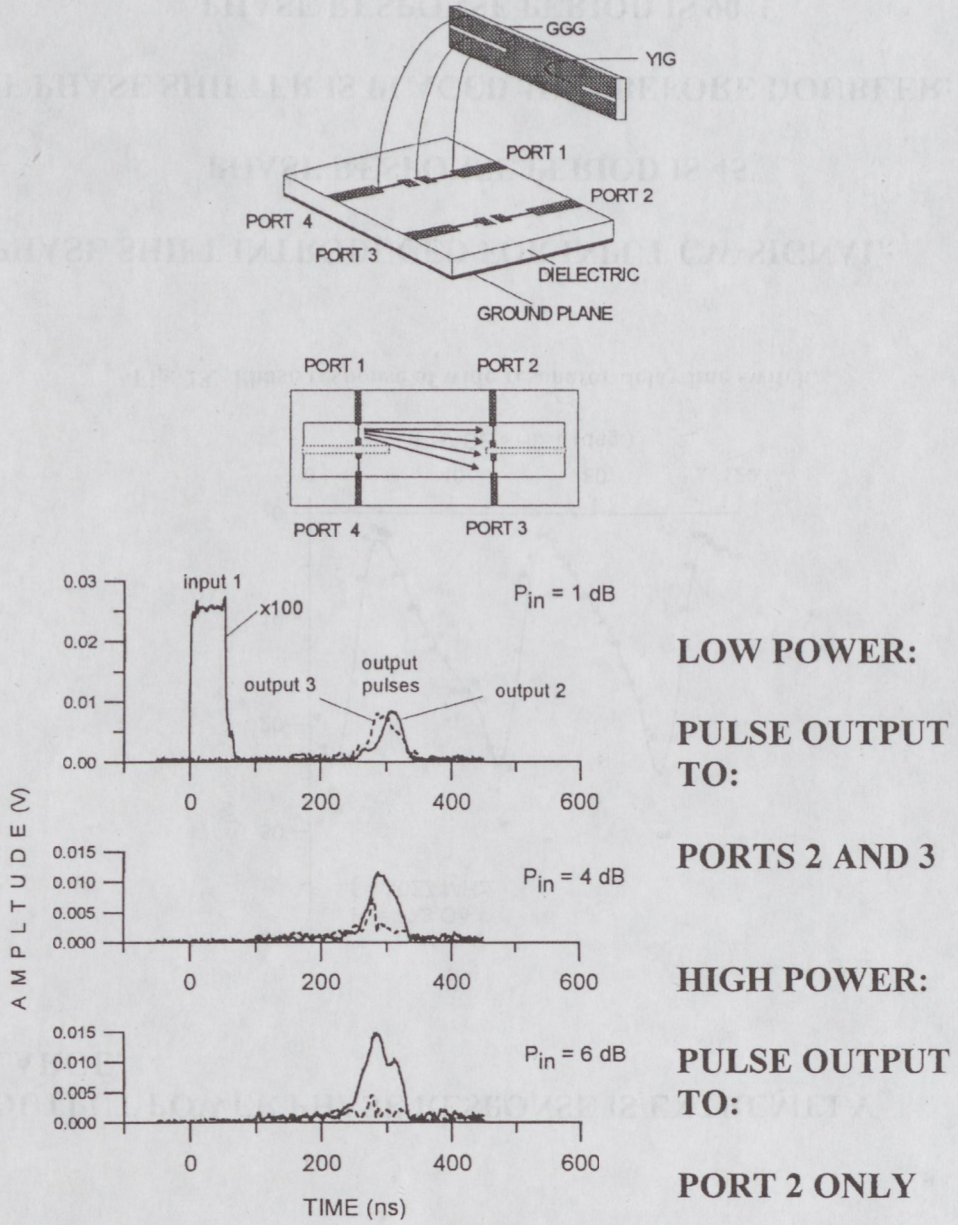


Fig. 30. Demonstration of self focusing soliton switch principle.

LOW POWER:

PULSE OUTPUT TO:

PORTS 2 AND 3

HIGH POWER:

PULSE OUTPUT TO:

PORT 2 ONLY

SUMMARY

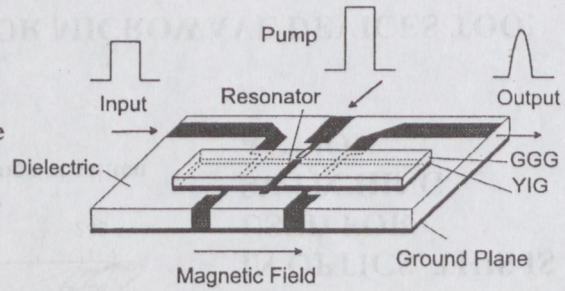


Fig. 31. Microstrip structure with input, output, and center antenna/ resonator elements for soliton pulse generation, amplification, delay, switching, and other types of processing.

Several types of MSW delay line based feedback devices developed:

I. "Active" Delay Line

II. "Interrupted" Feedback Soliton Train Generator

III. "Modulated" Feedback Soliton Oscillator

Two additional feedback applications:

IV. Feedback Controlled Bistable MSW Oscillator

V. MSW Interferometer with Bistable Power Response

Special "new concept" devices:

VI. Soliton Parametric Amplifier

VII. Wide Resonator Gate Switch

VIII. Resonator Based Phase Detector

IX. Switch based on Soliton Dragging

INTERNET A JOG HATÁRÁN

VEREBICS JÁNOS

HANGA@MAIL.MATAV.HU; HTTP://WWW.EXTRA.HU/VEREBICS

Az Európai Unió keretein belül folyó, az Internetet érintő jogalkotási és jogalkalmazás-koordinációs munka igen fontos állomását jelenti az Akcióterv, melyet 1998. december 21-én a Tanács elfogadott, s mely 1999. január 1-től hatályba is lépett. Az EU ezzel kapcsolatos sajtóközleménye (magyar fordítása a Függelékben), az EU Newsdesk tömör híre (Combatting illegal and harmful content: EU adopts Action Plan on promoting safer use of the Internet, http://www2.echo.lu/news.index.html, 1998. december 28.) kiemeli: az 1999 márciusig terjedő időszakban igen komoly munka vár a Tagállamok képviselőiből álló bizottságra. Az akcióterv valóra váltásának pontos és teljes forgatókönyvét igen széles körű összefogással kell elkészíteni. A munka tehát megkezdődik, egyelőre nélkülünk. Mennyiben érinti ez az Uniós csatlakozásra készülő Magyarországot, átformálja-e a magyar Internetet, s milyen hatással lesz jogunkra, s hol tapasztalható máris érdemi fejlődés? E kérdésekre keresi a választ ez az írás.

1. UNIÓS AKCIÓTERV: AZ ÖNSZABÁLYOZÁS FELÉRTÉKELŐDÉSE

1.1. Az európai jogalkotás folyamatának áttekintése

Első lényeges állomása az Európai Bizottság *Az Internet jogellenes és ártalmas tartalmáról* szóló 1996. október 16-i *Közleménye* volt (COM/96/487, http://www.echo.lu/legal/en/internet/communic.html), mely széles körű parlamenti vita, s a Régiók Bizottsága véleményének figyelembe vételével került kialakításra. Már ez a dokumentum is „haladéktalan akciókat" irányzott elő az Internet ártalmas és jogellenes tartalmának kezelésével kapcsolatban.

A Telekommunikációs Tanács 1996. szeptember 27-én létrehozott egy munkacsoportot, mely kifejezetten szakmai szempontból (az Internet szolgáltatók bevonásával) konkrét ajánlásokra kapott megbízást. Első jelentését a Tanács 1996. november 28-i ülésére terjesztette elő (http://www.echo.hu/legal /en/internet/wpen.html). Több lényeges kérdés mellett igen komoly formában foglalkoztak az önszabályozás s a felelősség kérdéskörével is. Ezt követte második jelentés (ezt 1997. június 27-i ülésén vette napirendre a Tanács, http://www.echo.lu/legal/en/internet/wp2en-toc.html), melyben már a nemzetközi kitekintés, az egyes tagállamok s Uniós intézmények idáig elért eredményeit, törekvéseit is értékelték.

Az első lépcső lezárását a Tanács Határozata (*Resolution on the Illegal and Harmful Content on the Internet*, elfogadva: 1997. február 17.) jelentette (http://www.echo.lu/legal /en/internet/resol.html). E dokumentumban már nem csak célokat fogalmaztak meg, de a cselekvés fő irányait is kijelölték.

1997. április 24-én az Európai Parlament elfogadta — Pierre Pradier jelentése szerint — az Internet jogellenes és ártalmas tartalma elleni küzdelem egyik kulcsdokumentumát (*Resolution on the Commission Communication on Illegal and Harmful Content on the Internet*, http://www.europrl.eu.int/dg1/a4/en/a4-97/a4-0098.htm). Ez már a konkrét keretmunka megvalósítására vonatkozott.

Az EU több más akcióterve, cselekvési programja is tartalmazott az Internet megrendszabályozásával kapcsolatos lényeges elemeket. (*Rolling Action Plan on the Information Society, 1996. december, illetve a Zöld Könyv a Kiskorúak és az emberi méltóság audiovizuális és információs szolgáltatások terén való védelméről*, (COM/96/ 483, http://www.europa.eu.int/record/green/gp9610/protec.htm, mely ugyancsak 1996. október 16-án került — a jogtalan és ártalmas kommunikáció elleni Közleménnyel együtt — elfogadásra). Ezt a Zöld Könyvet nagyon széles körben vitatták meg, s szakmai vélemények figyelembe vételével tovább formálták (lásd ehhez: http://www2.echo.lu/legal/en /internet/gpconsult.html), mígnem elkészült a jelentés végső változata Philip Whitehead előterjesztésében. Ezt az Európai Parlament 1997. október 24-én fogadta el.

Lényeges állomásnak számított az 1997. július 6-8. között Bonnban megrendezett Nemzetközi Miniszteriális Konferencia is, melynek 29 résztvevője a „Globális információs hálózatok: megvalósítani, ami bennük rejlik" (*Global Information Networks: Realising the Potential*) gondolat jegyében három deklarációt fogadott el (lsd. http://www2.echo.lu/bonn/final.html): a miniszterekét, az iparét s a felhasználókét. A miniszteri deklaráció lényeges eleme volt a szolgáltatások tartalomfüggvényű besorolásának támogatása.

Más téren — szervezett bűnözés elleni küzdelem, az információs társadalom oktatási, nevelési kérdéseivel foglalkozó 1996-98-as Akcióterv stb. — ugyancsak lényeges, az Internetet is érintő összefüggésekben fogalmaztak meg követelményeket.

Mindezekre — s ez a szövegben kifejezetten meg is jelenik — a december 21-én elfogadott új Akcióterv tudatosan épít. Maga az Akcióterv is hosszas előkészítő folyamat révén nyerte el végleges formáját. Első változata a weben ftp://ftp.echo.lu/pub/legal/en/internet/actplan.rtf alatt már hónapok óta hozzáférhető volt: a Tanács Közleménye nem csak az Akcióterv előzetes szövegét tartalmazta, de a jogalkotási folyamat hátterét is megvilágította.

Az Akcióterv szervesen illeszkedik a legújabb EU kezdeményezésekhez (*Council Recommendation on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity*, elfogadva: 1998. szeptember 24).

Az egyes nemzeti jogalkotások idáig is lényeges lépéseket tettek már az ártalmas és jogellenes tartalmak korlátozása terén, több ország is elkészítette saját, átfogó, a kérdést minden szempontból megvilágító tanulmányát, a jog-

alkotás munkatervét. (Pl. Anglia, vagy a nem Uniós országok közül Svájc). Mindezek a törekvések most összehangolva, s ami lényeges: az EU költségvetéséből is komoly anyagi támogatást kapva válnak majd valóra.

A „jog nélküli Internet" mítosza végképp elenyészik.

1.2. Az Akcióterv: ami mögötte van

Két előzetes kérdésre mindenképpen válaszolni kell, mikor az amúgy nem túl terjedelmes dokumentum vizsgálatába fogunk. Az egyik: mi számít „jogellenes és ártalmas" tartalomnak, a másik: kell e tartani a cenzúrától (amelyre az Akcióterv szerint technikailag széles körben nyílna lehetőség).

Az Akcióterv a „jogellenes és ártalmas tartalom" kifejezés alatt *nem csak a gyermekpornográfiát* érti. Ide tartoznak a nemzetbiztonsági kérdések (bombák készítéséhez adott segítségnyújtás, illegális kábítószer-előállítás, terrorista tevékenység), a kiskorúak (a marketing molesztáló jellegű formái, erőszak, pornográfia), az emberi méltóság (faji gyűlöletkeltés, faji megkülönböztetés), a gazdasági biztonság (csalás, hitelkártyákkal való kalózkodáshoz való segítségnyújtás), információbiztonság (rossz szándékú hacking), a magánszféra (személyes adatokkal való visszaélés, elektronikus zaklatás), a személyiség (rágalmazás, meg nem engedett összehasonlító reklám), szellemi tulajdon (copyright által védett művek, szoftver és zene jogosulatlan terjesztése) védelme is.

„Ártalmas tartalom" lényegében az, amely ugyan a véleménynyilvánítás szabadsága keretei között terjeszthető, mégis indokolt hozzáférhetőségét csak bizonyos körben (pl. csak felnőtteknek) biztosítani, másokat (kiskorúak) azonban – épp az ő védelmükben – a hozzáférésben meg kell gátolni.

Az Akcióterv lényegében ennek technikai, jogi feltételrendszerét kívánja össz-európai szinten megteremteni.

Jelentheti e ez a cenzúra valamilyen formában való megjelenését? E kérdés már az előkészítő munka korai szakaszában felvetődött (lsd. *European Comission Legal Advisory Board: Response to the Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services*, 3.2, http://www2.echo.lu/legal/en/internet/gpalabreply.html).

Az Emberi Jogok Európai Egyezményének 10. cikke az, amiből a jogalkotó kiindult.

E cikk első pontja általános alapelvként szögezi le, hogy mindenkinek joga van a véleménynyilvánítás szabadságához, majd részletezi ennek a jognak tartalmát is (véleményalkotás szabadsága, az információk, eszmék megismerésének és közlésének szabadságát országhatárokra való tekintet nélkül s a nélkül, hogy ebbe hatósági szerv beavatkozzon). A 10. Cikk 2. Pontja azonban azt is tartalmazza: „E kötelezettségekkel és felelősséggel együtt járó szabadságok gyakorlása a törvényben meghatározott olyan alakszerűségeknek, feltételeknek, korlátozásoknak vagy szankcióknak vethető alá, amelyek szükséges intézkedéseknek minősülnek egy demokratikus társadalomban a nemzetbiztonság, a területi sérthetetlenség, a közbiztonság, a zavargás vagy bűnözés megelőzése, a közegészség vagy az erkölcsök védelme, mások jó hírneve vagy jogai védelme, a bizalmas értesülések közlésének megakadályozása, a bíróságok tekintélyének és pártatlanságának fenntartása céljából." Az Európai Bizottság joggyakorlata (*Castells v. Spain, Piemenont v. France*) következetes, és nem enged kiterjesztő jellegű értelmezést. (lsd. ehhez *dr. Grád András: Kézikönyv a strasbourgi emberi jogi ítélkezésről, HVG-Orac, Budapest, 1998. 283. skk*). Maga a többször hivatkozott Zöld Könyv is megjelöli a lehetséges korlátozások feltételeit: jogszabály által előírt, szükséges, a létező, egy demokratikus társadalom értékrendszerével és szükségleteivel összhangban lévőnek kell lenniük, mely körön belül kiemelték a közegészségügyet, közerkölcsöt, a kisebbségek s az emberi méltóság védelmét (*Green Paper, Annex III*).

Kétségtelen, hogy az Akcióterv bizonyos körben korlátozásokat fog bevezetni. E korlátozások bizonyos fokú aggodalomra adhatnak okot: az első szakmai reakciók a veszélyekre figyelmeztetnek.

Erich Moechel a *Telepolis* december 23-i számában a terv szerint létrehozandó forró vonalak és az önkorlátozás kérdésével foglalkozik. Ezek kétféleképpen működhetnek: az érintett szereplők belátása révén (a klasszikus értelemben vett önkorlátozás) – vagy harmadik személyek (szoftver) beavatkozásával.

A britek az első verziót támogatnák, az olaszok és franciák a másodikat. Decemberben már számos jele volt annak, hogy a német és osztrák hatóságok nem várják be az akcióterv hatályba lépését: mint arról hétről hétre olvashattunk, egymást követték a szolgáltatókat együttműködésre bíró intézkedések, az ISPA létrehozta a gyermekpornó és újnáci oldalak bejelentését segítő hot-line vonalát. Ez azonban nem váltotta be a hozzá fűzött reményeket: az első 14 napban – mutat rá Moechel – nem érkezett olyan bejelentés, mely valóban jogellenes anyaghoz vezette volna a hatóságokat. Egyes elektronikus postaszolgáltatók buzgalmukban tovább mentek, s nem csak a gyerekpornó eltávolítását vállalták fel, hanem a jobb- és baloldali extremitást, rasszizmust, kábítószerek, vallási eszmények megsértése körét is. Különösen felháborította az osztrákokat az AON dicstelen szereplése. A szolgáltató – mutatnak rá többen is – nem veheti át a cenzor szerepét. Egyes szolgáltatók ezt eleve elutasítják, mások viszont a kelleténél is nagyobb lendülettel teszik.

A veszély tehát nem elhanyagolható. Ezzel azonban az Uniós jogalkotási folyamat résztvevői is tisztában voltak, vannak. Épp ezért fontos állomás az Akcióterv, amelynek valóra váltása közös munka révén, az Internet-ipar, a szolgáltatók, a felhasználók bevonásával történik majd. Ez a munka most, 1999 márciusában veszi valóban kezdetét. A terv maga – sajátos egybeesés – 2002-ig irányozza elő a tennivalókat. Legkorábban ez az az év, amikor Magyarországból is az Unió tagja válhat. Hazánk tehát már egy olyan Uniónak lesz tagja, amely (sok minden más mellett) az Internetre is jogi és jogon kívüli (Viselkedési Kódex) normákat alkotott, forró vonalakat működtet, szűrőket tett kötelezővé, ahol követelmény a weblapok „címkézése", ahol szigorú minőségi követelmények szerinti besorolással kerülhetnek új oldalak a hálóra.

Az Unió célja – s ez többször is megjelenik a dokumentumokban – *összeurópai* szabályozás. Egy „jogon kívüli" magyar, lengyel, szlovák Internetnek előbb vagy utóbb akkor is alkalmazkodnia kell az Uniós elvárásokhoz, ha ezt a játéktér egyes szereplői (felhasználók, szolgáltatók) nem

akarják. Az Uniós jogharmonizáció keretében az európai Internet joga valószínűleg előbb lesz a magyar jog része, mint országunk a Közösség tagállama.

Nem látok más utat, mint ennek az európai normarendszernek elfogadását, a magyar Internet „megszelídítését". Ahhoz azonban, hogy a magyar Internet érdekeit megjelenítsük, hogy a „nemzeti sajátosságokat" érvényre juttathassuk, igen komoly, az Internetes közösség s a kormányzati szervek együttműködésére alapuló munkának kellene megkezdődnie – méghozzá nagyon hamar.

Korábbi írásaimban már sokszor hangsúlyoztam: az állam, a közhatalom ott avatkozik be, ott érvényesíti a jogot, ahol más viselkedési normák nem elegendőek, nem elég hatékonyak, s a nem jogi szankcióknak nincs visszatartó erejük. Az Akcióterv által körvonalazott új európai Internet nem arra törekszik, hogy a jog eszközeivel teremtsen szabályozást. Egy bizonyos körön kívül azonban már be fog lépni a jog. Kérdés, hogy a hatályos magyar jogi szabályozás képes e erre, a más életviszonyokat rendező korábbi törvényeink, rendeleteink alkalmazhatók e az Internet virtuális világára is?

2. ÖNSZABÁLYOZÁS ÉS KORLÁTAI: FELEL-E A SZOLGÁLTATÓ?

E sorok szerzője a hazai Internet-ügyben a magánvádlói (feljelentői) álláspont jogi kifejtését segítő tanulmányában (A tér, a szabadság és a normák) feltette a kérdést: *mi alapozza, alapozhatja meg – hatályos polgári jogunk szerint – a szolgáltató polgári jogi felelősségét olyan anyagok közzétételéért, melyek* – polgári vagy büntetőjogi értelemben véve – *mások jogait, illetőleg a büntető jogszabályokat sértik*?

A válasz: *mindkét, a konkrét ügyben érintett szolgáltató általános szerződési feltételekkel köt tárterület igénybe vételére vonatkozó szerződést magánszemélyekkel. Ingyenes hozzáférést biztosítanak (miközben működési költségeiket hirdetési bevételekből fedezik). A szolgáltatást igénybe venni kívánóknak olyan tartalmú szerződést kell elfogadni, mely a személyiségi jogok védelmét, az üzleti és politikai célú felhasználás kizárásának klauzuláját tartalmazza, illetve felsorolja azokat az eseteket, mikor a szolgáltatás üzemeltető részéről felfüggeszthető vagy megszüntethető: részben politikai tevékenységhez kapcsolódó vagy azt elősegítő anyagok, információk, részben a rágalmazó anyagok tartoznak ide. Ezek közzétételétől való tartózkodásra tehát az egyik szerződő partner (a magánszemély tárhelybérlő) kötelezettséget vállal (és viseli a szerződésszegéssel kapcsolatosan felmerülő kárt), ugyanakkor a bérbe adó az elvárható magatartás (azaz a másik fél szerződésszerű teljesítésének ellenőrzése) elmulasztásáért felel.*

Véleményemet kezdetben nem sokan osztották. Az általános reakció – többek között a mostani ügyben érintett extra részéről is – az volt, hogy a szolgáltató a tartalomért nem felel, csak a tárhelybérlővel szemben van helye polgári (esetleg büntető) igény érvényesítésének.

Dr. Kiss Zoltán a Computer Technika 1998. október 27-i számában megjelent írásában (*Internet és szerzői jog*) mutatott rá, hogy az Internet a korlátlan szabadság látszatát hordozza magában, ami azt sugallja, hogy ebben a közegben jogi tiltások, előírások nem érvényesülnek.

A felelősség kérdésében ugyancsak helyesen tett különbséget a hozzáférést biztosító szolgáltatók (*service providers*) és tartalomszolgáltatók (*content providers*) között. Az amerikai joggyakorlat kapcsán *dr. Kiss Zoltán* arra is utalt, hogy a bíróság – szerzői jogi jogsértésért – többször megállapították már a hozzáférés-szolgáltatók felelősségét is, ha azok egyébként tudtak a jogsértésről.

Ugyancsak a Computer Technika adott hírt – a Számítástechnika közlése alapján – arról (1998. november 3.), hogy *Katona Kálmán* hírközlési miniszter szerint az Internet szolgáltató felel az általa nyújtott szolgáltatás tartalmáért, hisz módjában áll ellenőriznie a tartalmat, csak rá kell szánni az időt. A hírközlési miniszter ezt nem tekinti cenzúrának, mivel szerinte vannak általában társadalomellenesnek tartott dolgok, amelyeket nem szabad a hálózaton publikálni.

A legismertebb amerikai szabad szerver, a tripod szolgáltatási feltételei (http://www.tripod.com/membership/signup/tos.html) 10. pontja szerint a tripod-nak lehetősége van arra, hogy minden olyan információt, kommunikációt, adattovábbítást vagy weboldalt bármikor, külön figyelmeztetés nélkül **töröljön**, ha az a tárhelybérleti szerződés bármely pontját, vagy a tripod politikáját vagy irányelveit sérti. Azt pedig az amerikai szerződés is igen részletesen sorolja fel, hogy mi „nincsen megengedve" (az udvarias angolt nyers magyarra fordítva: mi van tiltva) a websiteokon. Első közöttük a szerzői jog által védett anyagok a szerző vagy jogtulajdonos hozzájárulása nélküli közzététele, második a 18 éven aluliak képi védelme (lsd. *Tripod Services And Conditions Of Use, 3. i-vii*).

A legfontosabb különbség azonban az, hogy a tripod – az amerikai jog szerint jogszerűen – zárja ki illetőleg korlátozza saját felelősségét a bérbevett tárhelyen elhelyezett site tartalmáért: annak minden jogi kockázatát a bérlő viseli (*8. Limitations of Liability and Warranty*). Massachusetts állam joga (amelyet a felek a jogviták esetére kikötnek, mint ahogy a pereket kizárólagos alávetéssel Massachusetts állam szövetségi bíróságai folytathatják le) a felelősség ilyen kizárását megengedi. A hatályos magyar polgári jog azonban *nem*.

A szolgáltató és a tárhelybérlő között polgári jogi szerződés jön létre, meghatározott feltételekkel. Csak emlékeztetőül: a bérlő ingyen kap 6 megát, melynek fejében két kötelezettséget vállal. Egyrészt a *tűrést* (annak elviselése, hogy a bérbe adó reklám anyagokat helyezhet el a bérlő oldalán), másrészt a *tartózkodást* (a szerződésszegő magatartástól).

A szerződési szabadság értelmében a felek a szerződés tartalmát akaratuknak megfelelően állapítják meg (diszpozitivitás). A jog bizonyos körben azonban áttöri e szabadságot: egyes, a felelősséget kizáró vagy korlátozó szerződési feltételeket (Ptk. 342. §) a szerződés semmisségét maga után vonó tényezőként értékel.

Abban az esetben azonban, ha a károkozás nem a szerződő felek közötti jogviszonyban következik be (az Interneten a bérlő által közzétett anyag mások, harmadik személyek jogait sérti), *szerződésen kívüli károkozásról* van szó. Ebben az esetben a károsultat semmilyen szerződési jogviszony nem fűzi a felekhez (a tárhelybérleti szerződés két alanya a bérbe adó és a bérlő), azonban őt az Internetes közzététel révén kár (pl. vagyoni hátrány) éri.

Kitől követelheti kára megtérítését? Hatályos polgári jogunk szerint attól, aki neki jogellenesen kárt okozott (Ptk.

339. § /1/). A károsultat nem érdekli, hogy a tárhelybérlő és bérbe adó között milyen szerződés van érvényben, s hogy ebben (jogszerűen vagy sem) milyen felelősséget kizáró tényezőkben állapodtak meg.

A Ptk. 342. § (1) bekezdése értelmében semmis valamely szerződésnek az a kikötése, amely a szándékos vagy súlyos gondatlanságból eredő károkozásért, életben, testi épségben, egészségben okozott károsodásért, továbbá bűncselekmény következményeiért való felelősséget előre korlátozza vagy kizárja. Miután kártérítési jogunk egységes (Ptk. 318. § /1/), a felek szerződésükben a fenti körben a szerződésen kívüli károkozásért sem zárhatják ki hatályosan a felelősséget.

Az a tárhelybérlő, aki a bérbe adóval kötött szerződést tudatosan megszegi (azaz vállalt kötelezettsége ellenére olyan anyagokat helyez el ott, melyeket a bérleti szerződés értelmében nem lett volna szabad) „jobb esetben" csak *súlyosan* gondatlanul, rosszabb esetben szándékosan cselekszik.

