International Journal of Advances in Telecommunications Electrotechnics, Signals and Systems

a publication of the International Science and Engineering Society

Vol. 1, No. 1
2012

ISSN: 1805-5443

www.ijates.org

I J A T E S²

International Journal of Advances in Telecommunications Electrotechnics, Signals and Systems

a publication of the International Science and Engineering Society

Vol. 1, No. 1, 2012 ISSN: 1805-5443

Aims and Scope

The International Journal of Advances in Telecommunications, Electronics, Signals and Systems (IJATES²) is an all-electronic international scientific journal with the aim to bring the most recent and unpublished research and development results in the area of electronics to the scientific and technical societies, and is supported by the ISES (International Science and Engineering Society, o.s.). The journal's scope covers all the aspects of telecommunication, signal processing, theory and design of circuits and systems for electronics.

The IJATES² is ready to publish experimental and theoretical full papers and letters submitted by prospective authors. Paper submitted for publication must be written in English and must follow a prescribed format. All papers are subjected to a critical peer-review prior to publication.

The IJATES² is an open access journal which means that all content is freely available without charge to the user or his/her institution. Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the articles in this journal without asking prior permission from the publisher or the author. This journal provides immediate open access to its content on the principle that making research freely available to the public supports a greater global exchange of knowledge.

www.ijates.org

CONTENTS

Vol. 1, No. 1, 2012 **ISSN: 1805-5443**

The Possibilities of Data Communication for Telemetry Systems in Energetics

Jiri Misurec

***Abstract*—The paper describes the possibilities of communication lines for automated data collection from any energy meter installed on the client's side. There are compared some types of communicatin lines, classical modem communication over PSTN, TCP/IP communication over Internet and PLC (Power Line Communication) - communication over power electrical distribution chain. The main focus is presented to PLC system. The remote data acquisition is modern trend for metering of energy, gas, water, heating steam etc.**

***Keywords*—PLC, data aquisition, communication, power lines, energetics**

I. Introduction

Today, many electricity distribution companies try to find efficicient ways to gather information regarding clients' energy take-off. The old-style method when a qualified person knocks at your door and asks for the relevant information seems to be outworm. This significant move towards automated data collection opens new doors for telecommunication companies and organizations. A lot has been written about data capture using classical telephone lines, xDSL and wireless technologies. The latest development in the field of Power Line Communication (PLC) allows us to use Power Line technologies (PLT) to transmit the relevant data from a client to the distributor's data access point and further on through the distribution network [4] [5]. The first chapters provide a brief overview of the available Power Line technologies, summarizing advantages and disadvantages as well as the implementation areas. Later chapters will try to analyze PLT and draw the scheme for automated energy data capture. Energy measurement devices represent highly sensitive information source most often installed on the clients' side of the electrical distribution chain. The implementation of an encryption standard on the entire data exchange network is an extremely critical and complex task. We avoid describing the higher level securing methods and concentrate on lower level implementations instead. Out of many available encryption standards we picked AES system.

II. The comparision of technologies for remote data acquisition

Recently, it is mainly telephone network (PSTN), dedicated industrial lines and GSM that is used for remote data acquisition. Pilot projects are focused on possibilities of the internet utilization, GSM GPRS and PLC utilization. However, this technology brings along plenty of new problems, mainly from the point of view of the data transmission security and the communication reach. We also know other technologies designed particularly for acquisition of data via mobile data stations. Emphasis is placed on transmission reliability and data security. The speed of the data transmission is not so important. Nowadays, common data transmission speed is about 9600 kbps and its increasing is not the main problem. The comparison of available communication technology can be seen in TABLE I.

Jiri Misurec is with Dept. of Telecommunications, Faculty of Electrical Engineering and Communication, Brno University of Technology,Purkynova 118, 612 00 Brno, Czech Republic, mail: misurec@feec.vutbr.cz .

Manuscript received June 25, 2012, accepted July 12, 2012

III. Overview of Power Line Communication

Power Line Communication is a general term used for describing communication over common power lines. Energy distrubution net represents the densest network in every country, where each building has a power line connection and a power line termination - electrical plug - is present in every room. It is obvious that use of the power line net as a data communication medium, is a very resourceful idea. At the latest stage, each device plugged into an electrical plug would be able to use the Internet services. Making of Power Line a suitable communication medium, however, opens some new issues:

- Power line medium is not suitable for high frequency signals. It actually introduces high attenuation and noise to the signal (e.g. pulse interference from motors or SMPS sources). The existing EU laws enable the usage of a frequency range from 3 kHz to 148.5 kHz for PLC transmissions[10].
- The topology is still not determined.
- Since devices are being plugged and unplugged from the electrical network randomly, the line impedance is strongly dependable on frequency and time.
- Power lines serve as antennas and they introduces harmful interference to the neighborhood.
- Transformers block the communication across Low- Voltage (LV) and Medium-Voltage (MV) network.
- The data sent from one point of the local LV network are present at all the other points, what is connected with a high security risk.

There seem to be no PLC standardization for all the implementation platforms, but some separate standards for industry and home usage exist.

A. EIA-709 Specification

The EIA-709 was originally proposed by Echelon LonWorks and standardized by EIA (Electronic Industries Association) as the protocol specification EIA/CEA 709.1-B-2002. The specification is available for purchase only. The

TABLE I
COMPARISON OF AVAILABLE COMMUNICATION TECHNOLOGY

Technology	positive	negative
GSM	- signal coverage in habitation area - solidity b	- price - more providers - poor signal coverage in non habitation area
Wi-fi	- non licence range - price	- radio interference - attenuation
Satellite comm.	- excellent signal coverage - excellent rate	- single way comm. - price
Laser comm.	- excellent rate - solidity	- direct visible of terminal unit
Dial-up	- availability - price	- obsolete - rate
ISDN	- digital comm. line	- rate
ADSL	- rate - price	- rate depend on distance
Structured wiring network	- rate - availability	- installation complexity
Optical fibre	- excellent rate - solidity	- price
Power line network	- pre-existent comm. line - rate up to 200Mbps	- interference - power line is not dedicated for data comm.