Egy további kör, ahol a felelősség korlátozása vagy kizárása nem érvényesülhet a bűncselekménnyel okozott károk köre. Az Internet segítségével sokféle bűncselekmény követhető el: ezek vagyoni és személyi jogokat egyaránt sérthetnek.

Álláspontom *A tér, a szabadság és a normák* megjelenése óta nem változott. A kérdésre, hogy *beszélhetünk e a szolgáltatók büntetőjogi értelemben vett felelősségéről, terheli e őket legalább gondatlanság annak vonatkozásában, hogy szerverükön olyan anyagok jelenhettek meg, melyek tartalma büntetőjogi szankcionálást tesz szükségessé? a válasz: a szolgáltatókkal szemben nem helyes (fair) a büntetőjogi eljárás, felelősségre vonás kezdeményezése. Az a magánszemély, aki az Internettel visszaélve, annak felhasználásával bűncselekményt követ el, viselje ennek büntetőjogi konzekvenciáit. A szolgáltató, aki jogi személy (vagy jogi személyiséggel nem rendelkező gazdasági társaság) e minőségben büntetőjogilag nem tehető felelőssé, a képviseletére jogosult személy megbüntetése pedig sem igazságos, sem célszerű nem lehet. Viselnie kell azonban – a cégnek – mulasztása civiljogi következményeit.*

A szolgáltató az általános kártérítési alakzat (Ptk. 339. § /1/) szerint mentesülhet a felelősség alól, ha bizonyítja: úgy járt el, ahogy az az adott helyzetben általában elvárható. A szolgáltatásbiztosítók legtöbbször azzal védekeznek, hogy nincs sem idejük, sem emberük (röviden módjuk) arra, hogy minden egyes weboldal minden egyes változását percre készen ellenőrizzék (azaz szerződésszerűségi szempontból felülvizsgálják).

Az *adott helyzetben általában elvárhatóság* szintje nyilván nem is ezt jelenti. Jelenti viszonyt az oldalak rendszeres, (szúrópróbaszerű vagy tematikus) végiglátogatását, s jogsértő tartalom saját, vagy külső figyelemfelhívó bejelentés alapján történő észlelése esetén felhívást a helyzet megszüntetésére.

Ez azonban még nem cenzúra: egy polgári jogi szerződés vállalt kötelezettségeinek betartására való felhívás. Ami – ha elmarad – súlyos szerződésszegésnek minősül bérbevevő részéről, s e szerződésszegő magatartása egyik szankciója a bérleti jogviszony azonnali felmondása (is) lehet.

Továbbra is vallom: *nem a jognak, a külső beavatkozásnak kell a világ legnagyszerűbb médiumát, az Internetet irányítani.* Ha azonban a weben a szabadosság, nem a szabadság, a az egyéni akarat kíméletlen érvényre juttatása, s nem az érdekek kölcsönös tiszteletben tartása uralkodik el, a jog (közhatalom) nyilván lépni fog, hogy a „rendet" s a „biztonságot" helyreállítsa. Ehhez azonban a jogi környezet megteremtése elengedhetetlen: elsősorban a felelősség kérdéskörét kellene törvényi szinten tisztázni.

A közelmúlt Internetes botrányai (kukkoló, s a hírességek arcát pornófotókra „kasírozó" CEL-EB oldalak) a személyiségi jogok védelmének vagy védhetetlenségének kérdésén túl a szex, illetőleg pornó jogi szabályozásának ellentmondásaira, elégtelenségére is ráirányítják a figyelmet. Ugyanakkor a jogszabályok hiánya itt is bizonytalansághoz vezethet.

3. EXTREMITÁS A HÁLÓN: MEGENGEDETT ÉS TILALMAS SZEX, PORNOGRÁFIA

3.1. A szex, mint áru: a forgalmazás szabályai

A magyar jogalkotás immár lassan egy évtizede nem tud (vagy nem akar) mit kezdeni a pornográfiával. A jogi szabályozás hajnalán, 1990-ben (fejest ugorva a „pógári" demokráciába) a szexuális áruk kérdésköre is napirendre került: napvilágot látott 6/1990. (IV. 5.) KeM rendelet az üzletek működéséről szóló rendelet.

Kimondta: szexuális áru – a többi árutól elkülönítve – csak zárt csomagolásban hozható forgalomba. A 18. életévét be nem töltött személy részére szexuális árut értékesíteni, kölcsönözni (értékesíteni), valamint ennek során ilyen áru megtekintését lehetővé tenni tilos. Szexuális árut közterületen vagy kirakatban elhelyezni, közszemlére tenni tilos volt. Volt egy további megkötés is: szexuális áruk üzlete nem működtethető ott, ahol az üzlet bejáratától számított 200 méteres körzetben alsó és középfokú oktatási, gyermek-, ifjúságvédelmi, valamint vallás gyakorlására szolgáló intézmény van. A rendelet tartalmazta a szokásos „gumiparagrafust" is, mikor kimondta: az üzlet működése nem zavarhatja a lakosság nyugalmát.

Szerencsére az értelmező rendelkezés sem maradt el, s a jogalkalmazóknak nem kellett többé sötét tudatlanságban vergődniük. Végre megtudhatták, mi a szexuális áru: minden olyan irat, kép, reprodukció, plakát, könyv, folyóirat, film, műsoros videokazetta, vagy egyéb termék, amely a nemi aktust, elsődleges nemi szervet, vagy szerveket közvetlenül ábrázolja továbbá egyéb, a szexuális élettel közvetlen összefüggő tárgy (segédeszköz), kivéve a szabadforgalmazású egészségügyi cikkeket.

Nem sokkal később már az Alkotmánybíróság előtt volt a szex szabadságának kérdése. Szentendre önkormányzata kerek-perec önkormányzati rendelettel betiltotta a szexuális áruk forgalmazását a városban. A köztársasági megbízott fellépése nyomán azonban az Alkotmánybíróság a kérdéses rendelet megsemmisítése lett. Ez úttal a (törvényi keretek közötti) szabadság diadalmaskodott...

A jogban az a szép, hogy folyton változik: 1997-ben hatályba lépett az üzletek működéséről és a belkereskedelmi tevékenység folytatásának feltételeiről 4/1997. (I. 22.) Korm. rendelet, melynek 14. §-a szerint szexuális áru – a többi árutól elkülönítve – csak zárt csomagolásban hozható forgalomba. A 18. életévét be nem töltött személy

részére szexuális árut értékesíteni, kölcsönözni (a továbbiakban együtt: értékesíteni) tilos. Tilos továbbá szexuális árut közterületen vagy kirakatban elhelyezni, közszemlére tenni. További megkötés: alsó- és középfokú oktatási, gyermek- és ifjúságvédelmi, valamint vallás gyakorlására szolgáló intézmény bejáratától számított 200 méteres közúti (közterületi) távolságon belül szexuális árut értékesítő üzlet nem működhet.

A rendelet 27. §-ának f) pontja az értelmező rendelkezések körében nagyot alkotott, mikor leszögezte: pornó és szex tartalmú áru minden olyan mű, amelynek fő célja – a mű egészéből megállapíthatóan – a szexuális ingerkeltés, szexuális cselekmények és a nemi aktus nyílt ábrázolása.

3.2. A szex adójoga

Volt a szexjognak egy másik vonulata is, s érdekes módon – és szerény véleményem szerint – inkább ez vezet el oda, miért nem volt sürgős – mondjuk német mintára – az erotika, a szex, a „kemény" és a „puha" pornó műfaji szétválasztása.

A Nemzeti Kulturális Alapról szóló 1993. évi XXIII. tv. és a végrehajtása tárgyában kiadott 8/1994. (IV. 26.) MKM. rendelet teremtették meg egyes, a törvény mellékletében megjelölt termékek speciális adóztatásának lehetőségét. Az erőszak, szex, pornó tartalmú művek esetében 20 %-os járulékot kell az importőrnek, hazai gyártónak, forgalmazónak fizetnie (ezt a törvény idei évre szóló módosítása 25 %-ra emelte). E „termékcsoportot" az ÁFA mellett további 25 %-os járulék sújtja, az össz adó- és járulék-teher tehát mindösszesen 37 %. Praktikusan ez azt jelenti, hogy közvetlen adó formájában minden 100, szexre, pornóra kiadott állampolgári forintból 37 közvetlenül a kincstárhoz vándorol. A kiadónál, forgalmazónál a bruttó ár lényegesen kevesebb része marad (a terjesztői, viszonteladói jutalék, a gyártási költségek levonása után maximum 15-17 %). Na, ez lesz majd az az adóalap, amely után még más adókat (társasági adó stb.) is fizetni fog...

Hogy éves szinten ez hány milliárd forint adóbevételt eredményez, nehéz felbecsülni. Sokat. Egyes termékek (pl. a videokazetta) ugyanis többször adóztathatók: az eladáskor, s az egyes kölcsönzések után is...

3.3. Mit vonhat maga után a malackodás?

Az egyes szabálysértésekről szóló 17/1968. (V. 14.) kormányrendelet 1991-es módosításai (62/1991. /IV. 26/. Korm. rendelet, majd az újabb, 95/1991 /VII. 23./ Korm. r.) a szexuális áruk forgalmazásával kapcsolatos előírások megszegését szabálysértésnek minősítették, így a pucér képek közzététele (s mint láttuk, egy egyszerű fénykép is ennek minősülhet) 30.000 forintig terjedő pénzbírsággal sújtható.

Mielőtt az eljárásjogi részletek maga alá temetnék a mondanivalóm (ki jogosult a bírság kiszabására, hogyan bizonyítja a szabálysértés megtörténtét, az elkövető kilétét stb.) hadd szögezzem le: még egyetlen Internetes bírságról sem tudok. A lehetőség azonban nyitott, s számolni kell vele.

Mindez „alapjáratban" minden szexfotóra, pornófotóra érvényes. A celeb oldalak anyagai azonban legtöbbször ennél súlyosabb jogkövetkezményekkel járhatnak: itt már nem a szabálysértési hatósággal, hanem a rendőrséggel, bírósággal találkozhatunk.

Büntetőjogunk a személyiségvédelem, az emberi méltóság védelmének körében oltalmat biztosít. A rágalmazás bűncselekménye (Btk. 179. §) (aki valakiről más előtt a becsület csorbítására alkalmas tényt állít vagy híresztel, vagy ilyen tényre közvetlenül utaló kifejezést használ, vétséget követ el, s „alapjáratban" egy évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő. A nagy nyilvánosság előtti elkövetés már két évig terjedő szabadságvesztéssel jutalmazható.

Ha figyelembe vesszük, hogy a joggyakorlat szerint az elkövetési magatartás történhet szóban, vagy írásba, vagy egyéb módon – pl. képes ábrázolás útján is –, valamint, hogy a tény, tényállítás valósága vagy valótlansága nem tényállási elem (azaz közömbös a büntethetőség szempontjából, hogy az elkövető az állított vagy híresztelt tény valósága vagy valótlansága tekintetében állást foglalt e), s ha mindezt értelmes magyar nyelvre is lefordítjuk, érdekes képet szemlélhetünk.

A CEL-EB oldalon megjelenik a fotó: Miss X és Miss Y, a népszerű női együttes tagjai búvárszivattyút játszanak a méltán népszerű televíziós személyiséggel, Mr Z-vel. Miss X és Miss Y – stílszerűen – köpni, nyelni nem tudnak a megdöbbenéstől: a fotók persze nem őket ábrázolják, miként Mr Z is ártatlan a dologban. A fejüket – ügyesen – a képhez „ragasztották". Sőt, a „hjumorreás" elkövető még jelzi is: fake-ről van szó, vicc ez, emberek!!!

Ha azonban Miss X, Miss Y és Mr Z nem ismeri a humort (vagy a Galláét jobban szereti), felhorgadhat, s azt mondja: a kép megjelentetése becsületüket csorbította. És ha sebtében feljelentik CEL-EB elvtárs rágalmazásért, méghozzá nagy nyilvánosság előtt elkövetett rágalmazásért, senki nem hibáztathatja ezért őket. A tényállítás ebben az esetben igen egyszerű: Miss X és Miss Y olyan erkölcstelen, buja fehérszemélyek, akik pornófotózásra vetemedtek (lsd. a képet!). Ami ugye nem igaz: hisz a kép hamisítvány. Csakhogy a személyiségi jogok attól még sérültek, az érintettek becsülete csorbult. Kérdéses, hogy a közismerten vaskezű magyar büntető bíróságok ítélkezési gyakorlata szerint ezért kijáró öt guggolás és hat fekvőtámasz, amit az elkövetőre kiszabnának majd, kompenzálja e a jogsérelmet.

Aligha. Ám a polgári jogi kártérítési lehetőségét (ami adott esetben milliós nagyságrendű lehet) épp ezért biztosítja a jog. Mint ahogy a kukkoló-oldalon meghurcolt hölgyek esetében is, akiknek személyiségi jogai nem vitatottan ugyancsak sérelmet szenvedtek.

S mint már sokszor leírtam, a kör itt nagyjából be is zárul. Ha – tegyük fel – elkövetőnk vagyontalan, s számítógépén, kalózszoftverein kívül semmije sincsen, nyilván a milliós kártérítést megítélheti ugyan a bíróság, behajtani azonban már nem sikerül. A jogsérelmet szenvedett fél tehát egyetlen logikus lépésként kénytelen lesz a pénzügyileg lényegesen jobban álló szolgáltatót berángatni a perbe, s mint arra korábban ugyancsak utaltam, eséllyel követelhet tőle (is) kártérítést.

A sajtó-hecckampánynak hála a közvélemény kezd úgy tekinteni az Internetre, mint a paráznaság és a durva jogsértések birodalmára. A közhatalom egy idő után akkor is rákényszerül, hogy lépjen, ha ez csak erkölcsi érdeke:

s mint fentebb láttuk, ez esetben erős anyagi (adó) érdek is fűződik ahhoz, hogy kiiktassa a konkurenciát. Mindez óhatatlanul visszaüt az Internet szabadságára, s olyan folyamatot indíthat el, mely nem tudni hová vezet.

4. S AHOL MÁR LÉPETT AZ ÁLLAM: A MAGÁNTITOK FOKOZOTT VÉDELME

A büntető jogszabályok módosításáról szóló 1998. LXXXVII. törvény (kihirdetve a Magyar Közlöny 1998/116. számában) ugyan csak 1999. március 1. napján lép hatályba, mégis indokolt már most részletesebben foglalkozni titokvédelem körében belépő, az Internetet is érintő változásokkal. Bár természetesen továbbra sem találunk „Internetes tényállásokat" (azaz kimondottan a hálózatok hálózatán vagy annak terhére elkövetett büntetendő cselekmény meghatározásokat), ez nem jelent szabályozatlanságot. Ha „a távközlési berendezés útján továbbított küldemény" kifejezés helyett E-mailt mondunk, ha „a technikai eszközökkel rögzít" helyett a ment, letölt szót használjuk, ez nyomban világossá válik.

Az utolsó, átfogó Btk-módosítás (az 1997. évi LXXIII. tv.) is „megérintette" az Internet világát: (pl. a különleges személyes adatokkal visszaélés vétségi alakzatának — amelyet bárki elkövethet — a szabadságvesztés, pénzbüntetés mellett közérdekű munkával való büntethetőségének lehetővé tétele /Btk. 177/B. § (2), vagy a tiltott pornográf felvételek készítésének széles körű szankcionálása (mely szerint kiskorú személyről készített pornográf felvétel forgalomba hozataláért — éppúgy, mint a készítéséért vagy az ilyen felvételekkel való kereskedésért) 2 évtől 8 évig terjedő szabadságvesztés büntetés szabható ki /Btk. 195/A. §/).

Most azonban a jogalkotó olyan területen nyúlt a törvényhez, amely a netes világot, s ezen belül is elektronikus levelezésünk biztonságát, a magántitok megőrzéséhez fűződő jogunkat közvetlenül is érinti. A Btk. II címe (*Szabadság és emberi méltóság elleni bűncselekmények*) körében a titokvédelemmel kapcsolatosan részben egy módosítás, részben egy új bűncselekményi tényállás megjelenése jelzi: az információs társadalomban a magántitok továbbra is igen lényeges, alkotmányos jogunk, melynek megsértése — adott körben — büntetőjogi szankciókat vonhat maga után.

4.1. Levéltitok megsértése

Levéltitok megsértése

Btk. 178. §:

(1) Aki másnak közlést tartalmazó zárt küldeményét, tartalmának megismerése végett felbontja, megszerzi, vagy ilyen célból illetéktelen személynek átadja, úgyszintén aki távközlési berendezés útján továbbított közleményt kifürkész, *ha súlyosabb bűncselekmény nem valósul meg,* vétséget követ el és pénzbüntetéssel büntetendő.

(2) A büntetés egy évig terjedő szabadságvesztés, közérdekű munka vagy pénzbüntetés, ha az (1) bekezdésben meghatározott bűncselekményt foglalkozás vagy közmegbízatás felhasználásával követik el.

(3) A büntetés

a) két évig terjedő szabadságvesztés, ha az (1) bekezdésben meghatározott bűncselekmény;

b) bűntett miatt három évig terjedő szabadságvesztés, ha a (2) bekezdésben meghatározott bűncselekmény jelentős érdeksérelmet okoz.

Ami új: a dőlt betűvel kiemelt módosítás az (1) bekezdésben. Ezzel a törvényhozó lehetőséget teremt arra, hogy ha a levéltitok megsértése valamilyen súlyosabb bűncselekményt (a most beiktatott 178/A § szerinti *magántitok jogosulatlan megismerése*) valósít meg, azt ne a vétségként, hanem bűntettként lehessen elbírálni.

A levéltitok megsértése csak szándékosan követhető el: ez azt jelenti, hogy az „elkövetőnek" arra kell törekednie, hogy a levél tartalmát megtudja, vagy azt mással tudassa.

A „hagyományos" levéltitok és az „elektronikus" levéltitok elkülönítésekor a kulcsszó a *kifürkész*.

Kifürkészésnek minősül minden olyan magatartás, amelyet a közlemény tartalmának jogellenes megszerzése végett hajtanak létre. A „hagyományos" távközlésben ilyen a telefonok lehallgatása, a lehallgatott szövegek rögzítése stb. Az elkülönítés tehát igen egyszerű: ha jogosult vagyok a közlemény tartalmának megismerésére (címzett, listatag), vagy ha a közlemény „mindenkihez szól" (körlevél, felhívás), magatartásom jogszerű, ha illetéktelen vagyok, ha a jogellenesen szerzem meg a küldeményt, megsértettem a levéltitkot.

Mint a bírói gyakorlat is rámutat: (BH1982. 276.) a levéltitok megsértése nem csak szándékos, de célzatos bűncselekmény is, ezért csak akkor valósul meg, ha az elkövető a más részére szóló zárt küldeményt azért bontja fel, hogy annak tartalmát megismerhesse.

Nem bűncselekmény a másnak szóló E-mail véletlenszerű felbontása, tartalmának megismerése, vagy a nyilvános levelezőlistákon érkező bármely — nem konkrétan nevünkre szóló — küldemény elolvasása nem tartozik a levéltitok megsértésének kategóriájába.

Figyelemre méltó a (2) bekezdés, mely a foglalkozás körében való elkövetést súlyosabban szankcionálja: az, aki az Internetes hálózatot működteti, felügyeli s e foglalkozása felhasználásával fürkészi ki más elektronikus küldeményét egy évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel sújtható.

4.2. Magántitok jogosulatlan megismerése

A módosított Btk-ban új alcím, s egy új bűncselekményfogalom, tényállás jelent meg.

Magántitok jogosulatlan megismerése

178/A. §:

(1) Aki magántitok jogosulatlan megismerése céljából

a) másnak a lakását, egyéb helyiségét vagy az ezekhez tartozó bekerített helyet titokban átkutatja,

b) másnak a lakásában, egyéb helyiségében vagy az ezekhez tartozó bekerített helyen történteket technikai eszköz alkalmazásával megfigyeli, illetőleg rögzíti,

c) másnak közlést tartalmazó zárt küldeményét felbontja vagy megszerzi, és annak tartalmát technikai eszközzel rögzíti,

d) távközlési berendezés útján másnak továbbított közleményt kifürkész, és az észlelteket technikai eszközzel rögzít,

bűntettet követ el, és öt évig terjedő szabadságvesztéssel büntetendő.

(2) Az (1) bekezdés szerint büntetendő az, aki az (1) bekezdésben meghatározott módon megismert magántitkot továbbít vagy felhasznál.

(3) A büntetés két évtől nyolc évig terjedő szabadságvesztés, ha a bűncselekményt
a) hivatalos eljárás színlelésével,
b) üzletszerűen,
c) bűnszövetségben,
d) jelentős érdeksérelmet okozva
követik el.

A magántitok elektronikus úton történő jogosulatlan megszerzése többféleképpen megvalósulhat: például zárt küldeményben továbbított, magántitkot tartalmazó floppy, CD stb.) tartalmának megismerésével. A törvény azonban a megismeréshez még egy feltételt fűz (s lényegében ezzel határolódik el a cselekmény a levéltitok-sértéstől): az (1) bekezdés b), c) és d) pontja a technikai eszközzel „kifigyelt" magántitok valamilyen ugyancsak technikai eszközzel történő rögzítését.

Az elektronikus levelezésre, a távközlési úton történő elektronikus adattovábbításra vonatkozó (1) d./ pont értelmében az Internet esetében *e feltételt automatikusan teljesül*, hisz a „kifürkészett" magántitok a letöltéssel a számítógép segítségével (floppyra, vagy merevlemezre) kétségtelenül technikai eszközzel *rögzítődik*.

A bűncselekmény (szaknyelven szólva) *jogi tárgya*: a sértettnek magántitka megőrzéséhez fűződő személyes joga.

Mi a „magántitok"? A büntetőjogi szakirodalomban elterjedt meghatározás szerint: „magántitok minden olyan, csak kevesek, beavatottak előtt ismert tény, amelynek megőrzésére a jogosultnak méltányolható érdeke fűződik. Ez lehet személyi, családi vagy vagyoni jellegű körülményekre vonatkozó bizalmas adat stb. Valamely tény, adat stb. titok jellegét mindig az eset konkrét összefüggései alapján kell megítélni" (Györgyi-Wiener /szerk./: *A büntető törvénykönyv magyarázata*, Közgazdasági és Jogi Kiadó, Budapest, 1996, 370. oldal).

Lényeges, hogy a magántitok védelme nem csak a természetes személyre terjed ki, hanem — a *személyiségi jogvédelem alá vontak teljes körére* (jogi személyek, jogi személyiséggel nem rendelkező gazdasági társaságok, önkormányzatok, egyesületek, társadalmi szervezetek stb.).

El kell azonban határolni a Btk. 300. §-a szerinti üzleti titok megsértésétől: az önálló bűncselekmény. Az üzleti titok fogalmát egyébként a Btk. 300. § (2) bekezdésének ugyancsak decemberi módosítása így határozza meg: *üzleti titok a gazdasági tevékenységhez kapcsolódó minden olyan tény, információ, megoldás vagy adat, amelynek titokban maradásához a jogosultnak méltányolható érdeke fűződik, és amelynek titokban tartása érdekében a jogosult a szükséges intézkedéseket megtette.*

A magántitok és az üzleti titok fogalmilag több, lényeges pontban különbözik (az előbbi a magánszférát feltétel nélkül védi, az utóbbi gazdasági tevékenységgel kapcsolatos olyan titkokat részesít oltalomban, amelyek *titokban tartása érdekében a jogosult a szükséges lépéseket megtette*).

A magántitok jogosulatlan megismerése csak szándékosan követhető el. Célzatos bűncselekmény (arra irányul, hogy a magántitkot jogosulatlanul megismerjék). A bűncselekmény *gondatlanul nem követhető* el: s természetszerűleg a véletlen megismerés sem büntethető.

A közelmúlt példájánál maradva: ha Hacker Bandi neves pénzintézetünk megfelelő szuperbiztonságos védelmi rendszere mögé hatol be, és letölti az adatbankot, a Btk. 300. §-ba ütköző bűncselekményt követi el (üzleti titok megsértése). Ha a számlájára átkönyvel néhány millió forintot, az már számítógépes csalás (Btk. 300/C. §). Végezetül ha behatol a nemibeteg-gondozó egyébként külön biztonsági rendszerrel nem védett adatbázisába, s letölti a betegek adatait a bűncselekmény magántitok jogosulatlan megismerése (Btk. 178/A. §).

Más kérdés, hogy az információs társadalomban minden érdekeltnek célszerű megtennie a szükséges és lehetséges védelmi intézkedéseket. Egy adott körben a magánszféra újabb körben került — indokoltan — büntetőjogi oltalom alá: véleményem szerint a sokat vitatott decemberi Btk-módosításnak (melynek minden pontjával magam sem értek egyet) ez feltétlenül javára írható.

1. FÜGGELÉK: AZ EURÓPAI UNIÓ SAJTÓKÖZLEMÉNYE

1998. december 21-én az Európai Unió elfogadja az Internet biztonságosabb használatát támogató Akciótervet — a sajtóközlemény http://www.echo.lu/iap/ nem hivatalos fordítása: Akcióterv az Internet biztonságosabb használatának támogatására (1998. december 21.).

1998. december 21-én az Európai Unió Tanácsa második olvasatban elfogadta az *Internet biztonságosabb használatát a globális hálózatok jogellenes és ártalmas tartalmú anyagi elleni harc útján támogató Akciótervet*. Ez a végleges elfogadását jelenti egy Európa Bizottság általi előterjesztésnek, mely az 1999. január 1-től 2002. december 31-ig terjedő időszakra vonatkozóan — 25 milliós teljes költségvetéssel — kezdeményezések sorára vonatkozik. Ezek — melyeket az iparral, a tagállamokkal és felhasználókkal szoros együttműködésben dolgoztak ki — magukban foglalják forró vonalak hálózatát, támogatják az önszabályozást, a technikai jellegű intézkedések kifejlesztését és a tájékoztatási kezdeményezéseket.

Az Internet a gazdasági szektorok sorát forradalmasítja, s a szociális, oktatási és kulturális területek hatalommal bíró részévé válik. Soha nem volt még hozzáférhető a polgárok számára információk és szolgáltatások oly nagy száma, mint most. A kommunikáció új formái vannak kifejlődőben, s ezeket az érdeklődési csoportokban való részvétel mindenki számára hozzáférhetővé tette. Az akcióterv célja, hogy biztosítsa a különböző, az Internet nem kívánt tartalmainak kezelésével kapcsolatos európai uniós kezdeményezések végrehajtását. Fontos annak hangsúlyozása, hogy az Internet végtelen tartalmi sokrétűsége egyáltalán nem jelent problémát. Mindamellett azonban s arra tekintettel, hogy az Internet törvénytelen és ártalmas tartalom hozzáférhetővé tételére is felhasználható, e kérdéseket úgy kell kezelni, hogy Európa fogyasztói és ipara az információs társadalom által kínált minden előnnyel élni tudjanak. Közelebbről: a szülők és tanárok aggódnak olyan tartalmak elérhetősége miatt, melyek ártalmasak lehetnek gyermekeikre.

Az akcióterv különösen olyan intézkedések elősegítését célozza, melyek esetében a Közösség pénzügyi támogatására van szükség. A felhasználókkal, az Internet-iparral s a tagállamok kormányaival való együttműködés keretében dolgozták ki, s az Unión belüli politikai egyetértésre épül. A terv fő céljai, hogy:

- ösztönözze a szereplőket (ipar, kereskedelem, felhasználók) az önszabályozás megfelelő rendszereinek kidolgozására és alkalmazására,
- bemutatók tartásával és a technikai megoldások alkalmazásának serkentésével erősítse a fejlesztést,
- a szülők és tanárok éberségre intése és tájékoztatása,
- az együttműködés és a gyakorlati eredmények cseréjének elősegítése,
- európai szintű, az egyes szereplőket átfogó együttműködés támogatása
- az Európában és másutt tapasztalható törekvések közötti összeegyeztethetőség biztosítása.

Az akcióterv négy fő körben irányoz elő intézkedéseket:

1./ Biztonságos környezet megteremtése (az ipar önszabályozásán keresztül)

Elismerve azt a fontos munkát, amit az európai Internet-ipar e vonatkozásban végzett, a Bizottság a ma meglévő forró vonal kezdeményezésekre épít s bátorítani kívánja az önszabályozás és a Viselkedési Kódex (Codes of Conduct) létrehozására irányuló további kezdeményezéseket. Akciókat kell szervezni forró vonalak megteremtésére s a bűnüldöző hatóságokkal való kapcsolattartás elősegítésére. A Viselkedési Kódex elkészítését az 1998. szeptemberi, *A kiskorúak és az emberi méltóság védelmére vonatkozó Ajánlás* keretei között támogatni kell. A Viselkedési Kódexnek megfelelő módon egy látható minőségi címkerendszer megvalósítását kell elősegíteni.

2./ Szűrő és besoroló rendszerek kifejlesztése

Európai összefüggésben a szűrés és besorolás számos olyan módját kell megvizsgálni , melyek a felhasználók számára lehetővé teszik, hogy különféle eszközök széles választékához jussanak, s ezekkel az eszközökkel megvédhetik magukat és családjukat a nem kívánatos anyagok ellen. Az akcióvonal arra összpontosít, hogy az európai tartalom szolgáltatók vonatkozásában besoroló rendszereket érvényesítsen, a besorolást a tartalomalkotás folyamatának részévé tegye, e technikai megoldások s a harmadik személyeket védő osztályozási rendszerek előnyeit kihasználja. Nyomatékosítva: a hatékonyság érdekében kezdeményezni kell a minősítési rendszerekre vonatkozó nemzetközi megállapodás előmozdítását.

3./ Éberségi akciók bátorítása

Szoros összefüggésben más irányvonalakkal, ez készíti elő az egyes tagállamok által kivitelezendő akciókra. Ezeknek az akcióknak célja, hogy a nagyközönséghez való eljutást segítendő feltárják a sokszorosítás lehetőségeit, felleljék a legmegfelelőbb csatornákat, médiákat és tartalmat, előkészítik az alapvető anyagokat s azokat a nyelvi és kulturális sajátosságokhoz igazítsák. A teljes körű éberségi akciók bátorítása a tagállamokhoz címzett, követésre felhívó akciók formájában történik.

4./ Támogatási akciók

Miután egymagában egyetlen eszköz sem lehet hatékony ahhoz, hogy a felhasználók önvédelmi lehetőségét megteremtse, s a terv céljait valóra váltsa, végre kell hajtani egy kiegészítő akciótervet, mely értékeli a közösségi intézkedések hatékonyságát, a törvénybe foglalást és összehangolja azokat a hasonló nemzetközi törekvésekkel, más kezdeményezésekkel. Az akciók az 1998. szeptember 24-i, *A kiskorúak és az emberi méltóság az audio-vizuális és online információs szolgáltatások körében való, nemzeti szinten, az önkorlátozás révén megvalósuló védelmének Irányelveiről szóló Ajánlás*sal összhangban lesznek. Az akcióterv az Internet iparral, a felhasználókkal és a Tagállamokkal való konzultáció révén valósul meg. Hogy a nemzetközi törekvések egyirányúak maradjanak, a kapcsolattartás a nemzetközi testületekkel folytatódik. A más programok keretei között létrehozott, már létező hálózatok felhasználását a technikai, jogi és más megoldások terjesztése érdekében támogatni kell.

2. FÜGGELÉK: AZ E-KERESKEDELEM JOGI HÁTTERE MAGYARORSZÁGON

Egyre több azoknak az elektronikus kereskedelemmel foglalkozó külföldi cégeknek száma, melyek – a hazai vagy nemzetközi sikerek, egyre növekvő eladási számok hatására – Magyarországon is szeretnének hasonló üzletággal foglalkozni, vagy egyszerűen külföldi székhelyről történő eladásaikat Magyarországra is kiterjeszteni. Milyen jogi környezetre számíthatnak, milyen – jelenlegi – feltételrendszer mellett szállhatnak be az elektronikus piacokért való versengésre? A terjedelem nem teszi lehetővé, hogy a business to business vagy a business to administration jellegű kereskedést vizsgáljuk: csak a business to consumer üzleti kapcsolatok sajátosságait szeretnénk felvázolni.

1. Internet és jog Magyarországon

Magyarországon jelenleg 500 és 700 ezer között jelölik meg az „Internet-populációt", azaz azoknak számát, akik Internet-hozzáféréssel rendelkeznek. Pontos adat nem áll rendelkezésre: a kétszázezer „rejtett" Internetező elsősorban azokból tevődik össze, akik nem saját hozzáféréssel, hanem valamilyen intézmény (főként iskolák, vállalkozások, közintézmények) lehetőségeivel élve kapcsolódhatnak rá a webre, bár önálló előfizetőként nem jelennek meg. Mindez jelentős vásárlói bázist jelent, nem csak – a zömében fiatalokból, tizen-huszonévesekből álló – többséget érdemes megcélozni, de azokat a rétegeket is, melyek a „hagyományos" webes értékesítésű árucikkek (könyv, video, CD stb.) körén kívül is szívesen vásárolnának számítógépük segítségével.

Az Internet jogának magyarországi rendezetlensége azonban sokakat visszatart az ilyen jellegű kereskedéstől, befektetésektől. Tény, hogy a magyar jogban jelenleg nincsenek olyan különös törvények vagy más jogszabályok, melyek az Internet szereplőinek (user, buyer, service provider, mediator, content provider, seller) helyzetét, az elektronikus úton történő szerződéskötést egyértelműen rendeznék, így a szerződéses biztonság igen komoly követelményei hiányoznak. Különös szabályozás hiányában az elektronikus kereskedelemre az általános törvényi előírásokat kell vonatkoztatni.

2. Ki foglalkozhat elektronikus kereskedelemmel?

Az elektronikus kereskedelem a magyar jogban nem különbözik más kereskedelmi tevékenységtől. Kétféleképpen válhat egy cég a magyar elektronikus piacon szereplővé:

a) Magyarországi alapítású vállalkozást indít (gazdasági társaság), így az a magyar társasági jog szerint szerez jogalanyiságot.

b) Kereskedelmi képviseletet, fióktelepet létesít, illetve külföldi székhelyű vállalkozás más elismert módon folytathatja tevékenységét.

Az első körben a gazdasági társaságokról szóló 1997. évi CXLIV. tv (Társasági törvény), illetőleg a cégnyilvánosságról és a cégbírósági eljárásról szóló 1997. évi CXLV. tv. (Cégtörvény) elsősorban irányadó.

A külföldi székhelyű vállalkozások magyarországi fióktelepeiről és kereskedelmi képviseleteiről szóló 1997. évi CXXXII. tv. pl. a fióktelep jogi státuszának szabályozásával, valamint a kereskedelmi képviseletre vonatkozó szabályozás törvényi szintre emelésével lehetővé tette ezek széles körű működését. A pénzügyi szektorban külön törvények alapján ugyancsak vannak létező – külön törvények alapján szabályozott – képviseleti formák, de hasonlóan jogiasultak a magyar jogban a külföldi egyéni vállalkozások is.

Bármely formában is folytatja tevékenységét a vállalkozás, magyarországi bevételei után a magyar számviteli törvény szerint vezeti könyveit s a magyar adójog alapján adózik majd. Egyéb kérdésekben (munkajog, társadalombiztosítási jog) is a magyar jog szerint jár el. Belföldön kötött szerződéseire a magyar polgári jog szabályai vonatkoznak majd (hacsak valamely más jogot nem köt ki a szerződésben: a magyar bíróságok azonban külföldi törvények szerinti jogviták lefolytatására nincsenek felkészülve).

3. Reklámjog

Amennyiben a weben keresztül a cég közvetlenül nem értékesít, csak valamely valós üzletének promóciójára tart fent virtuális shopot, a gazdasági reklámtevékenységről szóló 1997. évi LVIII. tv. lesz elsősorban érvényes rá. E törvény a reklám minden formájára, így a weben keresztüli reklámozásra kiterjed. Miután a web a magyar jog szerint nem tartozik a médiatörvény – 1996. évi I. tv. – hatálya alá, így ennek rendelkezéseit nem lehet alkalmazni rá (ez annyiból fontos, mert a sugárzott reklám esetében a médiatörvény tartalmazza az elsődleges rendelkezéseket).

Egyes termékkörökre külön jogszabályok vonatkoznak. Így például a közbiztonságra különösen veszélyes eszközökre a 124/1993. (IX. 29.) Korm. rendelet, az élelmiszerforgalmazásról az 1/1997. (I. 17.) IKIM. Sz. rendelet, a kozmetikai készítmények reklámozásának speciális szabályairól a 7/1994. (IV. 20.) NM. sz. rendelet tartalmaz különös reklámjogi szabályokat.

A reklámjog előírásai kötelező érvényűek, megsértésük esetén jelentős szankciókkal (pénzbüntetés) kell számolni.

Az alapkérdés, hogy az Internet a reklámtörvény szempontjából sajtóterméknek minősül-e. (A magyar polgári törvénykönyv szerint jelenleg nem). A tv. 2. § p./ pontja szerint – mely pl. a videolemezt kifejezetten említi – bármely tájékoztatást vagy műsort tartalmazó, nyilvános közlésre szánt technikai eszköz sajtóterméknek minősül. Álláspontom szerint az Internet e feltételeknek eleget tesz, tehát a reklámtörvény hatálya alá tartozik.

4. Minek minösül az elektronikus kereskedelem?

Külön jogi szabályozás hiányában a kereskedés jellege szerint kell besorolni, s ez a magyar jogban is jól ismert csomagküldő kereskedelem. Az ilyen jellegű tevékenységgel szemben azonban törvényeink számos többlet követelményt állítanak. Ezek részben reklámjogi, részben kereskedelmi jogi jellegűek.

A gazdasági reklámtevékenységről szóló 1997. évi LVIII. törvény 3. § (3) bekezdése például előírja: A fogyasztó részére csomagküldés útján belföldön értékesítendő árura vonatkozó reklámnak azonosítható módon tartalmaznia kell a reklámozó megnevezését, a székhelyének vagy az állandó belföldi telephelyének (üzlethelyiségének) megjelölését, valamint a külön jogszabályban meghatározott nyilvántartásba vételi számát. Az üzletek működéséről és a belkereskedelmi tevékenység folytatásának feltételeiről szóló 4/1997. (I. 22.) Korm. rendelet 7, 19. §-a az általános feltételek mellett – működési engedély – külön feltételeket is előír, míg az egyes kereskedelmi tevékenységek gyakorlásáról 15/1989. (IX. 7.) KeM rendelet 2. § (1) nyilvántartásba vételi kötelezettséget ír elő: bármely áruval csomagküldő kereskedést akkor folytathat, ha a nyilvántartásba vételére jogosult szerv a kereskedőt és üzletét vagy raktárát, tárolóját nyilvántartásba vette.

Tehát a weben keresztül, közvetlenül a fogyasztó felé történő értékesítés a csomagküldő kereskedelem szabályai szerint kerül megítélésre.

5. Felelősség, szerződéskötés, fogyasztóvédelem

A magyar jogban nincs külön szabály a szolgáltatói és tartalomszolgáltató felelősség kérdéseinek rendezésére. Hibás teljesítés, károkozás esetén tehát az általános polgári jogi szabályok szerint kell eljárni. Az elektronikus úton kötött szerződés lehetséges (ráutaló magatartással kötött szerződés), ám az elektronikus „okiratok" eljárásjogi szempontból bizonyítéknak nem tekinthetők. A szerződés tartalmát a felek szabadon állapítják meg, de a magyar jog széles körben védi a vevőket a kedvezőtlen feltételekkel kötött blanketta-szerződésektől, a gazdasági erőfölénnyel való visszaéléstől.

A fogyasztóvédelemről szóló 1997. évi CLV. tv. már az európai uniós normák szerint rendezte a terület jogi kérdéseit. A legújabb jogfejlődés jelentős lépéseként a távollévők közötti szerződésekről szóló 17/1999. (II. 5.) Korm. rendelet az Európai Parlamentnek és a Tanácsnak a távolban kötött szerződések tekintetében a fogyasztók védelméről szóló 97/7/EK irányelvével összhangban kialakult szabályozást tartalmazza.

A szerződés tartalmi összeállításakor tehát úgy az általános polgári jogi előírásokra, mint a fogyasztóvédelmi jog speciális előírásaira tekintettel kell lenni.

TŐZSDEI RENDSZER ELOSZTOTT, OBJEKTUMORIENTÁLT MEGVALÓSÍTÁSA

DÁN GYÖRGY, GAJDOS SÁNDOR, LUKÁCS ZOLTÁN, NAGY PÉTER

BME TÁVKÖZLÉSI ÉS TELEMATIKAI TANSZÉK
111 BUDAPEST, PÁZMÁNY SÉTÁNY 1/D

Az utóbbi években a számítógépek egyre nagyobb szerephez jutnak a banki és pénzügyi szférában egyaránt. A folyamat a területi kirendeltségektől kezdve a brókercégekig mindenhol jól nyomonkövethető.

A tőzsdei rendszerek fejlesztésekor figyelembe kell venni néhány – egyéb területen fel nem merülő – követelményt is. A nagy adatmennyiség és az egyszerű műveletek igen gyors végrehajtása mellett támogatni kell az elosztott működést is. A tőzsdei szabályok változása miatt az alkalmazásoknak rugalmasan változtathatónak kell lenniük, méghozzá a kliens programok egyenkénti újratelepítése nélkül. Az általános tőzsdei igények mellett vannak kimondottan magyar vonatkozásúak is.

A bemutatott megoldás minden szintjén objektum-orientált technológiákra épül. Az alkalmazásokat az Object Management Group által kidolgozott CORBA lehetőségeire építettük fel. Segítségével – többek között – lehetővé válik az elosztott rendszer hálózatfüggetlen módon történő megtervezése. A kliens szoftver dinamikus módosításáról a rendszer automatikusan gondoskodik.

A szerver oldalon az adatok tárolásáról egy vagy több, a szerver program mögött a kliens számára láthatatlan módon elhelyezett objektum-orientált adatbázis gondoskodik. Az átlátszóságnak köszönhetően a rendszer komolyabb beavatkozás nélkül skálázható, így rugalmasan tud alkalmazkodni a felhasználók igényeihez.

BEVEZETÉS

A szoftverfejlesztés folyamata jelentősen átalakult az elmúlt évtizedekben. A „guruk" tevékenységét a szoftverek ipari előállítása váltotta fel. Ehhez szigorú technológiai előírásokra és hatékony fejlesztő eszközökre van szükség. A szoftverfejlesztés során a technológiai előírásokat a fejlesztési módszertanok, az eszközöket pedig a CASE rendszerek és a programozási nyelvek jelentik. Napjainkban számos módszertan van versenyben egymással, ezek közül az alkalmazási területek növekvő részénél az objektum-orientált megközelítés került ki győztesen. Ennek oka talán az, hogy a többi módszerrel szemben az objektum-orientált elvek nem a számítástechnika elvont fogalmait kívánják ráerőltetni a világra, hanem a világ természetes, számítástechnika mentes működését helyezik előtérbe a feladatok megoldása során [2]. A szoftverfejlesztés objektum-orientált megközelítése a valós világból vett modelleken alapul, ezeket a modelleket használjuk, hogy egy – az implementációs nyelvtől független – tervet készítsünk. Ezen modellek jól használhatók a probléma megértésére, az alkalmazási terület szakértőivel való kommunikációra, programok és adatbázisok tervezésére. A szoftverfejlesztés objektum orientált megközelítésére sok módszertan létezik, ezek közül ma talán a legnépszerűbb, legelterjedtebb – ha nem is a legújabb – az OMT (Object Modeling Technique) [1], ezen okból választottuk mi is. A későbbiekben különböző diagramokon használt jelölések ebből a műből ismerhetők meg részletesen.

A számítástechnika hőskorában, de egészen a nyolcvanas évekig a számítógépek jellemzően egymástól elszigetelve léteztek, az információcsere meghatározó módja a lyukkártya, később a mágneslemez volt. Ez a szoftverek kialakításában is megmutatkozott: az alkalmazás számára rendelkezésre álló erőforrások egy gép erőforrásaira voltak korlátozva, valamint nem állt módjában más gépek szolgáltatásait igénybe venni. A korlátozott lehetőségekkel rendelkező architektúrának volt egy nagy előnye: az alkalmazások által kommunikációval eltöltött idő aránylag csekély és mindenképp előre jól behatárolható volt. A PC-s alkalmazások között még mindig az egy gépen futó alkalmazások dominálnak. A hálózatok elterjedése ugyanakkor megnyitotta az utat a gépek közötti gyors kommunikáció és nagymennyiségű adatátvitel számára. Az alkalmazások közötti kommunikáció során a felek egymást a Szolgáltatási réteg (Service Layer) által kezelt portokon azonosítják. A UNIX-os világban bevezetett RPC (Remote Procedure Call, Távoli Eljáráshívás) már egy kísérlet volt az elosztott feldolgozást megvalósító alkalmazások fejlesztésének megkönnyítésére, a hálózatkezelés magasabb szintre való emelésére. A módszer azonban nem eléggé rugalmas, nem támogatja a manapság oly kedvelt OO alkalmazások fejlesztését, valamint nem ad lehetőséget alkalmazások egymástól függetlenül történő fejlesztésére. Az elosztott alkalmazások fejlesztését egységesítendő és megkönnyítendő a kilencvenes évek elején a világ vezető szoftverfejlesztő cégei által alakított Object Management Group (OMG) kifejlesztette a CORBA (Common Object Request Broker Architecture) szabványt [11].

Ugyanakkor az utóbbi években egyre jobban elterjedtek az **objektum-orientált adatbáziskezelő rendszerek** (OODBMS-ek) is. Ez a tendencia többek között annak köszönhető, hogy növekszik az igény az olyan jó minőségű szoftverekre, amelyek megbízhatóak, könnyen bővíthetők és jól tesztelhetők. Az objektumorientált technológia megoldást nyújt mindezekre és az egyik legfőbb erénye: a kód újrahasznosíthatósága miatt növeli a programozói termelékenységet. Az OODBMS-ek természetes módon illeszkednek az objektum-orientált technológiai láncba. Elsősorban a következő területeken terjednek rohamosan: CAD, CASE, pénzvilág, távközlés, Internet, multimédia, térképészet [10].

1. A PROBLÉMA INFORMÁLIS LEÍRÁSA

A cél egy általános értékpapír-kezelő rendszer létrehozása volt. Egy ilyen tőzsdei alkalmazás fejlesztésekor számos különleges körülményt, illetve követelményt kell figyelembe venni:

- A magyar tőzsdei rendszer különbözik a világ többi rendszerétől. Magyarországon a tőzsdei tevékenységben részt vesz a Budapesti Értéktőzsde (BÉT), a Központi Elszámolóház és Értéktár Rt. (KELER) és az üzletkötők. A kereskedés zavartalan lebonyolításához a felek együttműködésére van szükség. A speciális szabályok miatt a külföldi, általános értékpapír-rendszerek nem alkalmasak (ill. nem teljesen alkalmasak) a magyar értékpapír-forgalmazó cégek szoftverellátására. Ez ösztönzőleg hat ilyen szoftverek kifejlesztésére.
- Az értékpapír-forgalmazó cégeknek jelentési és adatszolgáltatási kötelezettségük van a KELER, valamint az Állami Pénz- és Tőkepiaci Felügyelet (ÁPTF) felé.
- Mivel a magyar jogszabályok viszonylag gyakran változnak, ezért a szoftvernek könnyen változtathatónak kell lennie. Ráadásul a verziócseréket úgy kell megoldani, hogy azok ne okozzanak fennakadást a cég működésében.
- A befektetési konstrukciók választéka is egyre bővül, tehát a rendszernek fel kell készülnie ezeknek a kezelésére is, illetve ha ez nem megoldható, akkor alkalmassá kell tenni rá, ami (megint csak) nagyfokú rugalmasságot igényel.
- Az értékpapír-rendszerekre jellemző, hogy nagyon sok adatot kezelnek, de egyszerű műveleteket végeznek rajtuk, azaz klasszikus tranzakció kezelő rendszereknek tekinthetők.
- Egy új munkaállomás rendszerbe kapcsolása nem okozhat gondot, az elosztott működés alapkövetelmény. Az elosztott működést adatbázis- és applikáció-szerverrel lehet (szokás) támogatni.

A tervezett rendszer feladata, hogy a fenti tényezőket figyelembe véve bármilyen értékpapír-forgalmazással kapcsolatos tevékenység során hatékony informatikai segítséget nyújtson a forgalmazók részére.

Funkcionális követelmények:

- lehetőség tetszőleges tranzakció kezelésére (új tranzakciótípus definiálása, módosítása, törlése);
- az ügyfelek adatainak kezelése;
- különböző számlatípusok definiálása és ezek kezelése;
- értékpapírok nyilvántartása;
- felhasználókhoz rendelhető jogosultsági szintek kezelése;
- adminisztrációs tevékenységek biztosítása;
- külső jelentési és adatszolgáltatási kötelezettségek ellátása, riportok, kivonatok készítése.

Technológiai követelmények:

- elosztott működés;
- visszakereshetőség, naplózás;
- adatbiztonság.

A rendszer tervezése során a számos szóba jöhető tranzakciótípus közül kiválasztottunk egy nagy változatosságot mutató típust: az értékpapír jegyzést. A cél elsőként ennek a megvalósítása volt úgy, hogy ezzel biztosítsuk más, a jegyzés végrehajtási sémájához illeszkedő tranzakcióknak a rendszerhez történő hozzáadását oly módon, hogy a kliens oldali szoftvert ne kelljen módosítani és így újratelepíteni.

2. ELOSZTOTT OBJEKTUM-ORIENTÁLT TECHNOLÓGIA FŐBB JELLEMZŐI

2.1. Modellezés OMT-vel

A rendszer megtervezéséhez az OMT-t (Object Modeling Technique) használtuk.. Az OMT az egész szoftver fejlesztési életciklust átfogja kezdve a feladat analízisétől egészen a kész rendszer implementálásáig. A módszertan három fő fázisra osztható: analízis, tervezés, implementáció. a következőkben ezek rövid összefoglalása következik [1], [2].

2.1.1. Analízis

Az analízis célja a feladat megértése és az elkészítendő rendszer alapjainak lerakása. Az analízis négy modellen alapul: use case, objektum modell, dinamikus modell és a funkcionális modell. Ezek a modellek a rendszer különböző szempontok szerinti nézeteit adják.

A Use Case modell jelöli ki a rendszer határait, valamint definiálja a rendszer viselkedését. A modellben szerepelnek a rendszer használói: a szereplők (actor), és a használati esetek (use case-ek). A szereplők lehetnek emberek, gépek vagy akár más rendszerek is. A használati esetek azoknak a tevékenységeknek a szöveges leírásai, amelyeket a használók végezhetnek a rendszeren.

Az objektum modell célja az alkalmazási területnek a feladat szempontjából lényeges dolgainak (objektumok) és a közöttük lévő statikus viszonyok (kapcsolatok) meghatározása. A modell leírja a rendszerbeli objektumok struktúráit, attribútumait, metódusait, valamint az objektumok közötti viszonyokat (asszociáció, öröklés, komponens vagy tartalmazás reláció).

A dinamikus modell célja az objektumok időbeni viselkedésének, együttműködésüknek a leírása. A modell részei az állapot diagram (az osztály egy példányának a külső események hatására történő állapotváltozásai és a válaszul adott reakciók), kommunikációs diagram (az üzenet kapcsolatban álló objektumok ábrázolása), esetleg ún. forgatókönyvek (a rendszer külső interfészén történő események, vagy bizonyos objektumokkal kapcsolatos tipikusan előforduló események leírása).

A funkcionális modell a rendszer által végrehajtandó működéseket tartalmazza, azaz leírja, hogy a rendszer mit csinál függetlenül attól, hogy mikor és hogyan. A leírásra DFD (Data Flow Diagram) szolgál. A DFD-n terminátorok (adatok forrásai, és nyelői), processzek és adattárak szerepelnek.

2.1.2. Tervezés

A tervezési fázis célja az analízis eredményeinek leképzése hardver és szoftver elemekre.

A rendszertervezés célja a programnak az implementációs szempontokkal összhangban lévő alrendszerekre bontása, a rendelkezésre álló erőforrások megosztása, az adatszerkezetek implementációs stratégiájának kiválasztása (az objektumokat tranziensen vagy perzisztensen tároljuk), valamint ide tartozik a külső interfész típusának kiválasztása (programvezérelt vagy eseményvezérelt).

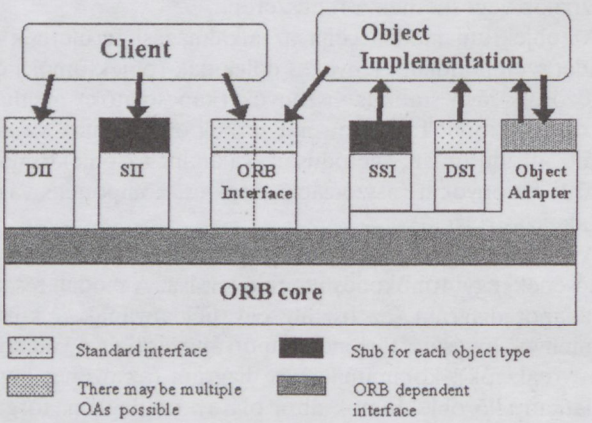
Az objektum tervezés során az analízis fázisban keletkezett három modellt finomítjuk tovább. Ebben a részben összekombináljuk az objektum-, a dinamikus- és a funkcionális modelleket, döntünk az asszociációk megvalósításáról, kiválasztjuk a metódusokban használandó algoritmusokat, esetleg optimalizálást végzünk valamilyen szempont szerint.

2.1.3. Implementáció

Az implementáció során a különféle modellekből előállítjuk a kommentezett forráskódot. A programozás viszonylag kisebb, ráadásul mechanikusabb része a fejlesztési ciklusnak, mivel az összes fontos döntés meghozatala a tervezési szakaszban történt. A célnyelv hatást gyakorolhat a tervezési döntésekre, de a tervezés nem függ a választott programozási nyelv részleteitől. A fejlesztési szakasz fontos állomása az elkészült alkalmazás tesztelése a követelmények teljesítésének ellenőrzése érdekében.