TABLE II
FREQUENCY RANGES FOR POWER LINE SIGNALING IN EUROPE

Band	Frequency range [kHz]	Application
A	9 - 95	Electricity suppliers
B	95 - 125	Consumer use without protocols
C	125 - 140	Consumer use with the CENELEC protocol
D	140 - 148,5	Consumer use without protocols
-	¿ 148,5	Prohibited

Echelon transceivers PL31xx [2] work in band A and C (see TABLE II for bands in Europe) in the double carrier mode with primary carrier at 86 kHz and 132 kHz respectively. Echelon guarantees data transfer rate 5.4 kbps (using BPSK) in band C up to distance of 1.5 km. Another transceivers work in band A with spread spectrum and data transfer rate 2 kbps. Transceivers PL31xx use narrow-band technology with digital signal processing to correct impulsive and continuous tone noise, phase distortion, etc. For error correction it uses patented low overhead FEC (Forward Error Correction) and classical CRC. LonWorks protocol uses all the seven layers of the OSI/ISO model. Three 8bit Neuron processors are the core of all the transceivers. They process MAC, network and application layer data. Additionally the receivers are consumer programmable using NodeBuilder Echelon's development tool. The LonWorks protocol is frequently used for capturing the energy consumption data from energy meters. Over 30000 nodes (devices, meters) can be connected to the same power line segment.

B. Topology of PLC for Energetics

The topology of data net for remote acquisition and control system via PLC is shown in 1. The data communication is possible between electricity meter and the first substation with concentrator unit of 1. level. It is acceptable communication over maximum three repeaters. This communication is on LV power line. Communication on MV power line is realized between concentrators of the first level and the second level. The conectivity to telemetering acquisition system or to control system is necessary create by another way, for example via Internet, PTSN, GSM or otherwise [11] [12].

IV. IMPLEMENTING AUTOMATED METER READING

There are three types of electrical meter reading: EMR (Electrical Meter Reading - On-Site Meter Reading), OMR (Off-Site Meter Reading) and AMR. Automated Meter Reading (AMR) [3] uses fixed telecommunication network (mobile or fixed radio, dial-in/out, PLC, broadband cable [4], Internet) to collect data. Data modem installed on the client's side sends the required information to the distrubutor's data access point or central database. The connection itself is often realized using backbone network built upon TCP/IP, telephone, ISDN or xDSL technologies. Speaking of capturing data from clients' energy meters, we need to point on the fact that not all the monitored places are connected over one of the mentioned technologies and the Power Line is the only remaining one. The actual implementation of AMR differs from manufacturer to manufacturer. One of the possible solutions is shown on 2. In this example, PLC serves as a communication medium in the access network and optionally in the distribution network. The data access point is placed in the MV/LV station. It is used to collect data from electric meters from all the connected clients. They can either have PLC installed or they can use one of the standardized protocols (Euridis, DLMS/COSEM, IEC 60870-5-102) to connect with a PLC modem. Data from the data access point can be send either via MV PLC or other communication medium (optical fiber, xDSL, PSTN, GSM) [8]. This solution is suitable for the environments,

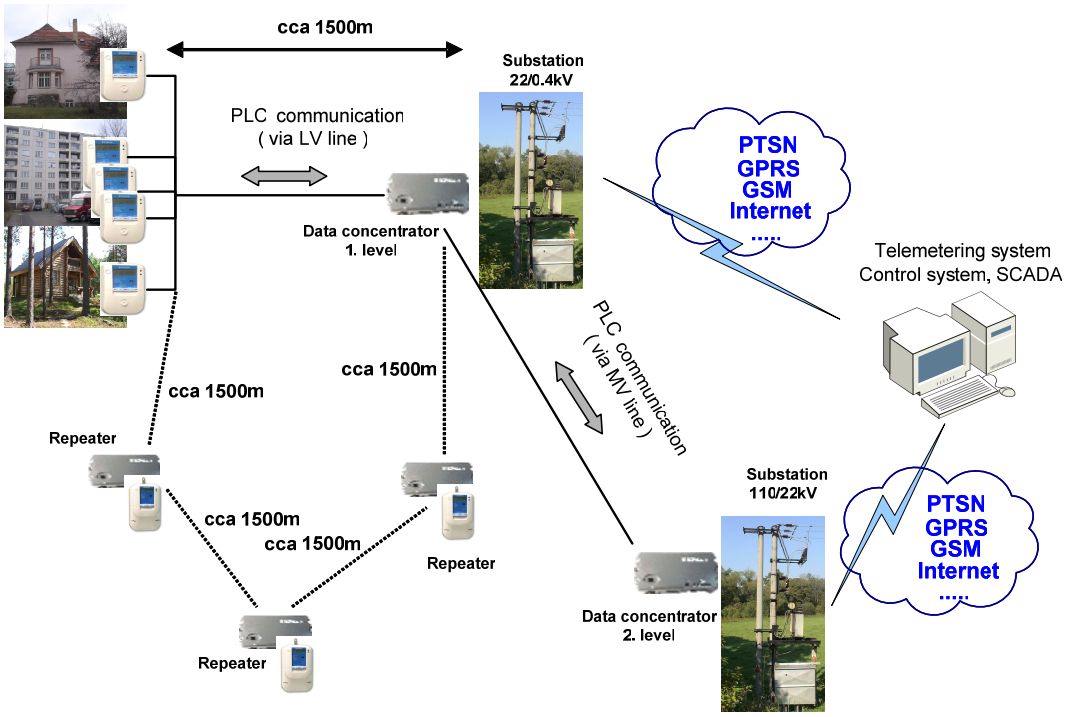


Fig. 1. System of Data Acquisition via PLC in Energetics

where it would be difficult or expensive to use other fixed communication network (PSTN, GSM) directly to the meters, e.g. villages with one MV/LV transformer have one data concentrator, which will connect to the central via PSTN, GSM or other technology and via PLC with all the electric meters.