2.2. CORBA

A CORBA alapját az Object Request Broker (ORB) képezi, amely az egyes gépeken futó CORBA alapú alkalmazások közötti kommunikáció transzparens lebonyolításáért felelős. Ez alatt az értendő, hogy a kliens program úgy használhatja a távoli szerver által rendelkezésére bocsátott objektumokat, mintha azok a saját gépén, sőt a saját címtartományában volnának.



1. ábra. Az Object Request Broker-ek felépítése

Mivel az ORB-ok által a külvilág felé mutatott felület szabványos, ezért adott a lehetőség akár különböző programnyelveken megírt programok egymással történő összekapcsolására is, s így heterogén rendszerek létrehozására.

Az ORB implementációs kérdéseiről a CORBA specifikáció nem rendelkezik, csupán azt az alapvető követelményt fogalmazza meg, hogy a különböző gyártók ORB-jainak meg kell érteniük egymást (interoperabilitás). Léteznek azonban ajánlások az átvitel mikéntjére, így például minden, magát CORBA kompatibilisnak mondhatni akaró ORB daemon kell, hogy ismerje az IIOP-t (Internet Inter-ORB Protocol), ami egy TCP/IP feletti megvalósítása az általánosan összeköttetés-alapú kapcsolatokra tervezett GIOP-nek (General Inter-ORB Protocol). Az adatok átvitelekor szükséges konverziót a fogadó oldali daemon végzi el (receiver makes right), így elkerülhető az azonos platformok közötti felesleges konverzió.

2.2.1. Az IDL leíró nyelv

Az alkalmazásfejlesztő szempontjából a legfontosabb az IDL (Interface Definition Language) nyelven megadott szerver interfész, amelynek alapján a fejlesztő megírhatja a saját programját, amely azután képes lesz a szerverrel való kommunikációra anélkül, hogy egy sor hálózatot kezelő kódot írt volna. Magának a nyelvnek a szintaktikája C++ jellegű, támogatja az objektumokat és az öröklődést. A szabvány néhány nyelvre megadja a leképezés standard módját, többek között a C, C++, Cobol, Ada, Smalltalk nyelvekre. Így az egyik implementációhoz írt forráskód másik CORBA implementációhoz készítettel is összeszerkeszthető lesz. Az IDL-ben megírt interfész leírás a kliens számára egyfajta ígéret, azaz számíthat rá, hogy a szerver az összes megadott szolgáltatást nyújtja. A szerver számára ugyanakkor kötelezvény, amelynek eleget kell tennie. Másfelől viszont az IDL leírás nem hordoz információt a szerver oldali implementációs döntésekről, így a szerver szállítójának módjában áll azon változtatni anélkül, hogy a kliensnek arról tudomása volna. Ilyen tekintetben tehát az IDL file – ami a kliens és a szerver között az összes szükséges információt közvetíti – hasonlít egy jól megírt C headerhez. Az IDL-ben megírt, és a kliens fordításakor már rendelkezésre álló interfészt felhasználva tud a kliens a szerver felé – statikus – hívásokat felépíteni.

2.2.2. A szerver oldal felépítése

A szerver oldal lelke az ORB mellett az Object Adapter (OA). Míg előbbi a kliensekkel történő kapcsolattartásért felelős, addig utóbbinak a szerver oldalon található objektumok menedzselése a feladata. A CORBA szabvány definiál egy OA-t, amelyet minden implementációnak tartalmaznia kell: ez a Basic Object Adapter (BOA). Ezen kívül készíthetők egyéb, felhasználási-terület specifikus OA-k, például perzisztens tárolást megvalósító OA, amely objektumorientált adatbázisban tárolja az objektumokat (pl. Orbix ObjectStore Adapter). Míg az ORB felépítése nem függ a kiszolgált szerver típusától és felülete szabványos, addig a különböző OA-k felépítése és interface-e eltérhet egymástól, felhasználás-specifikus igényeknek megfelelően.

A BOA generálja és értelmezi az objektumokat egyértelműen azonosító objektum referenciákat, valamint formátumokat ad meg. Bejövő hívások esetén ellenőrzi, hogy a hívó fél jogosult-e az adott szolgáltatás igénybevételére. Emellett a szerver implementációjának és objektumainak aktivizálásáért, valamint deaktivizálásáért is felelős.

Az OA kezeli a szerver oldalon található két információs forrást. Az egyik adatbázisban (csupán logikailag adatbázis, gyakorlatilag lehet könyvtárstruktúra is, vagy tetszőleges struktúra), amelynek neve Interface Repository, az adott helyen regisztrált szerverek interface-ei találhatók (amit az IDL file-ban adtunk meg). A másik adatbázis neve Implementation Repository, ebben történik az adott OA által kezelt szerverek nyilvántartása (szerverkezelési mód, hozzáférési jogosultságok).

Az adminisztráció mellett az OA felelős a beérkező függvényhívásoknak a szerver objektum felé való továbbításáért, amit két interface-en keresztül bonyolíthat le.

Teheti egyrészt a fordítási időben meghatározott Static Skeleton Interface-en (SSI, Statikus váz) keresztül. Ez a

váz az IDL leírásból készül, és hátránya, hogy futási időben nem módosítható, funkciója a beérkező CORBA hívásoknak a szerverobjektumok tagfüggvényeire való leképezése. Így a szerverben található implementációs objektumok írójának sem kell törődnie azzal, hogy az objektumai által nyújtott szolgáltatásokat egy elosztott rendszerben, a hálózaton keresztül veszik igénybe. Így azonban csak olyan hívásokat van mód fogadni, amelyek már fordítási időben ismert objektumtípusokra vonatkoznak.

A fordítási időben nem ismert objektumok kezelésére szolgál a Dynamic Skeleton Interface (DSI, Dinamikus váz). Alapötlete, hogy az összes, egy bizonyos objektumnak szóló hívást egy és ugyanaz a függvény, a Dynamic Implementation Routine (DIR) fogadja.

2.2.3. A kliens oldal felépítése

Az 1. ábrán látható módon a kliens három módon tud a külvilággal kommunikálni. Egyrészt közvetlenül kapcsolatba léphet a gépén futó ORB-bal, ily módon hozzáférhet és módosíthat olyan CORBA specifikus adatokat, mint az időtúllépési korlát vagy a lassú hálózati kapcsolatok lebontása. Jellemzően azonban a kliensek közvetve veszik igénybe az ORB szolgáltatásait, mégpedig a Statikus Hívási Felület (Static Invocation Interface, SII) és a Dinamikus Hívási Felület (Dynamic Invocation Interface, DII) közvetítésével.

Az IDL leírásból a kliens oldal számára származtatott leírás a Statikus Hívási Felület, ami a kliens és szerver között kommunikáció legfőbb közvetítője. Ez tartalmazza azt a kódot, amely a kliens kéréseit a szerveren elhelyezkedő CORBA objektumok felé továbbítja. így a távoli objektumok metódusainak meghívása a programozó számára jobbára átlátszóan valósul meg: megadva az objektum referenciát és a végrehajtani kívánt műveletet, az objektum a megszokott módon meghívható. A kliens nem ismeri az igénybevett objektum implementációját, csupán az interface leírásban megadott tulajdonságoknak van ismeretében. A SII azonban korlátozza az elérhető objektumtípusokat azokra a típusokra, amelyek már fordítási időben definiáltak voltak, azaz szerepeltek az IDL leírásban.

Az alkalmazásoknak egy kis számú, ámde annál fontosabb csoportja számára azonban nem elfogadható az a megszorítás, hogy csak fordítási időben ismert objektumokat használhat. Ezek közé tartoznak például keresőprogramok, de ide sorolhatjuk az általunk kifejlesztett alkalmazást is. Szükség van tehát olyan objektum kezelésének lehetővé tételére, amelyek fordítási időben még teljességgel ismeretlenek voltak, és így az IDL leírásba nem kerülhettek be. E probléma áthidalására született a Dinamikus Hívási Felület (Dynamic Invocation Interface, DII), ami lehetővé teszi hívások futási időben történő felépítését az objektum referenciájának és a meghívni kívánt metódus, illetve a beállítani kívánt paraméter nevének megadásával. A hívás felépítéséhez szükséges információt az alkalmazás a szerver oldalon elhelyezkedő Interface Repository-ból kapja meg. Hátránya a DII-nek, hogy a hívások felépítéséhez szükséges információ megszerzése idő- és erőforrásigényes. Itt érdemel említést ugyanakkor, hogy a szerver oldalon elhelyezkedő objektum a beérkező függvényhívásokról nem tudja eldönteni, hogy azok a SII-n vagy a DII-n keresztül jöttek-e, így nem áll módjában különbséget tenni a különböző módon felépített hívások között [6].

2.2.4. A CORBA által nyújtott egyéb lehetőségek

Mivel a CORBA folyamatos fejlesztés tárgya, a fenti, szinte a kezdetektől létező tulajdonságokon kívül van a CORBA-nak néhány olyan lehetősége, amely a fejlesztés későbbi szakaszában jelent meg és még nem teljesen kialakult.

Ilyen az először az Iona cég Orbix nevű CORBA implementációjában megjelent, és azóta már több gyártó által támogatott opaque IDL típus. Bevezetésének főleg az alkalmazások sebességének növelése volt a célja. Az objektum referenciák ugyan kis helyet foglalnak a hálózaton keresztül történő továbbítás során, ám előfordulhat, hogy egy objektum mezőihez egymás után többször kell hozzáférni, és ez esetben egymás után sok hívás felépítésére van szükség, ami a CORBA kommunikációs overhead-je miatt időigényes.

A CORBA IDL keretein belül az érték szerinti paraméterátadás megvalósítására két lehetőség adódik. Egyfelől tárolhatjuk az objektumok állapotát struktúrákban, amiket érték szerint átadhatunk paraméterként. A módszernek két nagy hátránya van: elválik egymástól az interfészben megadott információ és az állapot információ, valamint a programozónak az IDL leírásban implementáció specifikus adatokat kell megadnia. Másfelől átvihetjük az objektum állapotinformációját octet szekvenciaként is. Ebben az esetben az átvitt adatok típusa nincs explicit módon megadva, így nem sérül az objektum adatainak privát volta, ugyanakkor azonban a típusinformáció hiányában a szükséges adatkonverzió sem végezhető el CORBA szinten, tehát az alkalmazás-programozónak kell gondoskodnia róla. A CORBA IDL kereteit felrúgva azonban lehetőség nyílik a probléma kényelmesebb megoldására is. A megoldást az opaque típus használata jelenti, az ilyen objektumok objektumok minden esetben érték szerint kerülnek átadásra, nem pedig referencia szerint. A módszer, és egyben az érték szerinti átadás nagy hátránya, hogy az objektum implementációjának a kliens oldalon is szerepelnie kell. Ezért az elérhető sebességnövekedés kárpótolhatja a programtervezőt. Egyes esetekben – mint majd látjuk, a mi esetünk is ide tartozik – a kliens oldalra nem célszerű objektum implementációkat beépíteni, mivel azok gyorsan változnak, illetve bővülnek.

2.3. Objektum-orientált adatbázis-kezelés

Az objektumorientált adatbázis-kezelő (ODBMS) szabványok kidolgozása az Object Data Management Group (ODMG) nevéhez fűződik, amely szervezetet az Object Management Group (OMG) hozott létre.Az ODMG objektum modellje gyakorlatilag az OMG modelljének a kiegészítése.

Két további ODMG szabvány az Object Definition Language (ODL), valamint az Object Query Language (OQL). Az ODL az OMG Interface Definition Language (IDL) kiterjesztése, amely adattípusok és interfészük definiálására való, ugyanakkor a megvalósítással nem foglalkozik, programnyelvtől független, így hordozható ODL kompatibilis OODBMS-ek között.

Az OQL-lel az SQL-hez hasonlóan lehet lekérdezéseket megfogalmazni. A SELECT szintakszisa kibővült, lehetőség van metódusok hívására, navigációs kifejezések használatára és az öröklődés is támogatott.

Az OODBMS-ek által leggyakrabban támogatott programnyelvek: C++, Smalltalk, Java [9].

Jelenleg egy adatbázis-kezelővel szemben támasztott elvárások magukba foglalják az összetett adatszerkezetek kezelését, bonyolult kapcsolatok kialakítását, osztott adatbázisok támogatását. Mindemellett az adatbázis-kezelőnek nagy teljesítményűnek és egyszerűen programozhatónak kell lennie. Ma már az OODBMS-ek is egyre jobban meg képesek felelni ezeknek a követelményeknek.

Objektumorientált fejlesztő környezetben nyilvánvaló előnyként jelentkezik, hogy elmarad számos adatkonverzió, ami relációs adatbáziskezelő használata esetén elkerülhetetlen lenne.

2.3.1. ObjectStore

Az ObjectStore az Object Design Inc. objektumorientált adatbázis-kezelője. Számos programnyelvet támogat: C++, Smalltalk, Java, ActiveX-en keresztül pedig Microsoft Visual Basic-et, Borland Delphi-t és a Sybase PowerBuilder-ét is.

A fejlesztés során az ObjectStore C++-t támogató változatát használtuk, amely lehetővé teszi C++ objektumok perzisztens tárolását. Az objektumok ugyanolyan formátumban kerülnek tárolásra, mint a tranziens objektumok és a perzisztens objektumokhoz való hozzáférés hagyományos C++ program-konstrukciókkal történik.

A C++ nyelven megírt alkalmazások rendkívül egyszeruen elláthatók ObjectStore adatbázis támogatással, ami abból adódik, hogy az ObjectStore a mutatókat transzparensen kezeli, támogatja az öröklődést, lehetőség van parametrizált (template) osztályok használatára, és külön kivétel-kezelési mechanizmussal rendelkezik. Lehetőség van a C++ kivételkezelőjének behívására is.

Lehetőség van arra, hogy a különböző architektúrájú kliensek tetszőleges fordítót használjanak annak ellenére, hogy a különböző fordítók eltérő formátumú objektumokat állítanak elő és a különböző architektúrájú gépek eltérő formátumokat használnak. Ahhoz, hogy az egyes objektumok heterogén környezetben legyenek használhatók, a forráskódot megfelelően át kell írni, amiben segítséget nyújt az ObjectStore séma generátora.

Az ObjectStore C++ osztálykönyvtárakat kínál fel, amelyek az alábbi eszközökkel támogatják az adatbázis kezelő rendszereket: kollekciók lekérdezésekre, indexelésre vonatkozóan és az inverz kapcsolatok támogatásához, meta-objektum protokoll, séma evolúció.

A kollekció lehet halmaz, multihalmaz, lista, tömb és szótár típusú, de lehet általános kollekció is, amely nagy rugalmassággal rendelkezik. A kollekciók támogatják a lekérdezéseket, azaz az objektumok asszociatív elérését. A kollekciókat indexelni is lehet, ami nagymértékben optimalizálja a lekérdezéseket.

Az ObjectStore kapcsolatkezelési szolgáltatásai támogatják az objektumok közötti kétirányú kapcsolatot. Ez automatikus módosítást tesz lehetővé az ellentétes oldalon, ha az egyik fél oldalán expliciten módosítás történt. Megvalósíthatók egy-egy, egy-több és több-több kapcsolatok is [9], [10].

3. TERVEZÉSI MEGFONTOLÁSOK

3.1. Az OODBMS rendszerbe integrálása

A tervezésnél az volt a cél, hogy a létrejövő rendszer hálózat-használat szempontjából legyen optimális. Ezért az adatbázis-kezelő csak a CORBA szerver applikációhoz kapcsolódik, a kliens nem is tud arról, hogy milyen adatbázis-kezelő van a rendszerben.

3.2. Adattervezés

A rendszer tervezése során a fentebb már ismertetett szempontokon kívül az alábbiakat kellett még figyelembe venni:

- gyors kommunikáció a kliensek és a központ között;
- könnyen kezelhető, grafikus felhasználói felület;
- későbbi bővítés lehetőségének fenntartása.

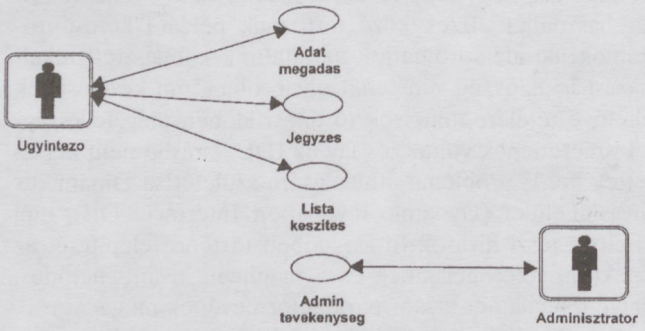
3.2.1. Analízis

3.2.1.1. Use Case

A rendszert első közelítésben kétféle szereplő használja: az ügyintéző, valamint az adminisztrátor. Az ügyintéző az a személy, aki az ügyfelekkel foglalkozik, felveszi az adatait, elvégzi a tranzakciót (a jegyzést), valamint különféle szempontok szerint listát készít (pl. egy titkárnő vagy egy bróker). Az adminisztrátor az a személy, aki a megfelelő jogosultságokkal rendelkezik ahhoz, hogy az egyes értékpapír fajták jellemző tulajdonságait, valamint a tranzakció fajták paramétereit beállíthassa (pl. egy bróker vagy a főnök, de nem egy titkárnő.).

A modellben felvett használati esetek egy konkrét tranzakcióhoz, a jegyzéshez kapcsolódnak (2. ábra):

- Adatmegadás: az ügyintéző felveszi az ügyfél jellemző adatait (név, lakcím stb.).
- Jegyzés: az ügyintéző elvégzi az ügyfél által kezdeményezett tranzakciót.
- Listakészítés: az ügyintéző különféle szempontok szerint listát készít.
- Adminisztrátori tevékenység: az adminisztrátor új értékpapírfajtát valamint a hozzá tartozó tranzakciókat vesz fel a rendszerbe.



2. ábra. Use Case

3.2.1.2. Objektum modell

A rendszerben az objektumokat hét nagyobb csoportba lehet besorolni: az ügyfélhez, a számlához, a tranzakcióhoz, az értékpapírhoz, a tranzakciót típusokhoz, a kliensol-

dalhoz, valamint a szerveroldalhoz tartozókba. Az osztály diagram a 3. ábrán látható.

Az ügyfélhez tartozó főbb és általánosítható attribútumokat az *Ugyfel* absztrakt osztály tartalmazza (pl. Törzsszám, Adószám, Név stb.). Az *Ugyfel*ből örökléssel származnak a valódi ügyfél típusok: belföldi magánszemély (*Belf_magan*), külföldi magánszemély (*Kulfodi_magan*), belföldi közület (*Belfoldi_kozulet*), külföldi közület (*Kulfoldi_kozulet*). Az öröklési hierarchia bevezetésével lehetőség van arra, hogy a későbbiekben egy új ügyfél típust könnyen be tudjunk vezetni. Az ügyfelek között esetleg fennálló meghatalmazotti viszonyt a meghatalmaz asszociáció írja le.

Az ügyfelek a birtokukban lévő értékpapírokat különböző típusú számlákon (pl. tőkeszámla, értékpapír-számla) tartják. Ezen számlafajták közös tulajdonságait tartalmazza a *Szamla* absztrakt osztály, ebből örökléssel származik a *Toke_szamla*, illetve az *ErtekPapirSzamla* osztály. A *Szamla* és az *Ugyfel* közötti kapcsolatot a Tartozik asszociáció írja le.

Egy adott számlafajtán egyszerre több különböző típusú értékpapír is lehet, ez tette szükségessé a *SzamlaRecord* osztály bevezetését. Egy *SzamlaRecord* az ügyfél egy adott számla fajtáján lévő adott értékpapírra vonatkozó információkat tárol (pl.: éppen ebben a pillanatban, az adott értékpapírból hány darab van az ügyfél tulajdonában).

A *SzamlaRecord* komponens relációban van a *Szamla*val. A *SzamlaRecord* a *ErtekPapirKonkret* asszociáción keresztül össze van kapcsolva az *ErtekPapir*ral (el lehet érni a *SzamlaRecord*on tárolt értékpapír tulajdonságait), valamint a Tartalmaz asszociáción keresztül a *TranzakcioKonkret*tel mik azok a tranzakciók, amik az adott értékpapírra, és így az adott *SzamlaRecord*ra vonatkoznak. A *Szamla* és a belőle származtatott *Toke_szamla*, *ErtekPapirSzamla*, valamint a *SzamlaRecord* alkotja a számla csoportot.

Az értékpapírhoz tartozik az *ErtekPapir* (absztrakt) a *Reszveny*, a *Kotveny* osztály. Az *ErtekPapir* tarolja az értékpapírok közös tulajdonságait (pl. Kibocsátó, Név stb.). Az *ErtekPapir*ból származik a *Reszveny*, illetve a *Kotveny*, mint egy-egy speciális értékpapírfajta.

A rendszerben történt összes tranzakciót a *TranzakcioKonkret* absztrakt, valamint a *JegyzesKonkret* és az *EladasKonkret* osztály tárolja (jelenleg a modellben csak ez a két tranzakciófajta van).

A *TranzakcioKonkret* tárolja az egyes tranzakció fajták közös jellemző paramétereit (pl. időpont, meghat_id, modify_uid, statusz stb.).

A *TranzakcioKonkret*ból öröklődik a *JegyzesKonkret*, valamint a *EladasKonkret*, amik egy-egy speciális tranzakció (jegyzés, eladás) adatait tárolja. Az öröklés bevezetésével itt is lehetőség nyílik a rendszernek új tranzakció fajtákkal történő bővítésére

A tranzakció típushoz tartozik a *TranzakcioTipus* a *JegyzesTipus*, az *EladasTipus*, *Jegyzes1,2,...*, valamint az *Eladas1,2,...* A *TranzkcioTipus* absztrakt osztály az összes tranzakcióra jellemző tulajdonságot tárol (tranzakció megnevezése, létrehozás ideje stb.). A *JegyzesTipus*, valamint az *EladasTipus* absztrakt osztályok egy-egy speciális tranzakciófajta jellemző attribútumait tarolja. A *Jegyzes1,2,...*, valamint az *Eladas1,2,...* osztályok egy-egy konkrét értékpapírhoz kapcsolódó tranzakciókat tartalmazza.

A szerver oldalhoz az *Applikacio_szerver* és az *TranzakcioTipusManager* tartozik. Az *Applikacio_szerver* metódusai végzik az egyes *Ugyfel*lel és az *ErtekPapir*ral kapcsolatos tevékenységeket (ügyfél felvétele, ügyfelek listázása, értékpapírok listázása). A *TranzakcioTipusManager* metódusai pedig a *TranzakcioTipus*sal kapcsolatos tevékenységeket végzik (lista a tranzakció típusokról, tranzakció típus megkeresése).

A kliens oldalhoz a felhasználói felület kialakításához szükséges osztályokat lehet besorolni, de ezekkel most nem foglalkozunk.

3.2.1.3. Dinamikus modell

A dinamikus modellezéshez állapot diagramot és kommunikációs diagramot használtunk, mert lényegesnek tartottuk az egyes objektumok közötti kommunikációt, illetve az egyes objektumok belső állapotát.

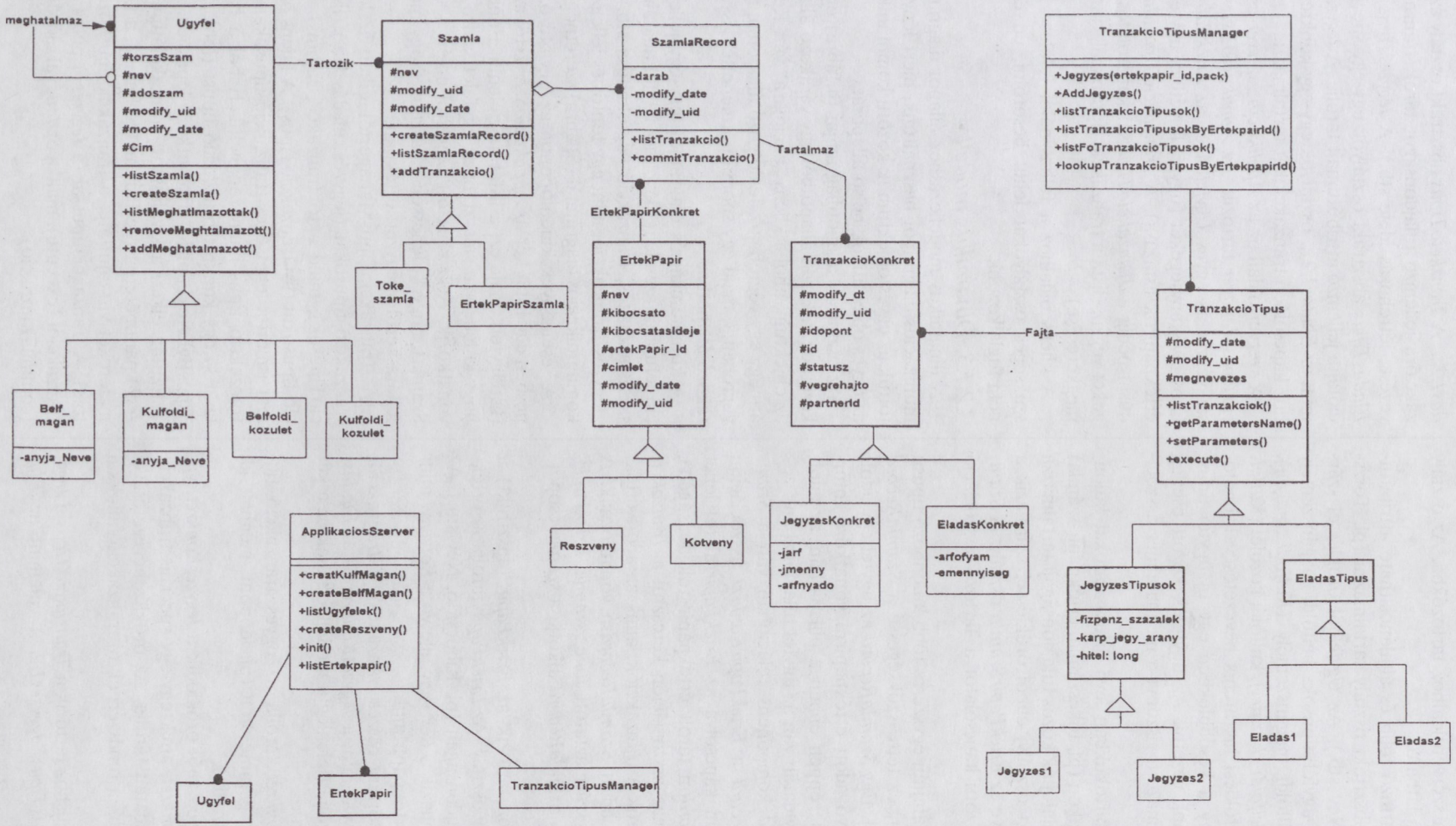
Az osztályok állapotdiagramjai (4. ábra) egyszerű szerkezetűek: a kezdő állapotból egy várakozó állapotba megy az objektum, ahol a kliens „akciójára" vár. Kérés hatására átmegy egy végrehajtó, feldolgozó állapotba, ahol a kérést végrehajtja, majd egy spontán átmenettel visszakerül a várakozó állapotba.

A kommunikációs diagramok egy-egy jellegzetes funkció lefutását szemléltetik: pl. az ügyfél adatainak megadása, listakészítés, tranzakció végrehajtása stb. Példaként a „jegyzés" tranzakció, mint egy fontos és jellegzetes funkció kommunikációs diagramját (5. ábra) szeretnénk bemutatni.

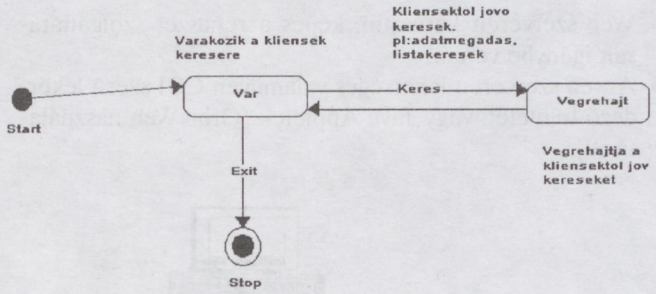
Az események kindulópontja az ügyintéző, aki első lépésben egy listát kér az *ApplikacioSzerver*től az ügyfelekről (listUgyfel), majd ezt a listát megjeleníti. Ennek az a célja, hogy ki lehessen választani az ügyfelet, akire a tranzakció vonatkozik. A kiválasztott *Ugyfel*től elkéri a számláit (listSzamla), hogy ki lehessen választani, hogy melyik számlafajtára kerül a jegyzett értékpapír.

A TranzakcioTipusManagertől elkéri a lehetséges fő tranzakció típusokat (jegyzés, eladás stb.) (listFoTranzakcioTipusok), majd a fő tranzakció fajtán belüli tranzakció típusokat (listTranzakcioTipus). A kliens program most már ismeri a lehetséges tranzakció típusokat egy nagyobb tranzakció típus halmazon belül. Ebből a halmazból választ ki egy konkrét tranzakció típust (lookupTranzakcioTipusByErtekPapirId) a következő lépésben.

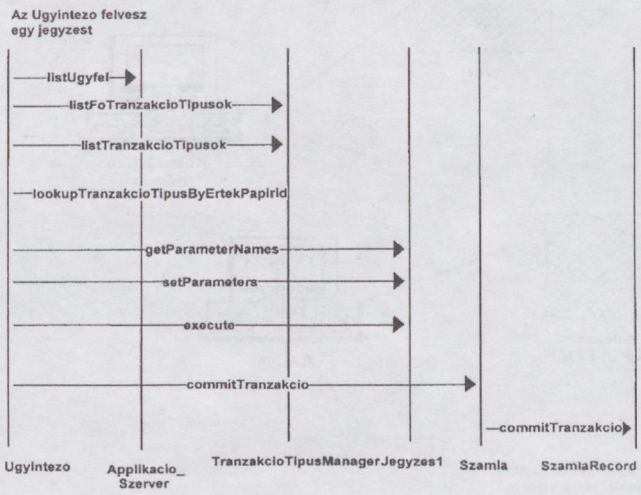
Ezután elkéri a kiválasztott tranzakciótípus (itt a *Jegyzes1*) paramétereit (getParameterNames), a kitöltött paramétereket visszajuttatja a tranzakciótípushoz (setParameters). A tranzakciótípussal (a *Jegyzes1*) pedig elvégezteti a tranzakciót (execute), majd a *Szamla*val „jóváhagyatja" azt (commitTranzakcio).



3. Ábra - Osztály diagram



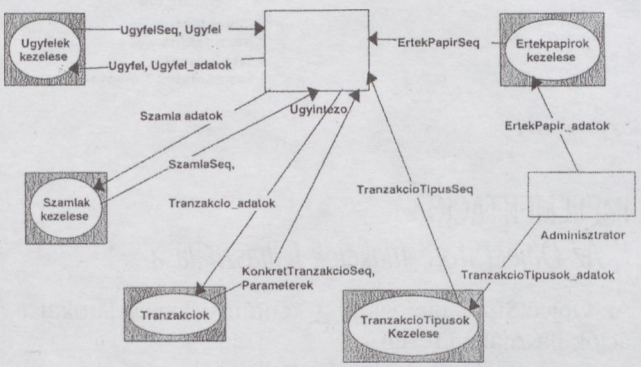
4. ábra. Állapotdiagram



5. ábra. Egy tranzakció (jegyzés) kommunikációs diagramja

3.2.1.4. Funkcionális modell

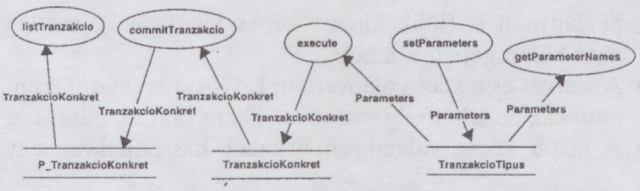
A funkcionális modellben (6. ábra) a két terminátor – az *Ugyintezo* és az *Adminsztrator* – és a rendszer közötti funkcionális kapcsolat került ábrázolásra egy DFD segítségével.



6. ábra. Funkcionális modell (DFD)

A rendszer funkcióit nagyobb csoportokba lehet besorolni (*Ugyfelek kezelese, Tranzakciok* stb.), az alapján, hogy min végeznek műveleteket, mihez kapcsolódnak. Példaként a tranzakciókhoz tartozó processzeket (7. ábra) szeretnénk bemutatni. A *Tranzakciok* az *Ugyintezo*vel áll kapcsolatba, tőle a tranzakciókra vonatkozó adatokat (*Tranzakcio_adatok*) kap. A *Tranzakcio_adatok* lehetnek: egy lista kérés részletei, a tranzakcióval kapcsolatos paraméterek értékei. Az *Ugyintezo* a *Tranzakcioktól* már megtörtént tranzakciók listáját (*KonkretTranzakcioSeq*), vagy a tranzakció paramétereit (*Parameterek*) kapja.

A *Tranzakciok* részletes kifejtése a 7. ábrán látható.



7. ábra. Tranzakciók processzei

Az egyes elemi processzek, az adatok és a store-ok rövid magyarázata:

- *getParameterNames*: a tranzakció típusra vonatkozó paraméterek nevét és típusát szolgáltatja.
- *setParameters*: a tranzakcióra vonatkozó paraméter értékeket állítja be.
- *execute*: végrehajtja a meghatározott tranzakciót az előzőleg megadott paraméterek szerint.
- *commitTranzakcio*: a tranzakció jóváhagyását végzi, berakja az adatbázisba.
- *listTranzakcio*: listát készít a már megtörtént tranzakciókról.
- *Parameters*: a tranzakció típusra vonatkozó paraméterek neve, típusa, értéke.
- *TranzakcioTipus*: egy adott tranzakció fajtára vonatkozó paramétereket tárolja.
- *TranzakcioKonkret*: egy megvalósult tranzakció adatait tartalmazza.
- *P_TranzakcioKonkret*: megvalósult tranzakciókat tartalmazó az adatbázisban.

Az egyes elemi processzek az objektum modellben mint metódusok jelennek meg: pl. a *listTranzakcio* processz a DFD-n megfelel a *listTranzakcio* metódusnak a *SzamlaRecord*ban.

3.2.2. Tervezés

Rendszertervezés: első lépésként az alrendszerekre bontást végeztük el. Három jól elkülöníthető alrendszerre lehet felbontani a rendszert: kliens oldali rész, szerver oldali rész és az adatbázis rész.

A kliens oldali részhez tartoznak a GUI elemei. A kliens oldali rész CORBA hívások segítségével kommunikál a szerver oldali résszel (az *Applikacio_szerver*rel és a *TranzakcioTipusManager*rel). Az *Applikacio_szerver* feladata kommunikáció a kliens oldallal, a kliens bizonyos kéréseinek a kezelése. A *TranzakcioTipusManager* végzi a tranzakciókkal kapcsolatos tevékenységeket.

A szerver oldalon van megvalósítva az összes funkció, a kliens oldalon csak az adatok megjelenítése, és bekérése történik.

Az adatbázis részbe tartozik az összes többi objektum (*P_Ugyfel, P_Szamla, P_Ertekpapir* stb.), ebbe a részbe tartozó objektumok közös jellemzője az, hogy perzisztensen kell őket tárolni.

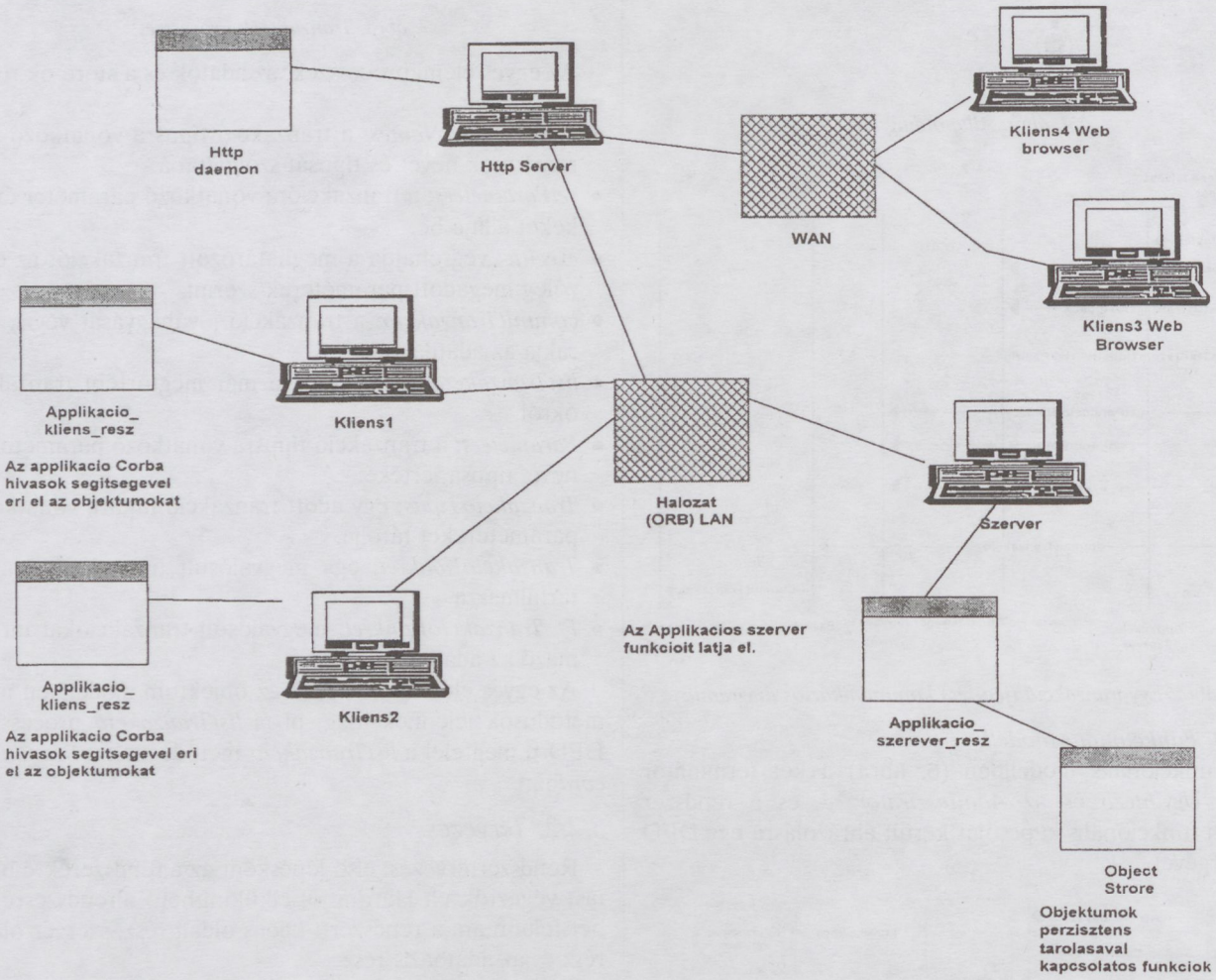
3.2.3. Architektúra

A rendszer egyes komponenseit a következőképpen rendeltük hardver elemekhez (8. ábra):

- A kliens rész (GUI) kerül a kliens gépekre, ezekből tetszőleges számú lehet.
- Az *Applikacio_szerver_resz*, valamint az *Object_Store* kerül a szervergépre. Az *Object_Store* egy példányban fut, az *Applikacio_szerver_resz* futhat egy vagy több

példányban is (több klienst képes kiszolgálni), esetleg akár külön gépen is lehet.

- A szerver és a kliens alapvetően LAN-on keresztül kommunikál, de lehetőség van távoli kliens csatlakozására is.
- A távoli kliens valamilyen browser használatával, egy Web szerveren keresztül, képes a rendszer szolgáltatásait igénybe venni.
- A web szerveren lehetséges valamilyen CGI-szerű lekérdező felületet, vagy Java Appletek (OrbixWeb használatával).



8. ábra. Architekturális diagram

Az adatbázis alrendszerhez tartozó objektumokat perzisztensen kell tárolni, erre a célra az ObjectStore-t használjuk.

3.2.4. Objektumtervezés

Az objektumok részletes tervezése során a következők lettek meghatározva:

- az egyes attribútumok típusa: jellegzetesen háromfajta típus szerepel: karakterlánc (char*), lebegőpontos (double), illetve egész (long);
- néhány metódus visszatérési értéke egy-egy lista (pl. az *Applikacio_Szerver* listUgyfel metódusának a visszatérési értéke egy, az ügyfeleket tartalmazó lista), e listákat a CORBA által nyújtott sequence típus segítségével valósítottuk meg;
- az osztályok közötti asszociációk megvalósítása az Object Store-os kollekciók segítségével történt.

4. IMPLEMENTÁCIÓ

4.1. Az ObjectStore funkciók felhasználása

Az ObjectStore támogatja a kétirányú kapcsolatokat a relációk használata révén.

Az egyes objektumok tárolása kollekciókban (halmazokban – *os_Set<Class*>*) történik. A kollekciók segítségével asszociatív módon (lekérdezésekkel) is hozzá tudunk férni az objektumokhoz, amire szükség is van a rendszerben.

4.1.1. A tranzakció-kezelés kibővítése

A rendszer működési elve szerint az applikációs kliens először lekéri az adatokat (adatbázis olvasás), majd a felhasználói felületen keresztül elvégzi a szükséges módosításokat és elmenti azokat (adatbázis írás). A lekérés és az elmentés között sok idő is eltelhet, ezért nem célszerű végig tranzakcióban maradni, mert azzal blokkolódik a hozzáférés a lefoglalt objektumokhoz. Ha az objektum(ok) olvasása után befejezzük a tranzakciót, ezáltal feloldva a

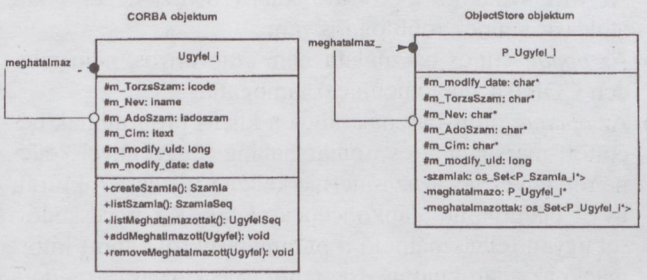
foglalást, akkor a többi kliens is hozzáférhet az adott objektumokhoz. Az írást külön tranzakcióban végezzük el. Ebben az esetben viszont felmerül az a probléma, hogy egy adott objektum megváltozhat egy kliens olvasása és írása közötti időben, ilyenkor a kliensnek nem szabad visszaírnia az adatait. A problémák áthidalására az a megoldás született, hogy időbélyegeket használnak az objektumok. Az időbélyeget alkalmazva, ha egy objektum időbélyege írási kísérletkor öregebb, mint a beolvasáskor volt, akkor a tranzakció abortál. Az időbélyeget az m_timestamp nevű long típusú attribútum tárolja. Ez kezdetben 0, majd minden íráskor eggyel nő.

4.1.2. Perzisztens mutatók megőrzése

A tranzakciók rövid ideig tartanak, ami növeli a hatékonyságot, de a tranzakció befejeztével a perzisztens objektumokra mutató mutatók érvénytelenné válnak az ObjectStore alapértelmezett működési módjában. Nem lenne túl hatékony mindig megkeresni az adatbázisban azt az objektumot, amit pl. frissíteni kell. Azt kellett elérni, hogy a perzisztens mutatók a tranzakció befejeztével is érvényben maradjanak, így egy következő tranzakcióban lehet hivatkozni rájuk. Ezt ObjectStore referenciákkal valósítottuk meg.

4.2. A CORBA és az ObjectStore objektumok

Az implementáció során számos probléma merült fel. A legfőbb gond, hogy a CORBA objektumokat nem lehet perzisztensen tárolni, ugyanis az ObjectStore séma generátora (ossg) nem tudja megállapítani a CORBA osztály sémáját, ami azért baj, mert a rendszerben tárolni kívánt összes objektum osztálya a CORBA osztály leszármazottja. E probléma áthidalására lenne hivatott az Orbix ObjectStore Adapter (OOSA) az IONA Technologies-tól, de ez nem állt rendelkezésünkre. Végül azt a megoldást választottuk, hogy az adatbázisban tárolni kívánt minden osztálynak lesz egy perzisztens tárolásra alkalmas megfelelője (9. ábra). Ezen osztályok neve a CORBA-s megfelelőjük neve elé történő *P_* illesztésével képződik. Pl. az *Ugyfel_i* CORBA osztály perzisztens tárolásra alkalmas párja a *P_Ugyfel_i* osztály.



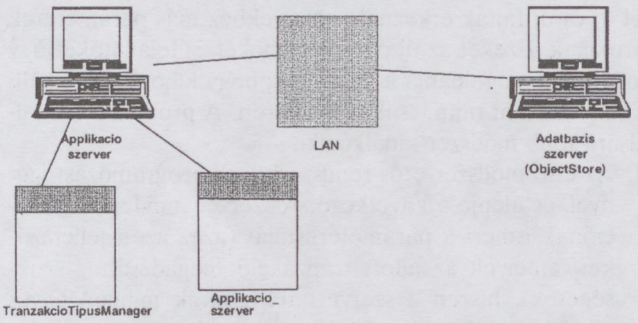
9. ábra. Eltérés a CORBA és az ObjectStore objektumok között

5. AZ ELKÉSZÜLT ALKALMAZÁS ISMERTETÉSE

5.1. A szerver oldal felépítése

A szerver oldalon kellett megoldani az Orbix és az ObjectStore összekapcsolását (10. ábra). A szerver oldalon két állandóan aktív CORBA objektum van az *Applikacio_szerver* és a *TranzakcioTipusManager*.

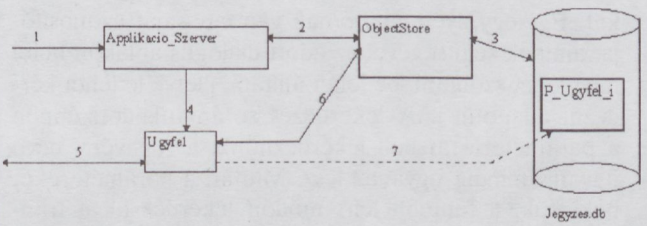
Az *Applikacio_szerver* végzi az „általános" adminisztratív tevékenységeket: ügyfelekkel, értékpapírokkal kapcsolatos tevékenységek. A *TranzakcioTipusManager* pedig a különböző tranzakciókkal kapcsolatos teendőket látja el.



10. ábra. Szerver oldal felépítése

Az adatbázis-kezelő egy másik gépen fut (természetesen a két szerver elhelyezkedhet azonos gépen is), az *Applikacio_szerver* és a *TranzakcioTipusManager* az adatbázis kezelő szolgáltatásait veszi igénybe. A kliens program először az *Applikacio_szerver*rel lép kapcsolatba az ORB segítségével, majd az Applikacio_szerver init metódusát meghívva megkapja a *TranzakcioTipusManager* címét. A szerver oldal működési módját egy példán keresztül (11. ábra) a legegyszerűbb bemutatni: egy új ügyfelet szeretnénk a rendszerbe felvenni, ez a szerver oldalon a következőképpen történik:

1. Első lépésben a klienstől egy új ügyfél felvételi kérés érkezik az *Applikacio_szerver*hez (meghívja az Applikacio-szerver createUgyfel metódusát).
2. Az *Applikacio_szerver* felveszi a kapcsolatot az adatbázis szerverrel, és annak interfészét használva létrehozza az ügyfélnek megfelelő perzisztens objektumot (*P_Ugyfel_i*-t).
3. Az a mód, ahogy az adatbázis-kezelő fizikailag kezeli az adatbázist rejtve marad az *Applikacio_szerver* elől.
4. Az *Applikacio_szerver* létrehozza az új ügyfélnek megfelelő CORBA objektumot, aminek a címét visszaadja a kliens programnak.
5. A kliens program ezután a létrehozott CORBA objektummal kommunikál közvetlenül, lekérdezi, beállítja annak attribútumait, használja annak metódusait.
6. Az újonnan létrehozott CORBA objektum is közvetlenül használja az adatbázis-kezelő interfészét az adatbázishoz való hozzáféréskor.
7. Az *Ugyfel* objektum tartalmazza az adatbázisban található perzisztens párjának (P_Ugyfel_i) a címét, ennek tárolására csak a gyorsabb adatbázis használat miatt került sor.



11. ábra. Példa a szerveroldal működésére

5.2. A kliens oldal felépítése

A kihívások egyike abban rejlik, hogy a tőzsdei tranzakciók sokféleségét és gyors változásait a programnak rugalmasan követnie kell. Az összes lehetséges tranzakció és paramétereik azonban nem ismertek fordítási időben, idővel új és új fajták érkeznek, amelyekhez más paraméterek tartoznak. Ezeket az új paraméterbekérési feladatokat úgy kell tudnia megoldania a kliensnek, hogy lehetőleg ne kelljen módosítani rajta, csak a szerveren. A probléma megoldására több módszer kínálkozik:

1. Az első módszer erős rendszerközeli programozást igényel, és alapja a következő. A szerver minden tranzakciónak ismeri a paraméterlistáját (azaz azon jellemzőket, amelyek az adott tranzakció megadásához szükségesek), hiszen a szervert felfrissítjük minden egyes alkalommal, amikor egy új tranzakcióval bővül a rendszer. A szerver a paraméterlista mellett tárolja a paraméterlista elemeinek típusát is, valamint resource-okat kezelni tudó grafikus felületet használó kliens (pl. MS Windows) esetén egy, a paraméterek bekérésére alkalmas ablak létrehozásához szükséges információt (MS Windows esetén egy dialógus ablak erőforrás). Amikor a kliens tranzakciót hajt végre, elkéri az objektum adatainak másolatát (ld. opaque kulcsszó). Mivel azonban nem rendelkezik az adatok értelmezéséhez szükséges kóddal, elvileg nem tudja értelmezni az adatokat. Itt kap szerepet a típus információ, ami egyértelműen megmondja, hogy milyen adatmezők találhatók az érték szerint kapott objektumban, amiket így a kliens típushelyesen tud kezelni. Az átadott resource kizárólag az operációs rendszernek szól, ami ez alapján fel tud építeni egy – a kitöltendő adatoknak megfelelő felülettel rendelkező – ablakot. A típusinformáció segít az adatoknak az ablaktól való lekérésében is. A hálózati adatforgalom csökkentésére a kapott leírók akár lokális cache-ben is elhelyezhetők átmenetileg. A módszer előnye a hatékonyság, hátránya, hogy rendszerközeli programozást igényel, és némileg eltávolodik az objektumorientált „fekete doboz" megközelítéstől.
2. A második módszer a CORBA korábban ismertetett Dinamikus Hívási Felületét (DII) használja a következőképpen. A kliens, amikor a végrehajtani kívánt tranzakció adatainak bekérésére van szükség, az *Object::get_interface* függvényhívással lekérdezi az aktuális tranzakciótípus interface-ét. Ebben szerepel egy *getParameterNames* nevű metódus, aminek paraméterlistája a paraméterek alapértelmezett értékeit tartalmazza, valamint a paraméterekhez tartozó controlID-ket, amik segítségével az MS Windows programozása lesz lehetséges. (Az MS Windows a dialógus ablakokban úgynevezett *Control*okban jeleníti meg az adatokat. Egy-egy ilyen *control*nak van egy saját azonosítója, aminek segítségével az adott dialógus ablakon belül meg lehet szólítani, be lehet állítani, illetve le lehet kérdezni állapotát.). A lekérdezés során tulajdonképpen a paraméterlistát kell lekérdeznünk, a függvény neve ugyanis mindig ugyanaz lesz. Miután a paramétereket bekértük, a fentebb leírt módon lekérdezzük a tranzakciót ténylegesen végrehajtó függvény paraméterlistáját (ami definíció szerint ugyanaz, mint a másik függvény paraméterlistája), és felépítjük, majd végrehajtjuk a függvényhívást az aktuális paraméterekkel, aminek hatására – amennyiben a megadott paraméterek helyesek, azaz a tranzakció által megkövetelt összes feltételnek eleget tesznek – végrehajtódik (regisztrálódik) a tranzakció. Ez a módszer ugyan teljes mértékben igazodik az objektumorientált programozás paradigmájához, ám az interface-lekérdezés sebességcsökkentő és hálózatterhelő volta jelentősen rontja alkalmazhatóságát a jelen probléma megoldásában.
3. A harmadik módszer rendkívül elegáns és – ellentétben az előzőekkel – nem igényel semmiféle speciális rendszerszintű ismeretet. Alapja az Iona OrbixWeb nevű, Java alapú CORBA implementációja, amely lehetővé teszi Java Appletek CORBA szerverekkel való összekapcsolását. A kliens tehát ez esetben nincs telepítve a munkaállomásokon, helyette le lehet tölteni a Java-ban megírt kliens szoftvert, ami így mindig a legújabb verziót képviseli, és ez esetben tartalmazza a tranzakciókhoz tartozó kódot is. A módszer előnye a rendszertechnikailag tiszta felépítés, ugyanakkor fel kell hívni a figyelmet néhány hátulütőre is. A kliens és a hozzá tartozó ORB letöltése rendszeresen terheli a hálózatot, illetve költségeket jelent. A Java technológia a rendkívül intenzív fejlesztések ellenére is lassabb, mint a gépi nyelv, és az is marad még jó ideig. Megemlítendő még, hogy az Appletek futtatókörnyezetéül szolgáló Internet böngészők korlátozzák az Applet számára rendelkezésre álló erőforrásokat, valamint a biztonsági szabályok betartásának ellenőrzése is csökkenti a kód hatékonyságát.

A módszerek egy kliensben való ötvözése nem megoldható, azonban a szerver felületének megfelelő kialakításával lehetővé vált két technológia egymástól független, de egyidejű alkalmazása. Ezáltal a rendszer a felhasználók egyik része számára a rendszerközeli programozásnak köszönhető többlet sebességet tudja nyújtani, míg a többi felhasználó számára az Internet nyújtotta korlátlan lehetőségeket, annak minden hátulütőjével együtt.