Using PLC in the distribution network brings some issues mentioned earlier in the paper. Their elimination connected especially with the use of massive injection capacitors and additional data paths in the transformer stations may result in highly expensive solution. Data modems often represent a simple counter block with PLC output. The counter module counts the incoming impulses while the communication unit encrypts and sends the data over a PLC line to the first data access point. This structure allows the devices to be used for counting of variety input pulse signals from e-meters including gas meters, water meters etc. The devices are additionally often equipped with a programmable interface such as RS-232. The core of the communication modules is usually built upon a programmable Digital Signal Processor (DSP) platform since it needs to contain support for encryption standards.

V. Building Secure Path over Power Line Communication

The implementation of an encryption standard on the entire PLC network is an extremely critical task. We recommend to use advantages of a physical-layer (hardware) encryption instead of building a complex upper-level security standards. Building VPN (Virtual Private Network) and IPSec on top of TCP/IP might be seriously considered when large data fragments are to be transported over the network. Hardware implementations of cryptographic algorithms have a long history. In confrontation with software implementation, it can be of benefit for high-speed applications applications where a cryptographic co-processors perform the cryptographic operations as well as the applications where low power and low area requirements are stringent. In both cases, the secure storage of cryptographic keys is crucial. Today, the traditional algorithms such as DES and RSA are being replaced by the AES (Advanced Encryption Standard). AES is suitable for small 8-bit microprocessor platforms, common 32-bit processors, and it is appropriate for dedicated hardware implementations. Hardware implementations can reach throughput rates in the Gigabit range [9]. The algorithm can encrypt and decrypt blocks using secret keys. The key size can either be 128-bit, 192-bit, or 256-bit. The actual key size depends on the desired security level. The different versions are most often denoted as AES-128, AES- 192, or AES-256 [9].

VI. Conclusion

Remote data acquisition is burgeoning area not only in the power energetics.. The main problem is suitable transfer channel that is brought to measuring equipment. Generally, we can use different technologies. All of the technologies are still in phase of improving but the most important improvement we want to achieve is coverage of the specific area. It was proved that it is necessary to employ several technologies and use their combination. The use of the internet and PLC systems is certain alternative how to provide connection between telemetering central system and remote measuring equipment. PLC is a communication method that makes use

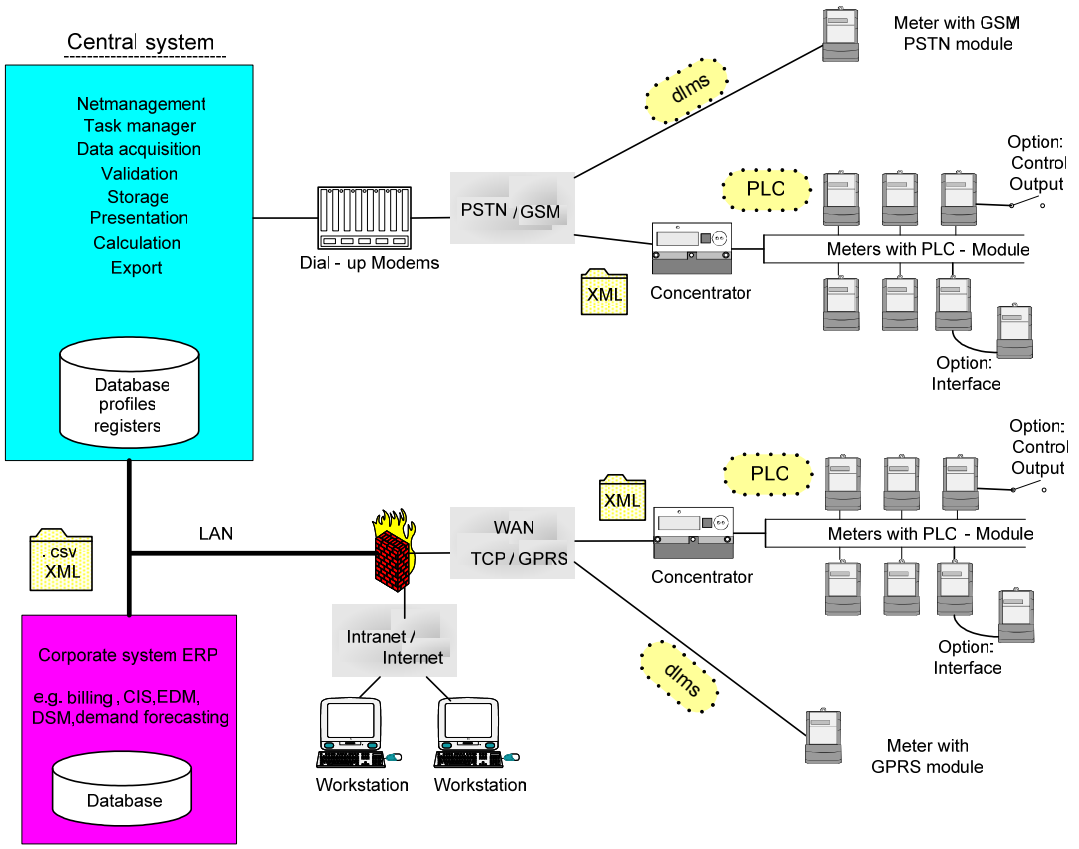


Fig. 2. Using Power Line Communication for Automated Meter Reading (AMR)

of the existing LV power lines as a communication channel. The possibility to transmit data messages with the use of the existing power lines as a communication medium has brought a new impulse to the development of applications in the field of industrial automation, integration and other communication solutions. The implementation of the PLC technology in the field of Automated Meter Reading seems to be a progressive way ahead. Nevertheless, the producers of the energy data collection devices tend to deploy their own private solution which leads into the lack of ability to communicate with devices of different origin. The AMR-PLC principal scheme for automated e-meter data collection is quite simple. On the client's side the energy measurement device is usually connected to a communication modem. Distributors access point is most often represented by a communication modem and server gathering information from all the clients. The PLC technology may be implemented in the access network. AMR represents a highly-sensitive information chain and the encryption standard is a crucial task. We strongly recommend to use existing hardware implementations of AES encryption algorithm. On a larger scale when the entire electrical distribution network must be considered we recommend to think of an upper level security management such as VPN.

REFERENCES

[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.
[2] Echelon's home page, www.echelon.com.
[3] OPERA project, "D57: Specification of Interfaces between home automation and PLC and between AMR and PLC". www.istopera.org.
[4] C.W. Gellings, K. George, "Broadband over Powerline 2004: Technology and Prospects", an EPRI White Papers.
[5] J. Ramie, "Review of FCC Report & Order 04-245 on Broadband over Power Lines (BPL)", www.conformity.com.
[6] HomePlug powerline aliance home page. www.homeplug.com.
[7] M.K. Lee, et. al., "HomePlug 1.0 Powerline Communication LANs - Protocol Description and Performance Results version 5.4", International Journal of Communication Systems 2000; 00:1-6.
[8] OPERA project, "D41: White Paper AMR". www.ist-opera.org.
[9] D.VAM.2 State of the Art in Hardware Architectures, report, IST-2002-50793231. July 2005.
[10] CENELEC, "EN50065-1, Signalling on low-voltage electrical installations in the frequency range 3 kHz to 148.5 kHz", Brussels, 1991.
[11] Mlynek, P., Koutny, M., Misurec, J. The communication unit for remote data acquisition via the Internet. In Proceedings of the 7th WSEAS International Conference on Circuits, systems, electronics, control and signal processing (CSES'08). Puerto de La Cruz, Spain: WSEAS Press, 2008. s. 168-173. ISBN: 978-960-474-035- 2.
[12] Mlynek, P., Koutny, M., Misurec, J. Modeling and evaluation of power line for smart grid communication. Przeglad Elektrotechniczny. 2011, vol. 8, pp. 228232. ISSN 0033-2097.

Mac Protocols in Mobile Ad Hoc Networks

Nermin Makhlouf and Pavel Vajsar

***Abstract*—Mobile Ad hoc NETwork (MANET) is a wireless network of mobile nodes connected by wireless link without a central control. The Medium Access Control (MAC) protocol is one of the important issues in such network, thereby the presented paper will discuss the MAC protocol used in MANET depending on IEEE 802.11 standard which known as Distributed Coordination Function (DCF).However, the limitation of MANET is that, the collision increases with the rise of nodes number. Therefore paper study the MAC protocol using directional antennas to reduce the collisions, increase the range of transmission and largely reduce the interference between the directions. However, the main problem of using directional antennas is caused by frequent node mobility. So the movement plays a vital role in wireless Ad hoc networks to predict the location of MNs.**

***Keywords*—Mobile Ad hoc network, MAC.**

I. Introduction

The popular Carrier Sense Multiple Access/Collision Detection (CSMA/CD) MAC method is used for wired network. In CSMA/CD, when a node wants to send over the network, first it sense the wire medium whether it's idle or busy. If it's idle, the node sends its data with sensing the medium continually. Otherwise, the node delays its transmission to avoid a collision with existing packets. While in the wireless networks, the signal strength is inversely proportional to the square distance from the transmitter node, thus nodes, which are out of transmitter's range, can't sense the transmitted signal causing problems as illustrated in fig.1. There are three nodes A, B, C. Node B is within the range of each nodes A and B, node C is out of the range of A. Node A wants to send to B, wherefore node A waits until the medium is idle, then A starts transmitting to B. Node C wants to send to node B while B is receiving data from A. But C can't sense the transmitted signal from A, thus C starts transmitting to B causing collision at node B. This problem is called "hidden- terminal problem". Another problem is illustrated in fig.2, there are four nodes A, B, C, D. Nodes B and C are within the range of both nodes A and D, but D is out of A's range. While node B is transmitting data to node A, node C wants transmitting data to D. But C senses the transmitted signal from A, thus C delays its transmission to D. Even through a transmission from C does not interfere with the reception at node A, this case is called "exposed terminal problem".

Nermin Makhlouf is with the Department of Telecommunications, Brno University of Technology, Czech Republic, e-mail: (xmakhl00@stud.feec.vutbr.czl).

International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems.
http://www.ijates.org/index.php/ijates

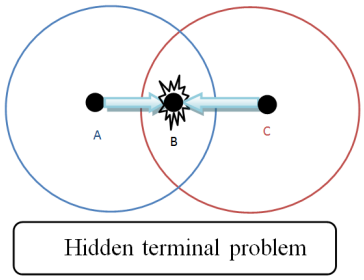


Fig. 1. Illustration of hidden terminal problem

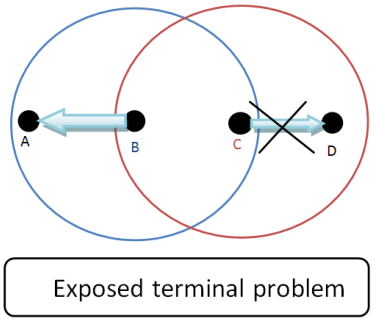


Fig. 2. Illustration of exposed terminal problem

II. Multiple Access Collision Avoidance (MACA) protocol

The Multiple Access Collision Avoidance (MACA) protocol doesn't fully solve the problem of CSMA/CD. It uses two additional packets, Request To Send "RTS" and Clear To Send "CTS", to reduce the collision at receiver. These packet are shorter than data packets, however, they contain the length of the data frame that will follow. Let us conceder an example with four nodes A, B, C, D as shown in fig.3. The node A wants to send data to the node B, so A broadcasts a RTS packet then B replay to A by sending a CTS packet. At node C the CTS packet collides with a RTS packet sent from D, so C doesn't replay to the RTS from D. But A starts sending data to B after A receives CTS from B. The node D sends another RTS packet because it didn't receive a CTS from C and then C responses to D by sending back a CTS packet which may collide with data packet at B node if the data reception isn't complete. We notice there is no acknowledge for receiving the data, thus the retransmission is started by higher layer (transport layer) [1].

The wireless LANs use the MACA protocol, but they use additional control packets like ACKnowledgement packet (ACK) which is received by the sender from the receiver node after data reception is complete. Thus, the arrangement of transmitted packets is (RTS-CTS-DS -ACK).