5.2.1. A Windows 95/NT alapú kliens

Az MS Windows alatt futó kliens ötvözi az első két megoldást, aminek több oka is van:

- Az *opaque* típus használata nem szabványos, nem minden CORBA implementáció támogatja.
- Az *opaque* típus használatához a kliens programnak beépített marshalling és unmarshalling függvénnyel kellene rendelkeznie, azaz ismernie kellene az adatstruktúrát, és ez ellentmond alapkoncepciónknak. Kis ügyeskedéssel ugyan felhasználható a paraméterekről kapott információ az adatoknak a streamből való kiolvasására, de a megoldás sokkal bonyolultabb lesz, mint a másik variáns, amikor a típusinformációval együtt visszük át az értéket is. A resource-oknak minden egyes alkalommal a hálózaton történő átvitele nem hatékony, célszerűbb azokat helyben tárolni, és rendszeres időközökben a hálózaton keresztül automatikusan frissíteni.
- A paraméterek lekérdezése rendkívül lassítaná a rendszert, terhelné a hálózatot.

A DII-n keresztül történő hívásfelépítéssel ugyancsak adódhatnak portabilitási problémák, a különböző implementációk és az egyes verziók közötti apróbb eltérések miatt. Végül a következő megoldás született:
A megjelenítéshez szükséges dinamikusan változó resourceokat (dialógus ablakok, a tranzakciók neve) a program egy külön DLL-ben (Dynamic Link Library) tárolja lokálisan. Ennek az állománynak a frissítésére a kliens szoftver minden induláskor egyezteti a szerverrel az éppen aktuális DLL verziószámát. Amennyiben a lokálisan tárolt verzió nem megfelelő, akkor letöltésre kerül az új, naprakész verzió. Erre tipikusan napjában egyszer kerül sor. Tranzakció végrehajtásakor a kliens a tranzakciótípustól lekérdezi annak paraméterlistáját a *getParameterNames()* függvény meghívásával, amely kitölt egy *JegyzesParameterLista* objektumot, minden paraméterhez megadva annak nevét, típusát, alapértelmezett értékét, valamint a paraméter értékének kiírásához használandó *control* (tipikusan *edit* típusú *control*) azonosítóját. A kliens ezen információk alapján meg tudja jeleníteni az adatokat, majd le tudja kérdezni a módosított értékeket. Ezután a kliens meghívja az *execute* metódust a kitöltött paraméterlistával.

5.2.2. A Web-es kliens

A Web-es kliens kialakításakor a cél az volt, hogy egy böngésző programmal egyszerűen, gyorsan lehessen a szerver szolgáltatásait elérni. Ennek megoldására napjaink népszerű Internet technológiáját a Java Appleteket használtuk. A Java használatával

- könnyen fejleszthető grafikus felület kialakítására nyílik lehetőség (az AWT (Abstract Windowing Toolkit) használatát támogató fejlesztő eszköz használatával),
- a Java platformfüggetlensége miatt a kliens gép majdnem tetszőleges hardvert és operációs rendszert tartalmazhat,
- könnyen meg lehet oldani a kliens oldalon a grafikus interfész frissítését (minden nap egyszer a kliens gép letölti az Appletet a szerverről, így a kliens mindig a legújabb változatot tudja használni.

A kliens fejlesztéséhez rendelkezésünkre ált az OrbixWeb3.0 programcsomag az IONA Technologies-tól. Az OrbixWeb segítségével CORBA alapú programokat lehet fejleszteni Java-ban. A csomagban megtalálható többek között egy IDL fordító, mely IDL-ek fordítását végzi Java kóddá, valamint egy Java-ban írt ORB.

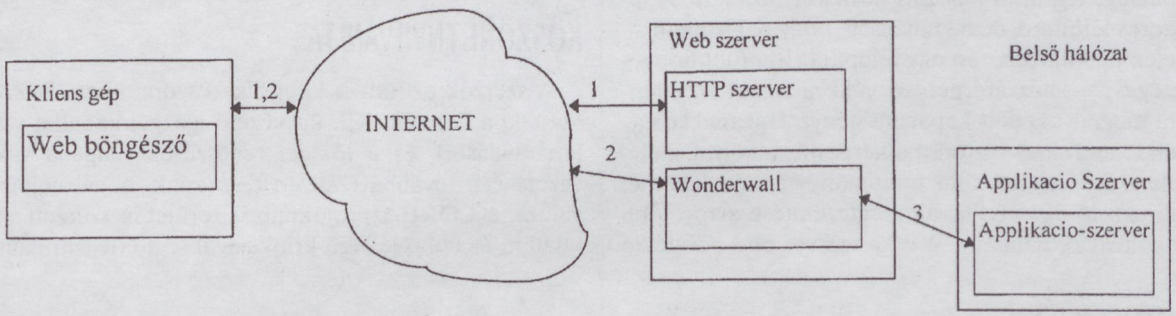
A grafikus felület fejlesztéséhez egy vizuális fejlesztést támogató fejlesztő környezetet használtuk. Java Appletek futtatásával kapcsolatban azonban nehézségek merülnek fel. Ennek az oka a Java-nak az Appletekre vonatkozó biztonsági megkötéseiben keresendő (pl. Applet csak a kódját tartalmazó géppel hozhat létre hálózati kapcsolatot stb.) [3]. Ezen megkötések „megkerülésére" léteznek megoldások [4]:

- Ún. signed Appletek alkalmazása: Java Appleteket digitális aláírással tudjuk ellátni. Az ily módon megjelölt Appletek a kliens gépre letöltve ugyanúgy viselkednek, mint a lokális Appletek. A módszer hátránya, hogy egy harmadik fél segítségét kell igénybe venni az aláírás hitelességének ellenőrzéséhez, valamint a különböző böngésző programok tekintetében nincs egységes eljárás a signed Appletek kezelésére.
- Sokkal jobb megoldást kínál IONA cég Wonderwall programcsomagjának a használata.

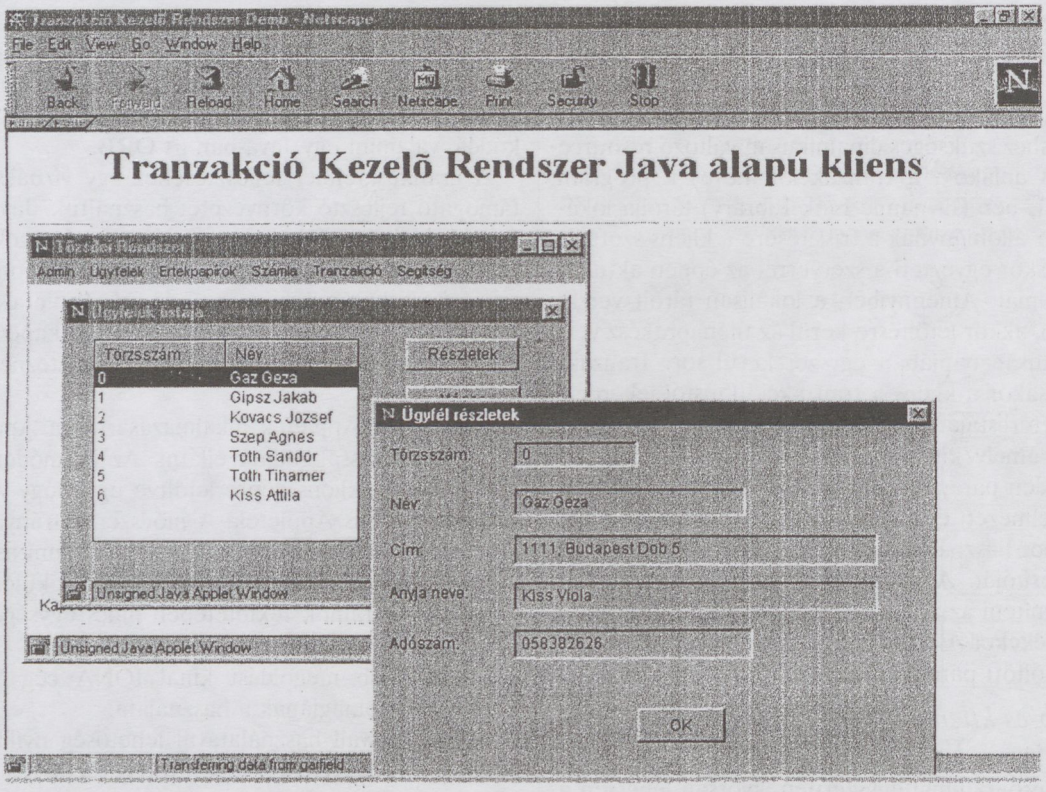
A Wonderwall használatával lehetőség nyílik egy IIOP (Internet Inter ORB Protocol) proxy tűzfal felállítására, ez a következőket nyújtja:

- lehetővé teszi a kérések és válaszok naplózását,
- IIOP forgalom routolásán keresztül az Appletek és háttérben lévő szerverek között (nem ugyanaz, mint a web szerver) megadható, hogy melyik klienstől fogadjon el kéréseket, valamint az egyes kliensek mely objektumokat érhetik el és azoknak mely metódusait használhatják,
- HTTP tunneling-et biztosít: egy mechanizmus a kliens oldali firewall átjárhatóságára (minden egyes IIOP üzenetet HTTP protokoll által kezelhető formában utazik a kliens és a Wonderwall között).

A Wonderwall alkalmazásával a következőképpen néz ki a Web-es kliens és a szerver program kapcsolata (12. ábra).
A 13. ábrán a Java alapú kliens grafikus felülete látható.



12. ábra. Web-es kliens és a szerver kapcsolata



13. ábra. Java alapú kliens

6. ÖSSZEFOGLALÁS

A bemutatott megoldások eredményeképpen a rendszer az alábbi tulajdonságokkal rendelkezik:

Rugalmasság: Mivel a fent ismertetett módon a kliens minden apriori ismeret nélkül végre tudja hajtani az adott tranzakcióhoz szükséges műveleteket, a kliens kódjának változtatására csak abban az esetben lehet szükség, ha valamilyen alapvető koncepcionális változtatásra kerül sor. Ennek valószínűsége azonban egy jól és körültekintően megtervezett rendszer esetében minimális. A Java alapú kliens rugalmasságát az állandó frissítés adja.

Hatékonyság: Ugyan a hálózati terhelést növeli az Applet rendszeres letöltése, de a szabadság, hogy bárhonnan – előfeltételek nélkül (pusztán egy telepített Internet böngésző szükséges) – hozzáférhetővé válik a rendszer, ellensúlyozza a megnövekedett kapacitásigényt. Ugyanakkor az Interneten felmerülnek biztonsági kérdések, amelyek mélyreható elemzése egy további tanulmány témája lehetne. A kommunikáció biztonságának megteremtése alapvetően nem az applikáció, hanem a WWW szerver és a böngésző feladata.

Az MS Windows alapú kliens a lehetőségekhez mérten kevés kommunikációval teszi lehetővé az igények dinamikus kielégítését.

Skálázhatóság: A kliensek a kezelni képes tranzakciótípusok számát illetően teljes mértékben rugalmasak az operációs rendszer szabta kereteken belül (legfeljebb 32767 féle resource tárolására van lehetőség egy resource forrásban). Az ObjectStore lehetőséget ad elosztott adatbázisok használatára, ami által a terhelésmegosztás, ill. az erőforrás-bővítés könnyen és a kliens számára transzparens módon megoldható.

KÖSZÖNETNYILVÁNÍTÁS

A szerzők ezúton is kifejezik köszönetüket *Konczos Tibor*nak, a Dorsum Kft. ügyvezető igazgatójának a szakmai tanácsadásért, és a tőzsdei rendszerek világába való bevezetésért, továbbá *Gesztesi Gábor*nak, hogy megosztotta velünk a CORBA programozás területén szerzett tapasztalatait, és építő jellegű kritikájával segítette munkánkat.

IRODALOMJEGYZÉK

[1] James Rumbaugh, Michael Blaha, William Premerlani, Fredrick Eddy, William Lorensen: Object – Oriented Modeling and Design ,1991., ISBN 0-13-630054-5
[2] Dr. Kondorosi Károly, Dr. László Zoltán, Dr. Szirmay-Kalos László: Objektum-orientált szoftverfejlesztés, 1997., ISBN 963-618-108
[3] Nyékyné G. Judit (szerk.): JAVA útikalauz programozóknak, 1996, ISBN 963 04 7417 4
[4] OrbixWeb Programmer's Guide, IONA Technologies PLC, November 1997
[5] Wonderwall Administrator's Guide, IONA Technologies PLC, December 1997
[6] Jon Siegel: CORBA Fundamentals and Programming, Wiley computer publishing, 1996., ISBN 0-471-12148-7
[7] Orbix Programmer's Reference, IONA Technologies PLC, Release 2.3, 1997.
[8] ObjectStore C++ API Reference, Object Design Inc., Release 5.0, 1997.
[9] Dimitris N. Chorafas – Heinrich Steinmann: Object-Oriented Databases, Prentice-Hall, 1993.

[10] Az Object Design Inc. weblapja (http://www.odi.com).
[11] CORBA 2.2 Update sheet, July 1998 http://www.omg.org/
[12] Orbix Programmer's Reference, Iona Technologies PLC, 1997

REALISATION OF STOCK EXCHANGE SYSTEMS USING OBJECT-ORIENTED TECHNOLOGY

DÁN GYÖRGY, GAJDOS SÁNDOR, LUKÁCS ZOLTÁN, NAGY PÉTER

TECHNICAL UNIVERSITY OF BUDAPEST
DEPARTMENT OF TELECOMMUNICATIONS AND TELEMATICS
H-111 BUDAPEST, PÁZMÁNY SÉTÁNY 1/D

As computer technology becoming more reliable computers play an important role in the financial and also in bank sector. It can be observed well from branches to broker companies. In this paper general and specific aspects of the topics are examined.
Developing applications for stock exchange, some special requirements – not arising in other areas – must be considered. Besides supporting large volumes of data and carrying out simple transactions quickly, distributed operation is essential too. And because of the changing rules of the stock exchange, applications must be quite flexible to alter them properly, moreover, without having to reinstall them. In addition to the general requirements of world's stock exchanges, there are some special, Hungarian needs as well.
The proposed solution is based on distributed object-oriented technology. That is why built the system on the advantages of CORBA, worked out by Object Management Group. By means of CORBA it is possible to design the distributed system network-independently. The dynamic modification of the client software (Windows or Web-Java based) is performed by the system automatically. On the server side data storing is provided by one or more object-oriented database placed behind the server application, that is invisible for the client. Thanks to invisibility, the system is scalable without any serious intervention, so it can adapt to the users' demands flexibly.

Dán György a Budapesti Műszaki Egyetem Villamosmérnöki és Informatikai Karán Műszaki Informatika szakon ötödéves hallgató. 1996-ban ösztöndíjjal a karlsruhei egyetemen töltött egy félévet, ahol egy helyben fejlesztett fordítóprogram Java Bytecode backend-jén dolgozott. Az egyetemi tanulmányai során mobil ügynök alapú és egyéb elosztott rendszerekkel, valamint multimédia-kommunikációval foglalkozik.

Gajdos Sándor a BME Villamosmérnöki karán 1986-ban villamosmérnöki oklevelet, majd 1988-ban híradástechnikai szakmérnöki oklevelet szerzett. Éveken keresztül digitális jelfeldolgozó processzorok távközlési alkalmazásaival foglalkozott, ebből a témából írta egyetemi doktori értekezését 1989-ben. A Távközlési Kutató Intézetben töltött két év után 1991-től a BME oktatója, jelenleg adjunktus. Érdeklődése az utóbbi években elsősorban az adatbáziskezeléshez kapcsolódó változatos területekre terjed ki. 1998. óta a Hewlett Packard-nál döntéstámogató rendszerek tervezésén dolgozik.

Lukács Zoltán ötödéves Műszaki Informatika szakos hallgató a Budapesti Műszaki Egyetem Villamosmérnöki és Informatikai Karán. Szakterülete az üzleti távközlés és a multimédia. Ezen kívül egy elosztott értékpapír-kezelő rendszer fejlesztésében vesz részt, valamint Web-es technológiákkal, adatbázis-kezelőkkel és adatbányászattal is foglalkozik.

Nagy Péter a Budapesti Műszaki Egyetem, Villamosmérnöki és Informatikai Kar, műszaki informatika szakon ötöd éves hallgató. Szakterülete a távközlés és szoftver tervezés. Az 1998. évi kari Tudományos Diákköri Konferencián Dán Györggyel és Lukács Zoltánnal hasonló témában első díjat kaptak az Informatikai rendszerek tervezése szekcióban.

ULTRAHANGOS TÁJÉKOZÓDÓ ESZKÖZ VAKOK SZÁMÁRA

MIHAJLIK PÉTER, TATAI PÉTER

TÁVKÖZLÉSI ÉS JELFELDOLGOZÁSI LABORATÓRIUM
TÁVKÖZLÉSI ÉS TELEMATIKAI TANSZÉK
BUDAPESTI MŰSZAKI EGYETEM
E-MAIL: {MIHAJLIK,TATAI}@BME-TEL.TTT.BME.HU

Az alábbi cikkben beszámolunk a BME Távközlési és Telematikai Tanszékén készülő ultrahangos tájékozódó eszköz fejlesztéséről. Célunk a visszhang alapján a tárgyak helyének közelítő meghatározása, és ennek a térbeli információnak sztereó hang formájában való visszajelzése a felhasználó számára. A készüléket kifejezetten vakok számára terveztük, de a megoldás egyes részletei máshol is felhasználhatók (pl. robottechnika, távolságmérés). A cikk elsősorban az ultrahang segítségével történő kétdimenziós helymeghatározással foglalkozik, de kitér a nem szokványos ember-gép kapcsolat tervezési problémáira is. Bemutatjuk a kísérleti eszköz áramköri felépítését és a jelfeldolgozó program működését. Ismertetjük az eddigi kísérletek eredményeit, valamint a készülék továbbfejlesztési lehetőségeit.

1. BEVEZETÉS

Az ultrahangos távolságmérés régóta ismert módszer a méréstechnikában. Az ultrahangimpulzus kibocsátása és a visszhang vétele között eltelt idő mérése révén érintésmentesen lehet távolságot mérni. Az eljárást a gyakorlatban több helyen alkalmazzák: például közeledésérzékelők, tolatásjelzők, riasztók, távolságmérők stb. Ezeknél az alkalmazásoknál általában egy adó és egy vevő (mely esetleg ugyanaz a transducer is lehet), elegendő a működéshez.

Ultrahang segítségével azonban ennél jóval több is megállapítható a környezetről. Jól ismert példa erre az állatvilágból a denevér, amely teljes sötétségben is tökéletesen tud tájékozódni. Nem meglepő, ha többeknek – így nekünk is – eszünkbe jutott, hogy az ismert távolságmérős módszert továbbfejlesztve, „denevér-elven" tájékozódó eszközt készítsünk vakok számára. Azt tűztük ki célul, hogy a legközelebbi akadály távolságát és irányát meg tudjuk határozni, és jól érzékelhetően jelezzük a vak felhasználónak. Ehhez legalább két vevőre, egy adóra, érzékeny vevőáramkörökre, pontos időmérésre és a visszajelzéshez célszerűen két csatornán (sztereó) jó minőségű hanggenerálásra van szükség. Lehetséges lenne tapintásra alapozott visszajelzés is, azonban ily módon nehéz lenne hatékony sztereó visszajelzést megvalósítani.

A tervezés során alapvető szempont volt, hogy az eszközt olyan alkatrészekből építsük fel, amelyek könnyen beszerezhetők, nem speciális drága áramkörök, tekintettel a lehetséges vásárlók anyagi lehetőségeire. Ugyanakkor lényegesnek tekintjük az egyszerű kezelhetőséget és a kis áramfogyasztást. A készülék egyelőre csak kísérleti formában létezik, de terveink szerint hamarosan elkészül egy kompaktabb, az adott feladatra optimalizált modell, amelyben minden áramköri rész egy kártyára kerül.

2. ULTRAHANGOS AKADÁLYLOKALIZÁCIÓ

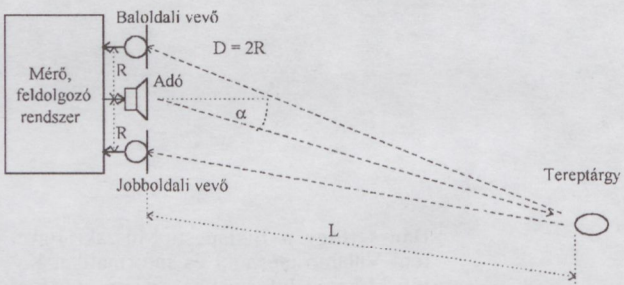
A következőkben szeretnénk ismertetni azt az eljárást, amelyet a készülékünkben alkalmazunk tárgyak helyének közelítő meghatározására. Először az ideális esetet vizsgáljuk, majd az ettől való eltéréseket tárgyaljuk.

2.1. Matematikai modell

Az idealizált matematikai modell az alábbi feltételezéseken alapszik:

- Az ultrahang sebessége állandó, v = 340 m/s.
- Az ultrahanghullám nem csillapodik (vagy a vevő érzékenysége végtelenül nagy).
- A detektálandó tárgy tökéletesen visszaveri az ultrahangot.
- Az ultrahang adó és a vevők izotropok.
- Egyetlen detektálandó tárgy van, amelynek mérete jóval kisebb mint a vevők egymástól mért távolsága.

A fentiek alapján a mérés elve és az elrendezés az 1. ábrán látható.

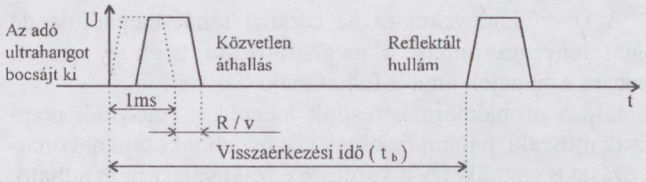


1. ábra. A kétdimenziós helymeghatározás elve

A mérés menete:

1. Az adó egy adott, kb. 1 ms szélességű ultrahangimpulzust bocsát ki.
2. Az impulzus kezdetével egyidőben indítjuk az időmérést a két vevőnél.
3. Először a közvetlen hullám jut a vevőkbe, tehát 1 ms + R/v ideig nem vesszük figyelembe a bemenetre érkező jeleket.
4. Az ultrahanghullám eléri a tereptárgyat és visszaverődik.
5. A visszavert hullám eléri az egyik, majd a másik vevőt.
6. A visszavert hullámok beérkezésének pillanatában leállítjuk az időmérést a megfelelő oldalon.

Szemléltetésül az egyik oldalon vett jel a 2. ábrán látható.



2. ábra. Az egyik vevő által vett jel

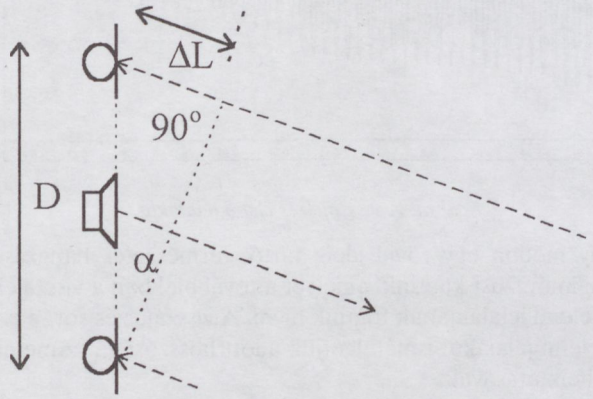
A jobb- és baloldali visszaverődési idő alapján, L » D feltételezéssel élve, a tárgy távolsága és iránya a következőképpen határozható meg:

- A távolság a két visszaérkezési idő átlagából kiszámítható.

$$L_b = \frac{v \cdot t_b}{2}\,, \quad L_j = \frac{v \cdot t_j}{2}$$

$$L \equiv \frac{L_b + L_j}{2}\,.$$

- Az irány meghatározásánál feltételezzük, hogy a két vevőbe érkező hanghullámok közel párhuzamosak (3. ábra). A hullámok beérkezési idejének különbségéből az α szög az alábbi módon számítható:



3. ábra. Az irányszög számításának szemléltetése

$$\alpha = \arcsin \frac{\Delta L}{D} = \arcsin \frac{\Delta t \cdot v}{D}$$

ahol $\Delta t = t_b - t_j$.

Mivel digitális rendszerrel dolgozunk, az időmérés pontosságát a mintavételi idő korlátozza. Legyen $\Delta t = k \cdot T$, ahol $T = \frac{1}{f_s}$ a mintavételi időköz, ekkor $\alpha = \arcsin\left(\frac{v \cdot k \cdot T}{D}\right)$.

A kísérleti eszköz paramétereivel ($D = 0.13$ m, $T = 62,5\mu s = \left(\frac{1}{16kHz}\right)$) számolva az érzékelt szög k-tól függően az alábbi értékeket veheti fel (1. táblázat).

1. táblázat. A mért irányok lehetséges értékei

k	0	1	2	3	4	5	6
α	0°	9,4°	19,0°	29,0°	40,8°	54, 8°	74,7°

Magasabb k értékeknél a szög 90°-nál nagyobbnak adódna. Látható, hogy a véges mintavételi frekvencia a szög kvantáltságát okozza, ami jelen esetben nem probléma, mert (mint később látni fogjuk) az emberi irányhallás sem lényegesen pontosabb ennél.

Bár eddig az ideális esetet vizsgáltuk, a modell alapján általános érvényű megállapításokat tehetünk, melyek a valóságos eset elvi korlátait adják meg.

- A minimális érzékelhető távolság:
  $L_{\min} = \frac{v \cdot \left(1ms + \frac{R}{v}\right)}{2} = 20,25$ cm
- A távolságmérés max. pontossága:
  $\Delta L_{\min} = \frac{v \cdot T}{2} = 1,06$ cm
- Az iránymeghatározás max. pontossága:
  $\Delta\alpha_{\min} = \arcsin\left(\frac{v \cdot T}{D}\right) = 9,4°$

2.2. Eltérések valós körülmények között

- Az ultrahang sebessége (hangsebesség) a levegő hőmérsékletének függvénye. Ennek következménye, hogy a mért távolság is függ a hőmérséklettől.

2. táblázat. A hang terjedési sebessége levegőben különböző hőmérsékleten

T (°C)	-10	0	10	20	30
v (m/s)	325,6	331,8	337,8	343,8	349,6

Ez nem várt hibákat okozhat. Például a 15 OC-on 340 m/s-ra beállított műszerrel egy jól fűtött szobában ugyanazt a távolságot kb. 2,7 %-kal rövidebbnek, fagyponton pedig ugyanennyivel hosszabbnak érzékeljük:

$$t = \frac{1L}{v'}, \quad L' = \frac{v \cdot t}{2} = \frac{v}{v'}L\,.$$

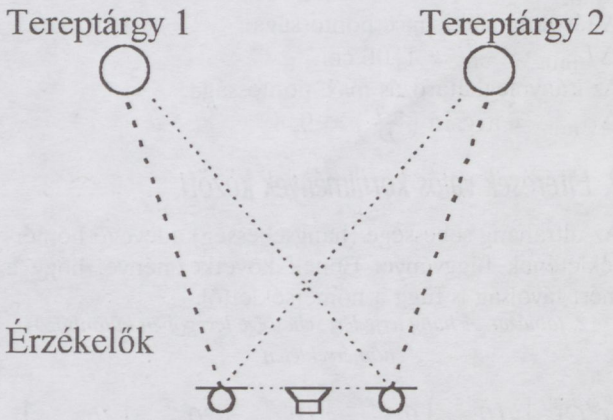
Ha $L = 3,40$ m, $v = 340$ m/s ($T = 15$°C),

- $L' = 3,302$ m ($T = 30$°C),
- $L'' = 3,492$ m ($T = 0$°C).