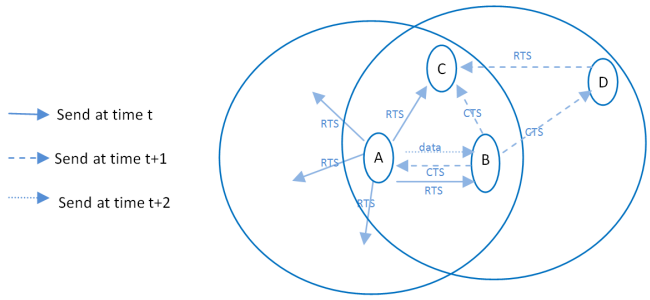


Fig. 3. Illustration of RTSCTS mechanism

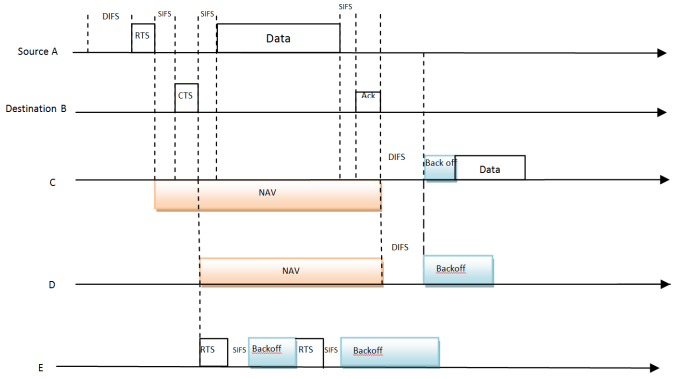


Fig. 4. CSMA/CA mechanism

III. IEEE 802.11 MAC SCHEME FOR MANET

The IEEE 802.11 standard determines DCF which is used for infrastructureless network like MANETs so we focus on DCF type. DCF is a combination of CSMA and MACA so it's called (CSMA/CA). It uses the (Data, ACK) sequence packets, but when the data packet is long it uses (RTS, CTS, Data, ACK) sequence packets. Each node has a timer called Network Allocation Vector (NAV) contains a time value. This time is the duration of the transmission to another node, as shown in fig.4, node A wants to send to node B. A senses the medium:

- If node A receives a signal weaker than a certain value called Carrier Sense Threshold (CST) for a specified time called Distributed Inter Frame Space (DIFS), the medium is idle and A broadcasts RTS packet, which includes information about the duration of the following transmission, fig.4. B receives RTS, and then if the medium is idle for a time called Short Inter Frame space (SIFS), destination B replays to A by sending CTS packet which includes the same information of duration. The other nodes, which can sense either RTS or CTS (i.e node C and D), set their NAV timer according to the duration information to prevent from access the medium as long as NAV > 0, therefore the probability of collision is decreased. When source A receives CTS packet, A starts sending data after time interval SIFS. Then if destination B receives data correctly, B sends ACK packet to A after time interval SIFS.
- If node A receives a signal stronger than CST, A senses the medium busy, A delays its transmission for time known as backoff time. The initial backoff time is chosen randomly in the range $(0, CW - 1)$, where $CW_{min} \leq CW \leq CW_{max}$ is contention window, therefore probability that two nodes choose the same value of CW is low. Then the backoff timer is decreased as long as the medium is idle, and it is stopped when the medium is busy. When the backoff timer reaches zero, the source node is allowed to send the data frame.

Fig.4 shows that node E wants to send data to D, while there is transmission between A and B. E is out of the ranges of both A and B. Wherefore E senses the medium idle for time longer than time interval DIFS. Then E sends RTS to D which isn't allowed to access medium because of NAVs CTS. E doesn't receive CTS from D after interval time SIFS, this means the medium isn't free. Therefore E chooses the backoff time randomly, in term of time slots. The backoff timer begins decreasing until it reaches zero, then D will retransmit RTS. D will double the backoff time (CW) at each retransmission depending on algorithm of Binary Exponential Backoff (BEB). But if the failure of transmission reaches to the maximum $CW_{min} = CW_{max}$, the node ignores the packet and CW will return to CW_{min}. Therefore we can notice that exposed-terminal problem isn't solved [2].

IV. DIRECTIONAL ANTENNAS IN MANET

Typically, a MANET [3] uses omnidirectional antenna, it means each node can transmit and receive signals from all directions. Using directional antennas improves the MAC protocol for MANET, where it reduces the interference between the directions because the antenna sends the most energy of signal in the right direction. And it increases the throughput and the range of transmission, and solves the exposed terminal problem [4].

A. The Node with antenna Model

It is supposed a MANET of n Mobile Nodes (MNs) [5], each MN has directional antennas with non-overlapping directions and all nodes use the same wireless channel. The antennas cover all directions (2π rad). The MN is supplied with a system for defining its position and speed, such as a Global Position System (GPS) which also provides a synchronized clock, and the MN has a Location Table (LT) in which the location information of its neighbors is stored temporarily; however, at the beginning the LT is empty. We assume an idle MN listens to the medium using all antennas; this is called Omni-Listen (OL) mode. But when a MN listens using a directional antenna, this is called Directional-Listen (DL) mode. The MNs update their Directional NAV (DNAV) when they receive either a Directional RTS (DRTS) or a Directional CTS (DCTS) packet.

1) MAC protocol using Directional antennas: A Location and Mobility Aware (LMA) MAC protocol is adapted for MANETs with directional antennas, because when there is a transmission between two nodes, the radiations of antennas have to be adjusted according to their location predictions. The

LMA MAC protocol assumes that all MNs move at constant speeds and angles during a short period of time and the style of kth content in the LT is [6]:

$$LT(k) = (Timestamp(k), NodeID(k), \quad (1)$$

$$Position(x_k, y_k), Movingangle(\alpha_k), Speed(S_k), TTL_k)$$

Where $1 \leq k \leq n, TTL_k$ is Time To Live of k^{th} content, $TTL_k = 0$ at each registration of LT(k) and then TTL_k is increased with time. When it exceed a certain threshold T, the LT(k) is deleted from the MN"s LT.

When a MN intends to start a new transmission, it uses either an Omni-listen/ Omni- RTS (OL/ ORTS) or a Directional-listen/ Directional- RTS (DL/DRTS) depending on the current information in its LT. Figs.5,6 and 7 illustrate the LMA MAC protocol where the medium is idle, node A wants to send data to B, and As LT doesnt have any information about the location of its neighbors. A sends an ORTS packet which includes location information of A: the time instant of ORTS transmission (t_k), the node ID_a, the current position $(P_A(t_r) = (x_a(t_r), y_a(t_r)))$, the moving angle (α_A) as shown in fig.7 and speed (S_A)

All As neighbors (B, C, D), which listen ORTS, will register As information in their location tables, so Bs LT, Cs LT and Ds LT will be updated as:

$$LT_B(A) = LT_C(A) = LT_D(A) = (t_r, ID_A, P_A(t_r), \quad (2)$$

$$(\alpha_A), (S_A), TTL_A)$$

Where the value of TTL_A is zero at every update of LT(A). And then destination B responses by sending a DCTS, where the direction of CTS is calculated as follow:

$$\theta(t_c) = tan^{-1} \frac{y_B(t_c) - y_A(t_c)}{x_B(t_c) - x_A(t_c)} \quad (3)$$

Where t_c is the time moment of sending DCTS from B to A, while $P_A(t_c)$ is calculated from $P_A(t_r)$ as:

$$P_A(t_c) = \begin{cases} x_A(t_c) = x_A(t_r) + S_A cos\alpha_A(t_c - t_r) \\ y_A(t_c) = y_A(t_r) + S_A cos\alpha_A(t_c - t_r) \end{cases} \quad (4)$$

The DCTS from B also includes the location information of B, thus A will update its LT as:

$$LT_A(B) = (t_c, ID_B, P_A(t_c), \alpha_B, S_B, TTL_B) \quad (5)$$

Node C receives DCTS from B, and then C updates its LT and sets its DNAV timer, thus C will not be allowed to access medium within this direction. But node C can start sending to any node which is out of DNAV range and is in the Cs LT. Now each of A and B is aware of the location of the other. The directional data transmission is started according to transmission angle θ_{data} from node A to node B where θ_{data} is computed as:

$$\theta_{data}(t_i) = tan^{-1} \frac{y_A(t_i) - y_B(t_i)}{x_A(t_i) - x_B(t_i)} \quad (6)$$

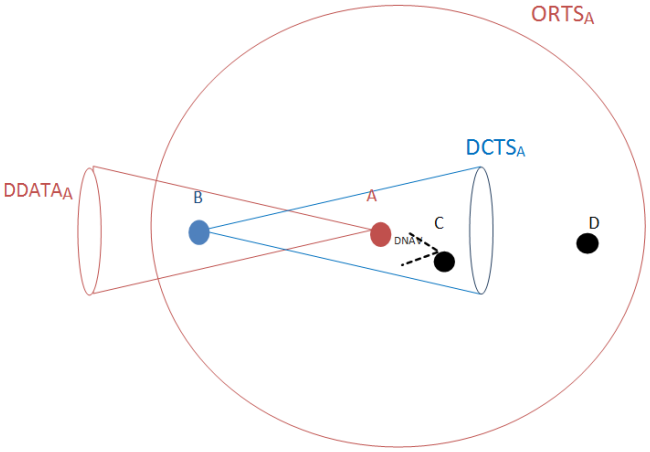


Fig. 5. MAC protocol using directional antennas the transmission direction

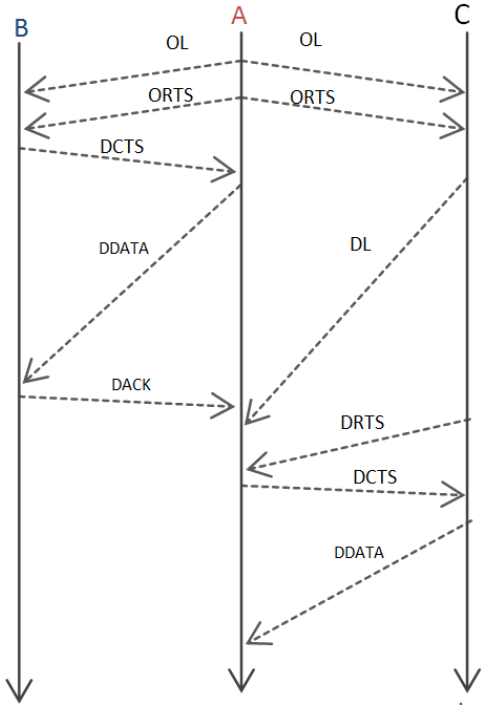


Fig. 6. MAC protocol using directional antennas the arrangement of transmission depending of the time

Where t_i ranges between the starting and the stopping time instants for data transmission, so $\theta_{data}(t_i)$ changes with time depending on MNs movement, and it can be adapted on the basis of existing antennas. The position of nodes at t_i is calculated using their LTs as:

$$P_A(t_i) = \begin{cases} x_A(t_i) = x_A(t_r) + S_A cos\alpha_A(t_i - t_r) \\ y_A(t_i) = y_A(t_r) + S_A cos\alpha_A(t_i - t_r) \end{cases} \quad (7)$$

$$P_A(t_c) = \begin{cases} x_B(t_i) = x_B(t_c) + S_B cos\alpha_B(t_i - t_c) \\ y_B(t_i) = y_B(t_c) + S_B cos\alpha_B(t_i - t_c) \end{cases} \quad (8)$$

After obtaining the transmission angle, the antenna beams of nodes A and B are pointed to the predicted direction and