Vagyis majdnem 10 cm-t tévedtünk. Ez nem elhanyagolható, de az adott alkalmazásnál nem jelentős hiba.

- A hanghullám kb. a távolság négyzetével fordított arányban csillapodik, így véges adóteljesítmény (és vevőérzékenység) mellett az érzékelhető távolság korlátozott. Az általunk használt transducerek kimeneti teljesítménye és érzékenysége esetén ez az érték 4-6 m körüli.
- A detektálandó objektumok a felületük alakjától, kiterjedésétől és minőségétől függően igen változatos módon, vagy néha szinte egyáltalán nem verik vissza az ultrahanghullámot. Ez egy komoly probléma, ugyanis a kis kiterjedésű és /vagy puha felületű tárgyak nem, vagy csak nagyon közelről vehetők észre ezzel a módszerrel. Az effektív hatótávolság tehát egyes tárgyakra jóval kisebb is lehet, mint a csillapításból eredő korlát.
- Az ultrahang adók és vevők az antennákhoz hasonlóan amplitúdó-iránykarakterisztikával rendelkeznek. Tehát a túlságosan jobb-, ill. balszélen lévő tárgyakat kevésbé lehet észrevenni. Ez igazából nem probléma, hiszen pl. egy 2 m-re 80°-ra balra lévő szekrény a vak mozgását nem zavarja. Az általunk használt adó-vevőknél a -10 dB-es irány 35°-65° körül van.
- A valóságos esetek nagy részében több tereptárgy veszi körül a felhasználót. A bonyolult, többszörös visszaverődéseket tartalmazó jeleket nehéz kiértékelni, ezért csak a legközelebb lévő (legveszélyesebb) tárgyat jelezzük vissza. Ezzel visszavezettük a problémát az egyetlen akadály esetére.

Egy kis tévedési lehetőséget azért rejt magában az eljárás, ugyanis elképzelhető olyan eset, hogy a jobboldalon elsőként beérkező reflektált hullám más tárgyról verődött vissza, mint a baloldalon detektált első hullám (4. ábra).



4. ábra. Példa a tereptárgyak speciális elrendezése esetén fellépő helymeghatározási bizonytalanságra

Súlyos problémát ez sem okoz, mert könnyen belátható, hogy ilyenkor valahová a két tárgy közé fog jelezni az eszköz. Ez, ha a két tárgy közel van egymáshoz, akkor egyáltalán nem baj, ha távol vannak egymástól, akkor pedig egészen kicsi elmozdulás is azt fogja eredményezi, hogy az eszköz a jobb- vagy baloldalra lévő tárgyra „fókuszál".

3. SZTEREÓ HANGÚ VISSZAJELZÉS

Ebben a fejezetben arról szeretnénk tájékoztatni az olvasót, hogy milyen problémák merülnek fel egy ilyen speciális ember-gép kapcsolat tervezése során, milyen lehetőségeket találtunk, és milyen megoldást választottunk végül.

3.1. A visszajelzés általános problémái

A feladat a következő: adott egy tárgy (2 dimenziós) helye a mérőeszközhöz viszonyított koordináta rendszerben. Jelezzük vissza ezt a két számértékkel jellemezhető elvont fogalmat a felhasználó számára úgy, hogy nem adhatunk át semmiféle vizuális információt.

A tájékoztató jelzésnek további követelményeket is teljesítenie kell:

- A jelzés magától értetődő, gyorsan és egyszerűen kiértékelhető legyen.
- A lehető legkisebb mellékhatást okozza, vagyis minél kevésbé zavarja a külvilágból érkező egyéb, esetleg létfontosságú (hang-)jeleket.
- Hosszútávon se legyen kellemetlen a felhasználó számára.

Nem kétséges, hogy a hallásra érdemes a visszajelzést alapítani, mint ahogy ezt már meg is előlegeztük.

Ezen megfontolások alapján a visszajelzés két független hangcsatornán történik, a jelek sztereo fejhallgató segítségével jutnak el a felhasználóhoz. Az ultrahang visszaverődés kiértékelésére és a visszajelzés előállítására digitális jelprocesszort (DSP: Digital Signal Processor) alkalmazunk, így elvileg szinte bármilyen bonyolult sztereó jelet elő tudunk állítani.

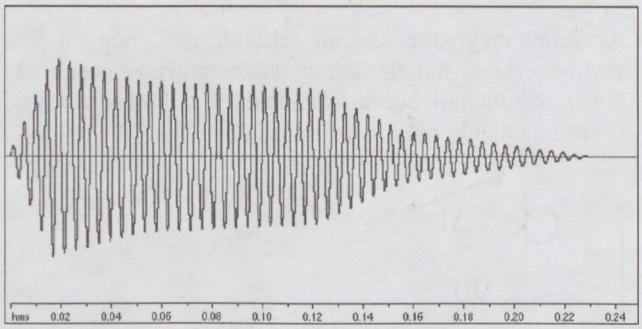
A követelményeket és az eszközt tehát megadtuk, de igen lényeges annak a meghatározása is, hogy milyen legyen a hangjel, amit a felhasználó hallani fog.

Olyan problémára keresünk megoldást, melynek nemcsak műszaki, hanem fiziológiai és pszichoakusztikai vonatkozásai is vannak, így a kérdésre egzakt válasz nem adható. Az intuitív úton kialakított elképzelések közül kísérletezéssel választottunk ki egy lehetséges megoldást. Ezen kísérleteinkről bővebb leírás található az [5]-ben.

Az alapelv a következő:

- Először előállítunk egy fix hosszúságú alapjelet, ami jelen esetben folytonos színuszjel.
- Speciális burkolóval látjuk el, mely egy gyors felfutású szakaszból, hosszabb „tetőesésből" és lecsengési részből áll.

Az így előállított jelalak az 5. ábrán látható.



5. ábra. A visszajelzés elemi jelalakja

Ily módon egy rövid ideig tartó, természetes hangzású hangimpulzust kapunk, amelyet a továbbiakban a visszajelzés elemi jelalakjának fogunk hívni. A visszajelzés során ezt az elemi jelalakot ismételgetjük adott hosszúságú szünetek közbeiktatásával.

- A távolságot az alapjel frekvenciájának (200...800 Hz) és a beiktatott szünetek hosszának (0.3...0.8 s) változtatásával érzékeltetjük.
- Az irányt úgy jelezzük vissza hogy a megfelelő elemi jelet mindkét hangcsatornára kiküldjük, de az egyik csatornára egy kis időkéséssel és valamivel kisebb amplitúdóval.

Ez a visszajelzési mód a tapasztalat alapján teljesíti a fenti követelményeket. Ugyanakkor előbbrelépés a hangjelzés térbeli hatásának elérése érdekében lehetséges. Ehhez azonban először vázlatosan meg kell ismerkednünk a térbeli hallás néhány alapfogalmával.

3.2. Térbeli hallás

Nyilvánvalóan az lenne a legszemléletesebb visszajelzés, ha a hallgató úgy érezné, mintha az akadály adná ki a hangot. A mindennapi életben is tapasztaljuk, hogy egy hangforrás iránya, térbeli elhelyezkedése elég jól megállapítható.

Az a távlati célunk, hogy fejhallgatón keresztül mesterségesen tudjunk olyan hangot kelteni, ami úgy szól, mintha a megadott távolságban és irányban lévő forrásból jönne. Annak eldöntésére, hogy ez mennyiben és milyen módon lehetséges tanulmányozzuk egy kicsit az emberi térbeli hallást.

A térbeli hallás talán egyik legfontosabb kérdése, hogy hogyan lehet „mindössze" két fül segítségével egy hangforrás helyét három dimenzióban érzékelni. A több hangforrás, többszörös reflexiók (visszhangzó szoba) problémáira a cikk keretei között nem térhetünk ki, csak az egyetlen forrás helyének meghatározásáról lesz szó.

Logikailag két részre bonthatjuk a térbeli hallás témakörét: távolságmeghatározásra és térbeli iránymeghatározásra.

A távolságot elég pontatlanul tudjuk megbecsülni, alapvetően két jellemzőből tudunk rá közvetkeztetni. Az egyik az abszolút hangosság, a másik pedig, hogy a magasabb hangok a levegőben jobban csillapodnak, mint a mélyek, vagyis minél távolabb van a hangforrás, annál inkább aluláteresztőként viselkedik a légtér.

Az irányérzékelés – talán evolúciós okokból – sokkal pontosabb. Háromféle alapesetet különböztetünk meg:

- a horizontális (vízszintes) síkban,
- a frontális síkban,
- és a mediális (vagy szagittális) síkban történő iránymeghatározást.

A síkokra bontásnak nemcsak rendszerezési okai vannak, hanem a különböző síkokban más mechanizmussal is történik az iránymeghatározás.

Az első kettővel a „kétfülű hallás" (binaural hearing) foglalkozik, az utolsóval az „egyfülű" (monaural hearing – ekkor ugyanis mindkét fülbe elvileg azonos jel jut) [2].

Érdekes, hogy hogyan lehetséges a mediális síkban (a fej szimmetriasíkjában) lévő hangforrás irányát meghatározni. A fej és a fülek aszimmetriájának következtében a különböző emelkedési szögeknél másképpen szűrve érkezik a dobhártyához a hangjel. Így a hallás során történő spektrális elemzésnek köszönhetően közelítőleg meg tudjuk becsülni a hangforrás helyét. Persze, csak ismert spektrumú hangra működik jó hatásfokkal az eljárás, vagyis az iránymeghatározó képesség tanulási folyamat eredménye. Ezért ebben a síkban nem hallunk túl pontosan, és könnyen tévedhetünk a hangforrás helyét illetően.

A horizontális (vízszintes) síkban a két füljel – az előző esettel szemben – különböző, így itt sokkal jobb lehet az irányszögfelbontás. Természetesen a spektrális elemzésnek ez esetben is fontos szerepe van – erre még később kitérünk –, azonban ennél egyszerűbb mechanizmusok adják az iránymeghatározás alapjait:

- Amikor egy hangforrás nem pontosan szemben van, az általa kibocsátott hanghullámok az egyik fülhöz kisebb utat tesznek meg, mint a másikhoz, így a két fülbe időkülönbséggel érkezik meg a hang. Ez a kicsi időkülönbség döntően fontos az irány meghatározása szempontjából, így külön jelöléssel ITD (Interaural Time Difference) illetik.
- Ehhez hasonlóan, oldalirányú beesésnél a fej és a fülek árnyékoló hatása miatt a két fülbe érkező hangjelek szintje különbözik. Erre a paraméterre az ILD vagy IID (Interaural Level Difference vagy I. Intensity D.) rövidítés használatos.

Az abszolút szintnek, illetve időnek nincs szerepe az irány meghatározásában, csak a két fül közötti különbség számít. Mindkét mennyiség monoton függvénye a beesési szögnek (0° – 90° között), és az ILD a hang frekvenciájától is függ.

Az ITD és az ILD az irány érzékelésében egyaránt fontos, de alacsonyabb frekvenciákon (1.6...3 kHz alatt) az előbbi dominál, magasabb frekvenciákon (3 kHz fölött) az utóbbi a meghatározó. Tehát jó irányérzet szimulálásához az ITD-re és az ILD-re egyaránt szükség van.

Laterizáció és lokalizáció

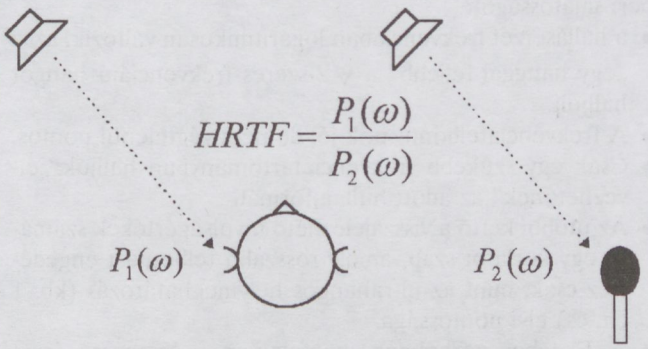
Ha – például fejhallgatón keresztül – a jobb és bal fülbe hangot vezetünk, ahol a két oldal között egy adott irányszögnek megfelelő idő- és amplitúdókülönbség van, egyértelmű irányhatást fogunk érzékelni. Ezt is vártuk, de összehasonlítva valamely külső forrásból származó hanggal, sokkal szegényesebb a hangzás, egész pontosan egyáltalán nem térbeli, egyszerűen csak egy irányt érzékelünk, és a hang forrása mintha a fejünkben lenne.

Az irodalomban ezt fejközép-lokalizációnak hívják [2], és azért történik, mert külső hangforrás jelét a fej és a külső fülek mindig sajátos módon megszűrik, ami ebben az esetben elmaradt.

Más megközelítéssel élve, az ITD és ILD szimulálásával csak laterizációt érhetünk el, a külső térbeli érzethez – a lokalizációhoz – a spektrum formálására is szükség van [4].

Fejhez rögzített átviteli függvények

Ha valósághűbb térbeli hangot szeretnék előállítani, akkor figyelembe kell venni a fej és a külső fül akusztikai árnyékoló-szűrő hatását. Mondhatjuk úgy is, hogy a hangforrás és a hallójárat bemenete közé egy átviteli függvénnyel jellemezhető csatorna ékelődik. Ez az átviteli függvény természetesen a tér három koordinátájától is függ (a frekvencián kívül), és HRTF-nek (Head Related Transfer Function) hívják.



6. ábra. A (monaurális) HRTF mérési elve

A jobb és bal fülhöz tartozó HRTF-ek szimulálásával elvileg tetszőleges térbeli elhelyezkedésű hangforrás-érzet kelthető. A nehézséget az jelenti, hogy elvileg végtelen sok átviteli fügvény kellene ehhez. Szerencsére a távoltérben ($r > 1$ m) a HRTF-ek a távolságtól jó közelítéssel függetlenek, így csak két koordináta függvényében szokták mérni őket. Az adabázisméret csökkentése érdekében térbeli interpoláció alkalmazható a függvények között, jó HRTF modell – a függvények bonyolultsága miatt – egyelőre nem ismeretes.

A pontosságot befolyásoló hatások

Az iránymeghatározás pontossága sok körülménytől függ. A hallási folyamatban történő spektrális elemzést az is igazolja, hogy szélessávú jelekre nagyobb a pontosság, mint a keskenysávúakra. Hosszú ideig tartó hangjelek for-

rását is pontosabban tudjuk azonosítani. Bizonyított, hogy a fejmozgás engedélyezésével is növekszik a pontosság, és a „front-back" hiba (a mediális síkban az elől-hátul irány felcserélése) is megszűnik. Összefoglalva, az irányérzékelési hiba a körülményektől függően ritkán nagyobb mint 10°, és az abszolút minimum 1° körül van [3].

A frontális síkban történő iránymeghatározással nem foglalkozunk külön, a másik két síkban lévő mechanizusok működnek itt is.

Az irodalomkutatási eredményeket összefoglalva azt mondhatjuk, hogy laterizációval – vagyis az ITD és ILD szimulálásával – lehet egyszerűbben visszajelezni az irányt, ha azonban szemléletes térbeli érzetet akarunk kelteni, akkor a HRTF-ek alkalmazandók.

Jelenleg az egyszerűbb módszert használjuk, de becsléseink alapján a hardver HRTF szimulálásra is alkalmas, ezért a közeli jövőben ennek a kipróbálását tervezzük.

3.3. A megvalósított visszajelzés

A tájékoztató hang mintáit egy DSP állítja elő, majd két csatornán, 14 bites, 16 kHz-es D/A átalakítókon keresztül adja ki a jobb- és baloldali hangcsatornára.

A visszajelzés két független részre bontható:

- távolság-
- és irányjelzésre.

A *távolság* visszajelzésének fő eszköze a hangmagasság változtatása. Ezt az alapjel frekvenciájának változtatásával érjük el: ha közelebb van a tárgy, nagyobb frekvenciájú, ha távolabb van, alacsonyabb frekvenciájú jelet állítunk elő. Így „ál-Doppler hatást" is elérünk.

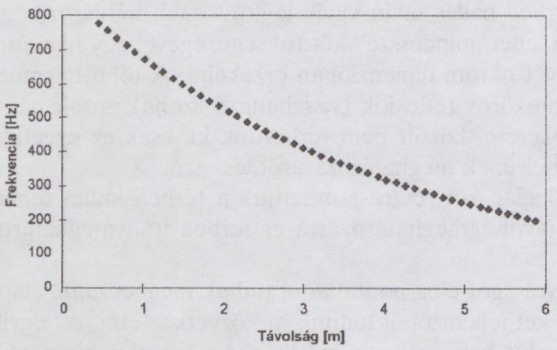
A megvalósításnál figyelembe kellett venni néhány emberi sajátosságot:

- a hallásérzet frekvenciában logaritmikusan változik, azaz „egy hanggal feljebb" a $\sqrt{2}$-szeres frekvenciájú hangot halljuk.
- A frekvenciafelbontásunk jó, de nem végtelenül pontos.
- Csak egy szűkebb frekvenciatartományban halljuk „élvezhetőnek" az adott hullámformát.
- Az utóbbi kettő a visszajelezhető távolságértékek számára egy korlátot szab, amely rosszabb felbontást engedélyez csak, mint az ultrahangos helymeghatározás (kb. 1 cm-es) elvi pontossága.
- A Fletcher görbéknek megfelelően a hangosságérzet erősen függ a frekvenciától [1].

A felsoroltaknak megfelelően a jelenleg megvalósított visszajelzésnél 49 fokú lépcsővel érzékeltetjük a távolságot, ahol a lépcsőfok egy negyedhang változást (a „kisszekund fele") jelent. Az alsó frekvencia 200 Hz, a felső 800 Hz.

Az alapjelet a DSP memóriájában lévő 256 pontos színusztábla segítségével állítjuk elő. Ebből lineáris interpolációval 16.536 pontos virtuális színusztáblát készítünk, így a kívánt frekvenciát kb. 1 Hz pontossággal tudjuk előállítani. A távolság és a frekvencia közötti nemlineáris leképezés egy memóriába bevitt táblázat alapján történik.

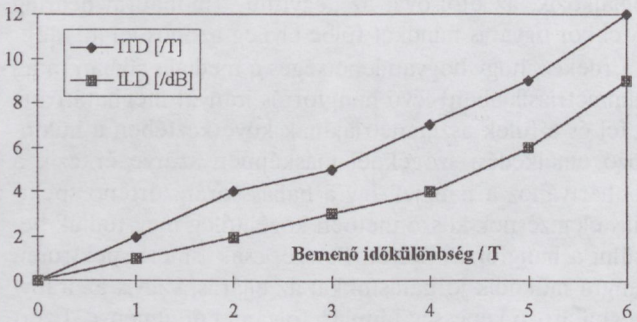
A távolság visszajelzésének másodlagos eszköze a hangkiadások közti szünet változtatása. Vagyis, ha közelebb van a visszajelzendő tárgy, akkor az elemi jelalakok közötti szünet rövidebb, ha távolabb van, hosszabb. A távolság-szünethossz kapcsolat egyszerű, lineáris.



7. ábra. A visszajelző hang frekvenciája a távolság függvényében

Az irány visszajelzése az előző alfejezetben ismertetett ITD és ILD paraméterek változtatásával történik. Mivel a készülék által érzékelhető szög kvantált (kb. 10 fokos lépcsővel), véges számú irányt kell csak visszajelezni. Így itt is alkalmazható a táblázatos módszer az irány és az ITD, ILD közötti leképzésre (a megfelelő értékeket az [1], [2] szakirodalmakból vettük át).

A gyakorlatban nem érdemes szétválasztani az ultrahanghullámok beérkezési időkülönbsége -> irány és irány -> ITD,ILD leképezéseket, hanem egy lépésből elvégezhető a konverzió. Ezt szemlélteti a 8. ábra.



8. ábra. A kétoldali visszhangok beérkezése közti idő leképezése az irány visszajelzés ITD és ILD paraméterére

3. táblázat. A kétoldali visszhangok beérkezése közti idő leképezése az irány visszajelzés ITD és ILD paraméterére

k	0	1	2	3	4	5	6
α	0°	9,4°	19,0°	29,0°	40,8°	54, 8°	74,7°

Az ITD realizálása egy szoftveres késleltető művonal segítségével történik, az ILD-hez pedig csak egy szorzásra van szükség.

Természetesen az így megvalósított visszajelzés az irányt csak lateralizációval adja vissza, de ez nem feltétlenül baj. A tapasztalatok szerint így is egyértelműen érzékelhető a hang irányítottsága, a jövőben pedig ugyanezzel a hardverrel „finomabb" hangjelzést is generálhatunk.

4. A KÍSÉRLETI ESZKÖZ

Az előző két fejezetben elemeztük a vakok számára készülő tájékozódó eszköz bemeneti és kimeneti részét. Most arról lesz szó, hogy milyen elektronikai és szerkezeti konstrukciót választottunk az adott feladat megvalósítására.

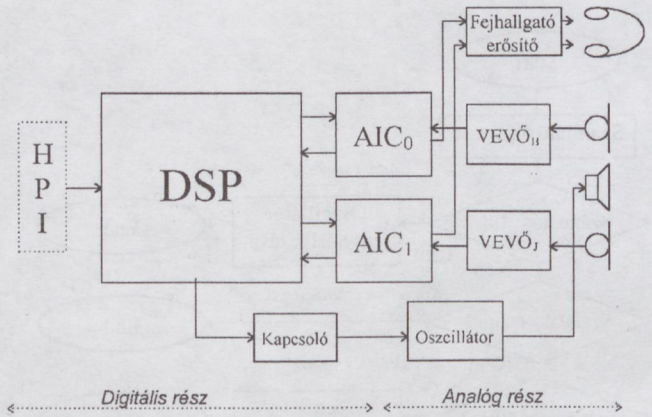
Az eszköz a Texas Instruments által gyártott TMS 320 C542-es jelprocesszorra épül [9], amely egy közepes teljesítményű (40 MIPS), 16 bites fixpontos típus. A DSP-t egyelőre nem különálló alkatrészként használtuk fel, hanem egy Starter Kit-nek nevezett egységben [10], amely egy – a gyártó által kifejlesztett – egydimenziós jelfeldolgozásra alkalmas eszköz. Ezt bővítettük különböző digitális és analóg áramkörökkel, valamint az elektro-akusztikus átalakítást végző ultrahang adó/vevőkkel. Az ultrahang átalakítók külön vannak elhelyezve a jelfeldolgozó egységtől, ugyanis ezeknek a fejjel együtt kell mozogniuk (szemüvegen, fejpánton vagy sapkán lehetnek), különben a hallgató összezavarodik amiatt, hogy az akadály-detektálás és visszajelzés nem a fejéhez rögzített koordinátarendszerben történik.

A készülék végleges kivitelét egy „walkman" küllemű doboz formában képzeljük el, amelyhez vékony kábellel lennének illesztve a szemüvegen elhelyezkedő könnyű ultrahang átalakítók és fülhallgatók.

4.1. A hardver

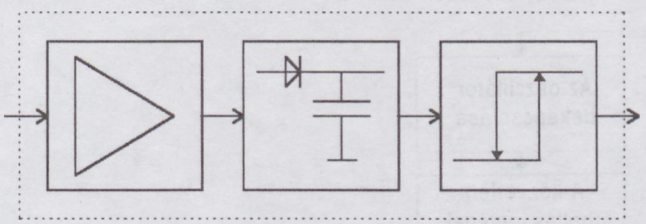
A tervezés során az jelentette a legnagyobb nehézséget, hogy esetlegesen nagyon kis szintű jelek (néhányszor 10 V) megjelenésének idejét nagy pontossággal kell mérni (100 s nagyságrendben). Ezért az analóg részt és ennek a digitális áramkörökkel való kapcsolatát nagyon gondosan kellett tervezni és megvalósítani. Külön szempont volt – a készülék hordozhatósága érdekében –, hogy egyetlen tápfeszültségről működjön minden, valamint, hogy ne használjunk speciális, drága alkatrészeket.

A készülék egyszerűsített blokkvázlata a 9. ábrán látható.



9. ábra. A hardver egyszerűsített blokkvázlata

- A DSP végzi a mérés vezérlését (az oszcillátor ki-be kapcsolása, a vett jelek feldolgozása), az eredmények kiértékelését és a tájékoztató hangjelzés mintáinak előállítását. A DSP-n 'on-chip' 10 kszó RAM van, ezt külön nem jelöltük. A PC-n megírt DSP assembly programot a Host Port Interface-en (HPI-n) keresztül lehet letölteni a memóriába, a HPI-nek a továbbiakban nincs szerepe. Az analóg illesztő áramkörök (AIC-k) [8] az időosztásos soros porton érhetők el, az analóg oszcillátor kapcsolgatása pedig egy címvezetéken keresztül történik.
- Az AIC-k funkcionálisan egyenrangúak, logikailag 'master-slave' elven vannak összekapcsolva. Egy AIC tulajdonképpen egy 14 bites A/D és D/A konverterből áll, amelynek a bemeneti és kimeneti szűrője, valamint a mintavételi frekvenciája programozható. Mivel a D/A átalakító maximális mintavételi frekvenciája 25 kHz, ultrahang közvetlenül nem állítható elő vele. Az AIC-k analóg bemenetére a demodulálást végző vevőáramkörökből jövő jel jut, az analóg kimenetükről pedig a fejhallgatóra kerül a hangjelzés.
- Az oszcillátor egy egyszerű időzítő-áramkörrel megvalósított astabil multivibrátor, és 40 kHz-es négyszögjelet állít elő. (Az ultrahang adó nem igényel szinuszos jelet.)
- A vevőáramkörök további részblokkokra bonthatók (10. ábra).



10. ábra. A vevőáramkör blokkvázlata

A bemeneten egy nagyerősítésű fokozat található, ez három szelektív, műveleti erősítővel felépített áramkör soros kapcsolásából áll. ($A_{max} = 50.000$, így kb. 100 μV is teljesen kivezérli a kapcsolást.) A tápfeszültség többszörösen van szűrve az áramkör zavarvédelmének fokozására.

- Ezután egy csúcsérték-egyenirányító (burkoló-demodulátor) következik. Erre azért van szükség, mert az A/D konverter maximális mintavételi frekvenciája 43.2 kHz, így a 40 kHz-es ultrahang nem dolgozható fel vele közvetlenül.
  Végül egy hiszterézises komparátor következik. Ezt nyilván fölösleges alkalmazni, ha utána A/D átalakítóra kerül a jel, de szeretnénk a jövőben ugyanezzel a vevőáramkörrel, de A/D konverter nélkül megoldani a vett jel detektálását, hogy minél olcsóbb legyen a készülék.
- Az ultrahang adó és a vevők (transducerek) „piezo-elven" működnek, 40 kHz-re vannak optimalizálva. A kicsi, 10 mm átmérőjű plasztik tokozás lehetővé teszi, hogy a felhasználót nem zavaró módon rögzítsük őket, pl. szemüvegszáron. A frekvencia kiválasztásánál több szempontot kellett figyelembe vennünk: minél nagyobb a frekvencia, annál jobban nyelődnek el a hanghullámok, viszont minél kisebb a frekvencia, annál nagyobb szögtartományban ad az adó (és érzékel a vevő). Ez az alsóbb frekvenciák javára tolta el a döntést, de azt is figyelembe kellett venni, hogy a vakvezető kutyákat a túl alacsony ultrahang zavarná. Így a 40 kHz mellett döntöttünk (ebben az is megerősített minket, hogy csak ilyen frekvenciájú típusok vannak közforgalomban...).
- A fejhallgató erősítő impedanciaillesztést végez, valamint a hangerő manuális állítását is lehetővé teszi. (Erre feltétlenül szükség van, hiszen a külső zaj szintje széles határok között változhat).