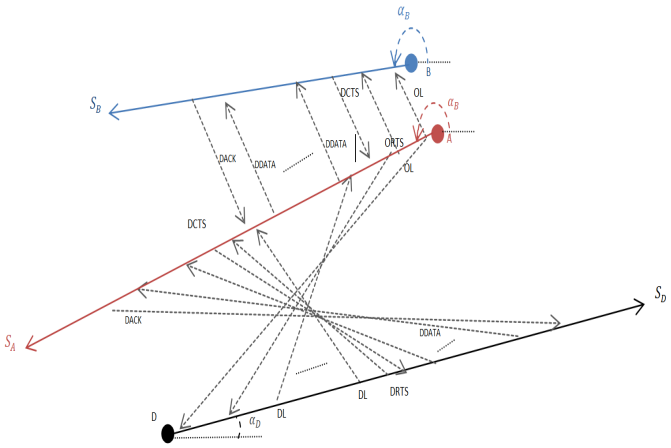


Fig. 7. The LMA MAC mechanism depending on movement direction

begin transmission. If the data transmission is completed, node B will send directionally ACK to node A. During the Transmission from node A to node B (T_{A-B}), node D may want to send data to node A, however, node D knows the As position from $ORTS_A$. Therefore node D listens to node A directionally and holds transmission medium directionally. Node D takes into account the change of As position over time to compute the current transmission angle $\theta(t)$. When transmission (T_{A-B}) is completed, node D senses medium idle using DL mode and then it sends DRTS packet to node A after the ending of backoff time, where the transmission angle for RTS is computed at the time moment of sending it (t'_r) as:

$$\theta(t'_r) = tan^{-1}\frac{y_D(t'_r) - y_A(t'_r)}{x_D(t'_r) - x_A(t'_r)} \quad (9)$$

Where $P_A(t'_r)$ is calculed from $P_A(t_r)$ as following:

$$P_A(t'_r) = \begin{cases} x_A(t'_r) = x_A(t_r) + S_A cos\alpha_A(t'_r - t_r) \\ y_A(t'_r) = y_A(t_r) + S_A cos\alpha_A(t'_r - t_r) \end{cases} \quad (10)$$

And then the transmission sequences between nodes A and D comply similarly with the previous transmission T_{A-B}. The predicted position by LMA MAC protocol could be inaccurate because the speed and moving angle during the data transmission can be changed. This protocol can be enhanced by using the Directional Beacon (DB) mechanism which makes the MNs get the update of mobility information via DB after any change of one nodes moving angle or speed. For example, when node B change its moving angle at t_m during T_{AB} the DB will distribute this modified mobility information to Bs neighbors within the transmission range (e.g., node A). Therefore node A will calculate transmission angle $\theta_{data}(t_m)$ depending on the update information.

V. Conclusion

This paper has studied the MAC protocol in MANETs and how can improve the MAC protocol by using directional antennas. The collisions among the MNs could be decreased based on the proposed LMA MAC protocol, where the MN can predict the location of its destination, and then it adjusts its antenna beam to the predicted direction of desired receiver in order to begin transmitting. Thereby the frequency reuse and the interference are enhanced. Moreover, this protocol could have more accurate of predicted location by using the DP mechanism, even if the MNs continually move during the data transmission.

References

[1] Subir Kumar Sarkar, T G Basavaraju, C Puttamadappa. *Ad Hoc Mobile Wireless Networks , Principles, Protocols, and Applications*, 1st ed. Auerbach Publications, 2008.

[2] Xin Wang, Koushik Kar. *Throughput Modelling and Fairness Issuesin CSMA/CA Based Ad-Hoc Networks.*, Proceedings of Infocom, 2005.

[3] Z. Huang and C.-C. Shen. *A comparison study of omnidirectional and directional MAC protocols for ad hoc networks*, Global Telecommunication Conference, 2002.

[4] Jin-Jia Chang, Wanjiun Liao, Jiunn-Ru Lai. *On Reservation-Based MAC Protocol for IEEE 802.11 Wireless Ad Hoc Networks With Directional Antenna*, IEEE Transactions on Vehicular Technology, 2011.

[5] P. Vajsar, J. Hosek, K. Molnar and M. Bartl. *Advanced Trajectory Management Techniques for Mobile Nodes in OPNET Modeler Environment*, In Proceedings of the 35th International Conference on Telecommunications and Signal Processing - TSP' 2012, 2012.

[6] Kai-Ten Fengi. *LMA: Location- and Mobility-Aware Medium-Access Control Protocols forVehicular Ad Hoc Networks Using Directional Antennas*, IEEE Transactions on Vehicular Technology, 2007.

Nermin Makhlouf Currently postgraduate student at the Department of Telecommunications of the Faculty of Electrical Engineering and Communication, BUT. Her research work has been concentrated on prediction of movement of wireless nodes in mobile ad-hoc networks MANETs. Recently she has also been concerned with MAC protocols in mobile ad hoc networks and improvement of interference and collision among the nodes in such networks.

Pavel Vajsar Currently postgraduate student at the Department of Telecommunications of the Faculty of Electrical Engineering and Communication, BUT. His research work has been concentrated on routing in MANET networks with regard on quality of services. Recently he has also been concerned with wireless sensor networks and developing of application for monitoring of these networks.

Simple Electromagnetic Analysis in Cryptography

Zdenek Martinasek, Vaclav Zeman, Krisztina Trasy

***Abstract*—The article describes the main principle and methods of simple electromagnetic analysis and thus provides an overview of simple electromagnetic analysis. The introductory chapters describe specific SPA attack used visual inspection of EM traces, template based attack and collision attack. After reading the article, the reader is sufficiently informed of any context of SEMA. Another aim of the article is the practical realization of SEMA which is focused on AES implementation. The visual inspection of EM trace of AES is performed step by step and the result is the determination of secret key Hamming weight. On the resulting EM trace, the Hamming weight of the secret key 1 to 8 was clearly visible. This method allows reduction from the number of possible keys for following brute force attack.**

***Keywords*—elektromagnetic analysis, simple analysis, EMA, side channels.**

I. Introduction

Since their public appearance in the mid-90s [1], side-channel attacks have attracted a significant attention within the cryptographic community. The power analysis (PA) and the electromagnetic analysis (EMA) are typical examples of successful attacks against trusted cryptographic devices. Scientist van Eck [2] had merit in the advancement of electromagnetic attacks in the public sector, Eck proved that it is possible to capture and measure the size of the electromagnetic field of computer monitors and it is possible to obtain the original image from measured waveforms. Scientists Kuhn and Anderson [3] invented countermeasurement against the attack and it was a special shielding film, which reduce the electromagnetic radiation of the monitor.