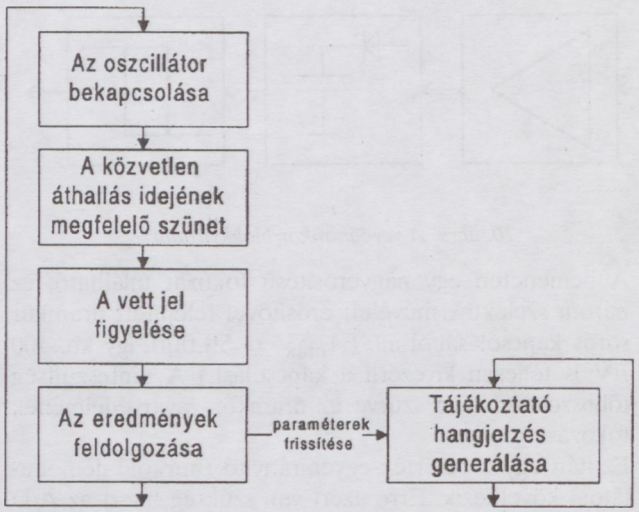
4.2. Az eszköz működése

A működés egyszerűsített folyamatábrája a 10. ábrán látható. Az ábrán a baloldali ciklus 40 ms ideig tart, a jobboldali pedig mintavételenként ismétlődik.

Az egyes részletekkel már foglalkoztunk (akadálylokalizáció, sztereó visszajelzés, hardver leírása), csak a szoftver blokkvázlat szintű ismertetése van hátra.

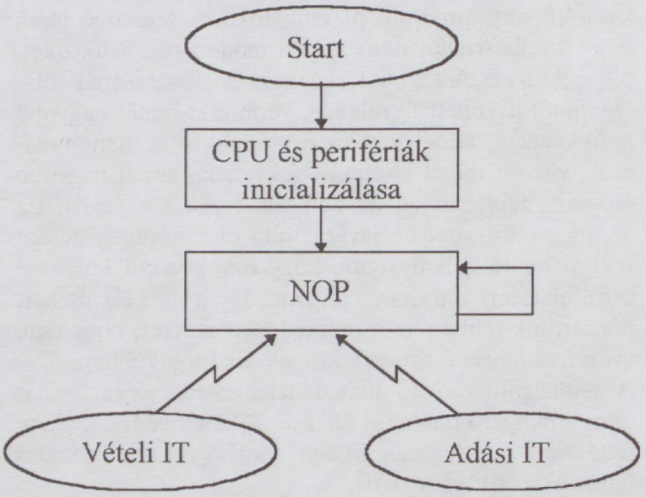
4.3.1. A szoftver általános felépítése

A főprogram szerkezete nagyon egyszerű, egy egyszer végrehajtódó inicializálási részből és egy (üres) végtelen ciklussal megvalósított várakozási részből áll. Az üzem közben rendszeresen jövő, pontosan időzített megszakítások a megszakításkezelő rutinoknak adják át a vezérlést, a működtető program lényegi része (mérés-vezérlés, sztereó visszajelzés) ezekben van.



11. ábra. Az eszköz működésének egyszerűsített folyamatábrája

A megszakításokat egymáshoz szinkronizáltan az analóg illesztő áramkörök adják, a DSP időosztásos soros portján ekkor fizikai adatátvitel is történik. A vételi megszakítás (Rec. IT) esetén a vevő felől jövő digitalizált minta továbbítódik a DSP-nek, adási megszakítás (Transmit IT) esetén pedig az analóggá konvertálandó minta kerül a megfelelő AIC-hez. Mindkét AIC-től jön adási és vételi IT, és szoftveresen állapítható meg, hogy a master-től vagy a slave-től jött-e.



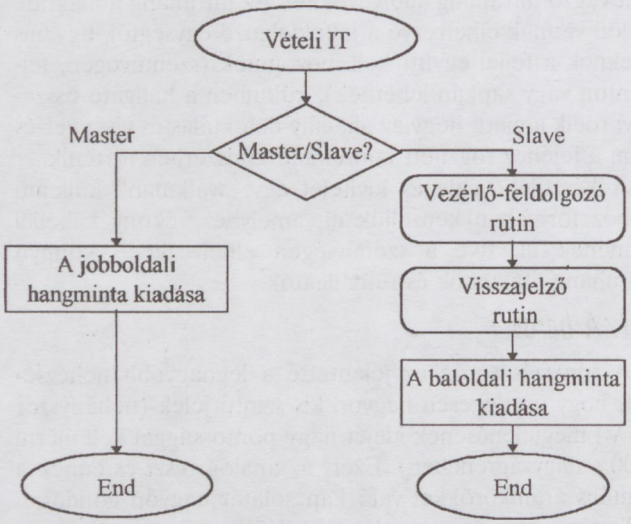
12. ábra. A működtető program általános felépítése

A DSP számítási kapacitását a jelenlegi programmal távolról sem használjuk ki, így a slave AIC vételi megszakításkezelő rutinja elegendő az összes számítás elvégzéséhez. Az adási rutinok üresek, a master AIC vételi rutinja pedig csak néhány értékadó utasítást tartalmaz.

A lényegi program tehát két fő részből áll:

- vezérlő-feldolgozó rutin,
- visszajelző rutin.

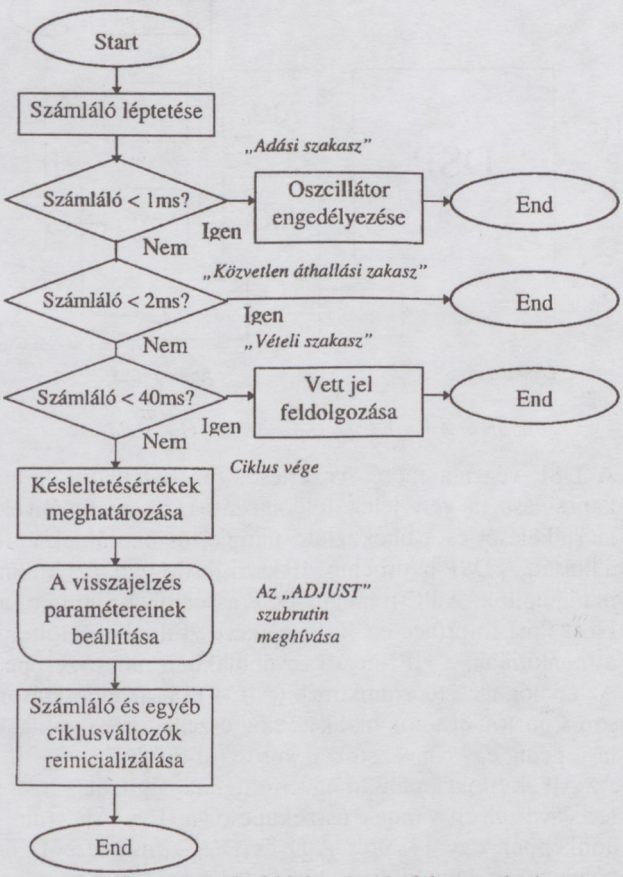
A két alprogram egymástól lényegében függetlenül, aszinkron módon fut. Az egyetlen kapcsolatuk, hogy az első 40 ms-onként frissíti a visszajelzés paramétereit.



13. ábra. A vételi megszakítás kezelőrutinjának egyszerűsített folyamatábrája

4.3.2. A vezérlő-feldolgozó rutin

Itt történik az akadálylokalizációs mérés vezérlése, az adatok feldolgozása, és a paraméterek beállítása a visszajelzés számára (14. ábra).



14. ábra. A vezérlő-feldolgozó rutin folyamatábrája

Az „adjust" szubrutin logikailag a visszajelzéshez tartozik, de itt kell meghívni, hogy a mérési eredmények mihamarabb érvényre jussanak. Benne a 3.3. pontban elmondottak szerint történik a beérkezési idők/frekvencia, szünethossz, ITD, ILD leképezés.

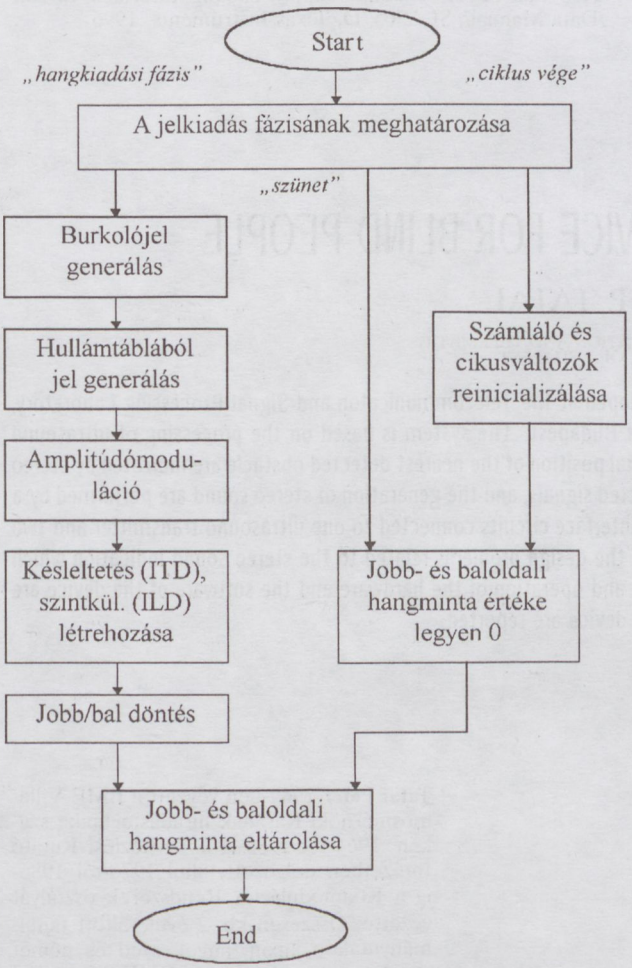
4.3.3. A visszajelző rutin

A visszajelző rutinban a sztereó tájékoztató hang generálása történik. A két csatorna hangmintáit nem külön algoritmus állítja elő, hanem a visszajelzés soronkövetkező mintájának előállítása után azt eltároljuk, majd létrehozzuk az időkésést és a szintkülönbséget, így kapjuk meg a második csatorna hangját. Ezután döntjük el melyik csatorna jelét adjuk a bal- és melyikét a jobboldali fülhallgatóra.

5. ELŐZETES KÍSÉRLETI EREDMÉNYEK

Mint már több helyen is említettük, a készüléknek még csak a kísérleti verziója készült el, egészen pontosan fogalmazva, a harmadik kísérleti verziónál járunk. Az első változat csupán távolságmérésre volt alkalmas, a második pedig majdnem megegyezik a mostanival, az analóg részével és a helymeghatározás módszerével voltak problémák, ezeken kellett változtatni.

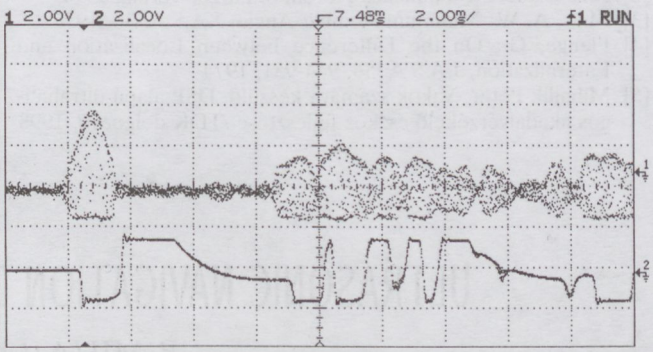
Az ultrahangos helymeghatározáshoz fizikai kísérleteteket végeztünk (részletek a [6]-ban), és a visszajelzést is többrétű pszichoakusztikai kísérletek alapján terveztük meg (bővebb leírás az [5]-ben).



15. ábra. A visszajelző rutin folyamatábrája

Magával az eszközzel végzett „igazi" kísérleti eredményeket azért nem tudunk még felmutatni, mert a cikkben ismertetett készülék összeszerelését még nem fejeztük be, a többi pedig csak korlátozottan működőképes. Ezért az előző verzióval készült „előzetes" kísérleti tapasztalatokat összegezzük:

- *Általános tapasztalatok:*
  (Néhány, a készüléket kipróbáló érdeklődő hallgató véleményének összefoglalása.)
- Közeli tárgyak távolságát és irányát az eszköz jól jelzi.
- Távolabbi akadályoknál csak az érzékenyebb oldal észlelte a bejövő jelet, így csak a távolságérzékelés működött. Közepes távolságban lévő, de nagyon „szélen lévő" tárgyakat sokszor szintén csak az egyik oldal érzékelte.
- „Befogott" tárgyak esetén a hallgatók nagyobb része egyértelműen érezte az irányt, kisebb része bizonytalan volt, ha az akadály közelítőleg szemben helyezkedett el.
- A legkisebb visszajelzett távolságváltozás nem mindenki számára érzékelhető („negyedhang" hangmagasság változás), a nagyobb és gyorsabb elmozdulás azonban a tájékoztató hang alapján igen jól kivehető volt.
- *Reflexiós képek:*
  Az eszköz érzékenysége nem a szükségesnek megfelelő, de az ultrahangos helymeghatározás működik. A 16. ábrán látható szemléltetésül egy visszaverődési kép, mely a Távközlési Labor egy részletét „ábrázolja".



16. ábra. Valós környezetben felvett visszaverődési kép. (1. csatorna: az ultrahang vevő felerősített jele; 2. csatorna: a feldolgozott jel.)

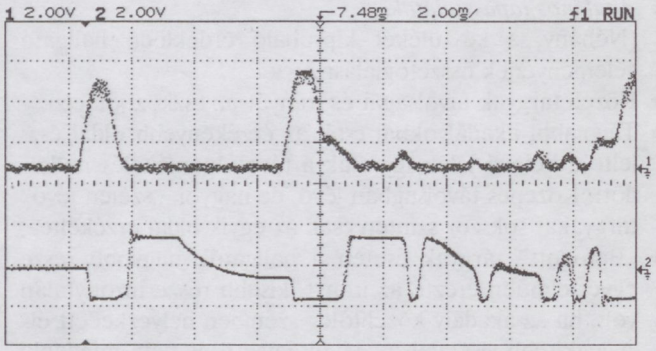
Az oszcilloszkóp 1-es csatornáján az ultrahang vevő által érzékelt jel felerősítve látható, a 2-es csatornára pedig a már feldolgozott, az A/D konverter bemenetére kerülő jelet kapcsoltuk. (Ehhez a ponthoz közvetlenül nem fértünk hozzá, így a mérés céljából a beolvasott jelet visszaalakítottuk analóggá, és valójában a D/A átalakító kimenetét mértük. Ez okozza a jól kivehető késleltetést a két csatorna jele között.) A képernyő baloldalán jól látható a közvetlen áthallásból eredő impulzus, később pedig a különböző távolságban elhelyezkedő tárgyakról visszaverődő reflektált hullámcsomagok.

A kép alapján érthető, miért elégszünk meg egyelőre a legközelebbi akadály detektálásával. Az egyenirányítás (burkoló-demodulálás) után egy felületeresztő jellegű szűrőn is átmegy a jel (negatív deriváló hatás), ezért kapjuk a 2-es csatornán lévő jelformát. A legközelebb lévő tárgyat egyértelműen jelzi a jel negatív éle, ezt a hirtelen változást jól lehet a szoftverrel detektálni, így ezt tekintjük a reflektált hullám megérkezési időpillanatának.

Az adott oldali visszaérkezési idő kb. 2,4 x 2 ms = 4,8

ms (kb. 80 cm-re van a tárgy). A másik oldalon ugyanígy megmért visszaérkezési idő alapján a már ismertetett módon történik a távolság és az irány meghatározása.

A 17. ábrán egy másik visszaverődési kép látható, ahol az 1-es csatornára az egyenirányított (demodulált) jelet kapcsoltuk.



17. ábra. Másik példa valós visszaverődési képre. (1. csatorna: az ultrahang vevő felerősített és demodulált jele; 2. csatorna: a feldolgozott jel.)

IRODALOMJEGYZÉK

[1] Tarnóczy Tamás: Zenei akusztika, Zeneműkiadó, 1982
[2] Jens Blauert: Räumliches Hören, S. Hirzel Verlag, 1974
[3] Mills, A. W.: Minimum Audible Angle, J.A.S.A. 30, 1958
[4] Plenge, G.: On the Difference between Localization and Lateralization, J.A.S.A. 56, 944-951, 1974
[5] Mihajlik Péter: Vakok számára készülő, DSP alapú ultrahangos akadályérzékelő eszköz fejlesztése /TDK dolgozat/, 1998

Szeretnénk hangsúlyozni, hogy ezek csak előzetes tapasztalatok az eszköz előző verziójával. A cikk írásának idején a javított verzió analóg része elkészült, és a tesztelés alapján az érzékenysége a tervezettnek megfelelő.

6. ÖSSZEFOGLALÁS

Beszámoltunk egy készülékről, amely jelentős segítséget nyújthat a vakok számára a tájékozódásban. Az eszköz érzékeli a használója előtt lévő tárgyakat, és a legközelebbi akadály kétdimenziós helyéről sztereó hang visszajelzést ad. Az akadálydetekció ultrahang segítségével történik, a mérés vezérlését, kiértékelését, valamint a tájékoztató hangjelzés előállítását digitális jelprocesszor végzi. A készülék 5 V-os akkumulátorról üzemeltethető, kísérleti formájában is kisméretű; az ultrahang átalakítók külön szemüvegre, vagy sapkára szerelhetők. Az eszközt egy olyan kiegészítőnek szánjuk, amely a vak felhasználónak a saját érzékszervein keresztüli tájékozódását teszi lehetővé.

Szeretnénk köszönetet mondani dr. Osváth Lászlónak, Ambrus Sándornak, Doka Gyulának, Molnár Istvánnak és Sachs Tamásnak.

[6] Doka Gyula, Molnár István, Sachs Tamás: DSP alapú ultrahangos akadályérzékelő vakok részére, 1997
[7] TMS 320 C54x DSP, 1994
[8] TLC 320 AC01 C Single-Supply Analog Interface Circuit /Data Manual/, SLAS057D, Texas Instruments, 1996

ULTRASONIC NAVIGATION DEVICE FOR BLIND PEOPLE

P. MIHAJLIK, P. TATAI

DEPARTMENT OF TELECOMMUNICATION AND TELEMATICS
TECHNICAL UNIVERSITY OF BUDAPEST

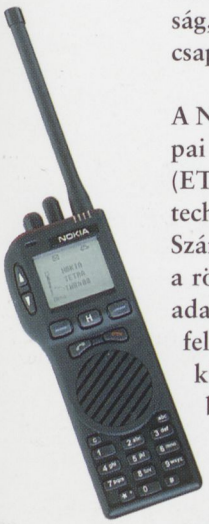
The paper describes a navigation aid for blind people which has been developed at the Telecommunicaton and Signal Processing Laboratory, Department of Telecommunication and Telematics, Technical University of Budapest. The system is based on the processing of ultrasound reflected from the objects in front of the user. The distance and the horizontal position of the nearest detected obstacle are indicated by stereo sound effects. The control of distance measurement, the processing of reflected signals, and the generation of stereo sound are performed by a fixed point digital signal processor (TMS320C542) equipped with suitable interface circuits connected to one ultrasound transmitter and two receivers. The paper discusses the applied echolocation method, as well as the design problems related to the stereo sound indication which is based on the characteristics of human spatial hearing. Also the structure and operation of the hardware and the software of the device are briefly introduced. Finally, some measurement results with an experimental device are reported.

Mihajlik Péter a BME Villamosmérnöki és Informatikai Karának ötödéves villamosmérnök hallgatója. Az 1998-as Kari TDK konferencián 2. helyezést ért el „Vakok számára készülő, DSP alapú ultrahangos akadályérzékelő eszköz fejlesztése" című dolgozatával.

Tatai Péter 1964-ben végzett a BME Villamosmérnöki Karának híradástechnika szakán. 1964-től 1986-ig a Távközlési Kutató Intézetben dolgozott, ahol 1976-tól 1986-ig a Kódmodulációs Rendszerek osztályát vezette. Összesen kb. 2 évet töltött tanulmányutakon japán, angol, svéd és német egyetemeken. 1986 óta a BME Távközlési és Telematikai Tanszékén dolgozik. Több, mint 60 publikációja jelent meg.

A kezében van a helyzet megoldása

Az új Nokia TETRA professzionális mobil rádió megsokszorozza a gyorsaság, a higgadtság, a döntésképesség, a csapatmunka erejét.

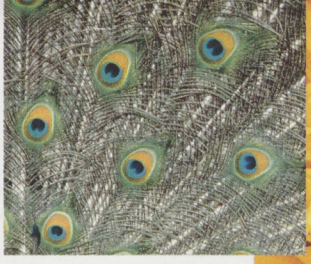


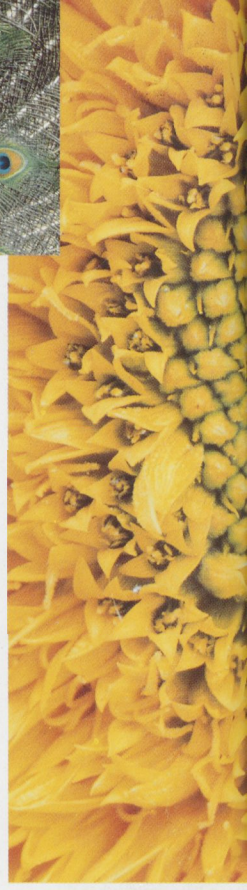
A Nokia TETRA rendelkezik az Európai Távközlési Szabványügyi Intézet (ETSI) által specifikált új digitális technológia minden lényeges elemével. Számos helyzetben jó szolgálatot tesz a rövid hívásfelépülési idő, a hang- és adatátviteli lehetőség, a megosztható felhasználás, a hatékony frekvenciakihasználás, a prioritási szintek beállításának lehetősége.

A Nokia a teljes rendszerek szállítása és a rádiós berendezések területén szerzett rendkívüli tapasztalatával és nemzetközi ügyfélszolgálati hálózatával segíti az Ön munkáját.

Nokia TETRA. Megbízható technológia egy megbízható cégtől.

NOKIA
CONNECTING PEOPLE





A Nokia nagy kapacitású GSM rendszere

A GSM mobiltelefonok területén robbanásszerű fejlődés ment végbe. Mára több, mint 100 millió ember használ GSM készüléket, 2005-re pedig számuk meghaladja az 1 milliárdot.

GSM - a legelterjedtebb telefon

A szolgáltatók bevételüket nem pusztán előfizetőik számának növelésével, hanem a telefonok használatának fejlesztésével tudják növelni. A mobil készülék nélkülözhetetlen elemévé válik életünknek és az emberek egyre többet telefonálnak - utazás közben, otthon, az irodában - tehát állandóan.

Emellett megjelennek a színen az olyan vezetéknélküli adatátviteli szolgáltatások is, mint az elektronikus posta (E-mail) és a GSM-távirat (SMS). Az adatátviteli kínálatot olyan szolgáltatások bővítik, mint a HSCSD és a WAP. A GPRS technológia bevezetésével pedig egy teljességgel új korszak kezdődik a vezetéknélküli adatátviteli felhasználói szokások területén.

A szolgáltatók üzleti tevékenysége bővülni fog - feltéve, hogy szolgáltatásaikat megfizethető áron tudják kínálni és rendelkeznek az igények kielégítéséhez szükséges hálózati kapacitással. A Nokia nagy kapacitású GSM rendszer bevezetése azt jelenti, hogy a GSM kapacitása új szintre emelkedhet, miközben a szolgáltatók csökkenthetik a hálózataik üzemeltetése során felmerülő költségeket.

Tízszeres kapacitás féláron

Az új Nokia MetroSite használatával a szolgáltatók tízszeres kapacitást építhetnek ki, összehasonlítva a hagyományos makrocellás hálózatokkal. Ráadásul, mindez fele annyiba kerül, mint a versenytársat jelentő mikrocellás rendszer.

A Nokia MetroSite megoldás csökkenti a bázisállomás telepítési költségeit és időtartamát is. A megoldás részeként kínált innovatív, az 58 GHz-es frekvenciasávon működő hozzáférési átviteltechnikai rendszer teljességgel új telephely-kiépítési gyakorlatot tesz lehetővé. Az összeköttetés azonnal megteremthető, közvetlenül a berendezések telepítése után.

Kétszeres kapcsoló központi teljesítmény

A Nokia DX 200-as mobil központ termékcsalád legújabb tagja, a DX 200i-sorozat feldolgozási teljesítménye több, mint kétszerese a korábbi termékeknek, miközben mérete csökkent. Az MCSi akár 400 ezer előfizetőt is képes kezelni, még azt feltételezve is, hogy minden, a hálózatban létrejövő hívás intelligens hálózati szolgáltatást is igényel. A hálózati elemek számának minimálisra csökkentése révén a DX 200i sorozat jelentős megtakarításokat eredményezhet a szolgáltatóknak.

A Nokia DX 200i sorozat teljeskörűen kompatíbilis a korábbi DX 200-as mobil központokkal - ezért zökkenőmentesen beilleszthetők a már meglévő hálózatokba. A szolgáltatók azonos szolgáltatásokat nyújthatnak hálózatukon belül mindenhol és maximalizálhatják a befektetéseik hasznos élettartamát.

Bizonyos hálózatok egyszerűen jobban működnek

A Nokia új, költséghatékony berendezéseinek köszönhetően a szolgáltatók tovább csökkenthetik üzemeltetési költségeiket. A hálózat gyors kiépítése és üzembe helyezése céljából a Nokia hatékonyabb telepítési és üzemeltetési folyamatokat dolgozott ki.

A tervezési szolgáltatások a legjobb mikrocellás, kapcsolóközponti és átviteltechnikai megoldásokon alapulnak. A Nokia ügyfelei rendelkezésére áll a meglévő hálózatok átalakítása és optimalizálása során is.

A Nokia által kínált integrált hálózattervezési, adattárolási, valamint távvezérelt letöltést lehetővé tevő eszközök segítik a szolgáltatókat a gyorsan fejlődő hálózat irányításában, miközben még a legösszetettebb, legnagyobb kapacitású GSM hálózatban is magasabb hatékonyságot érhetnek el.

A Nokia új, nagy kapacitású rendszere természetesen minden GSM sávban, vagyis 900 és 1800 MHz frekvencián is a szolgáltatók rendelkezésére áll.

Hozzon ki többet GSM hálózatából!

NOKIA
CONNECTING PEOPLE