The first published articles focused on the EMA of integrated circuits and computing units performing the cryptographic operations were [4] by Gandolfi in 2001 and [5] by Quisquater and Samyde. The attacks were realized by using several antennas located near the integrated circuit of smart card. These attacks were invasive, which means that it was necessary to destroy of smart card cover to give the antenna as close as possible to the chip. Agrawal [6] build on this work and used the declassified materials from the project TEMPEST and showed that EM side channel attacks on cryptographic devices are practically realizable and also some information that leaked through EM channel are more significant than information that leaked through the power side channel. Articles [7], [8], [9] are focused on systematic study of EM leakage information from computing equipment such as smart cards, computer processors and cryptographic accelerators.

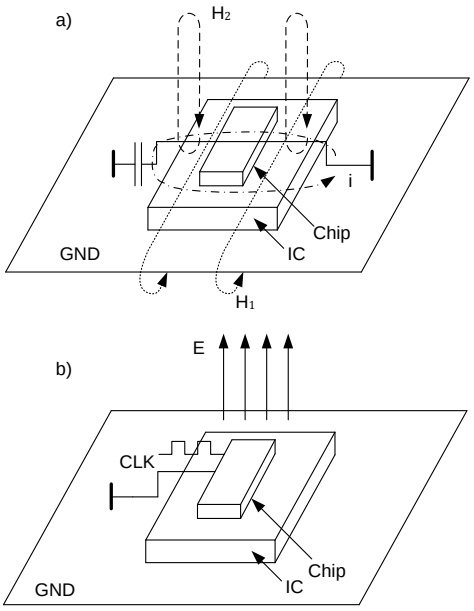


Fig. 1. The principle of direct emissions of the magnetic field of IC

As well as in classical power analysis, the attacker is measuring dynamic electromagnetic field of cryptographic device depending on input data. The plain text is encrypted by using a secret key and measured waveforms are recorded within a measuring device for encrypting each plaintext. The attacker can deduct sensitive information directly (SEMA, Simple Electromagnetic Analysis) or can use mathematical approach (DEMA, Different Electromagnetic Analysis). In SEMA, the attacker tries to determine the key more or less directly from one measured trace. In other words SPA attacks are useful in practice if only one or very few traces are available. DEMA and DPA attacks are the most popular because the attacker does not need any detailed knowledge about the attacked device. In contrast to SA, the DA attacks require a large number of power traces measurements. DPA attack uses mathematical approach to determine the sensitive information.

The goal of the article is to describe the main principle and the methods of simple electromagnetic analysis. In the other words, the article create an overview of simple electromagnetic analysis. Another aim of the article is the practical realization of SEMA which is focused on AES implementation with a description of the experimental testbed. The SEMA of AES is performed step by step and the result is the determination of secret key Hamming weight. After reading the article, the

Zdenek Martinasek is with Brno University of Technology, Brno, Czech Republic. He is now with the Department of Telecommunications, Purkynova 118, 612 00 Brno, (martinasek@feec.vutbr.cz).

Vaclav Zeman is with Brno University of Technology, Brno, Czech Republic. He is now with the Department of Telecommunications, Purkynova 118, 612 00 Brno (zeman@feec.vutbr.cz).

Krisztina Trasy is with Department of Garden and Open Space Design, Faculty of Landscape Architecture, Corvinus University of Budapest, Fovam ter 8, Budapest, Hungary (krisztina.trasy@stud.uni-corvinus.hu).

Manuscript received September 3, 2012; revised January 11, 2007.

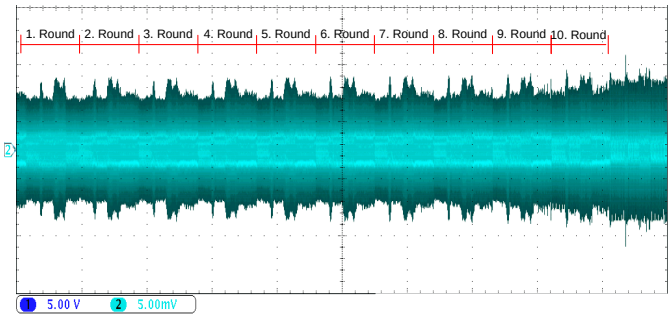


Fig. 2. EM trace of AES

reader is sufficiently informed of any context of SEMA.

The article is divided as follows: the following section describes SEMA attacks and the following three subsections discuss specific attack types used visual inspection of EM traces, template based attack and collision attack. The last chapter illustrates a specific example of SEMA attack, which was realized on the encryption algorithm AES. Visual analysis of electromagnetic traces was aimed at operation `AddRoundKey`.

II. Side channel sources

The most modern cryptographic equipments are based on CMOS technology. The basic element of this logic is the inverter [10]. The inverter contains two field-effect transistors with the opposite type of conductivity PMOS (P-channel) and NMOS (N-channel) and works as follows:

- when the voltage of input is high the PMOS transistor is off and the NMOS transistor is on and the output of inverter is low,
- on the other hand, when the voltage of the input is low NMOS transistor is off and the PMOS is on, so the output voltage is high.

The power consumption is minimal for both these stable states. Power peak occurs during the transition between these states when both transistors are open in a short time and power supply is shorted to the ground. The size of current peaks is directly proportional to the number of transistors which have been switched in the whole integrated circuit. The main source of power change is charging and discharging a parasitic capacity by a current [11]. This parasitic capacity represents the capacity of control electrodes following transistors in the integrated circuit. The dynamic power consumption of the inverter can be expressed by the formula [11]:

$$P_{\text{dyn}} = C \cdot V_{\text{CC}}^2 \cdot P_{0\to1} \cdot f, \qquad (1)$$

where C is the parasitic capacity, $P_{0\to1}$ is the probability of transition between states $0 \to 1$, f is a switching frequency and V_{CC} is the supply voltage. If the power consumption is measured (to ground or power junction of the inverter) will be the highest peak while charging the parasitic capacity [11].

The result of charging and discharging of parasitic capacitance is the step change of circuit current which affects emit electromagnetic fields in the vicinity of the inverter. Modern

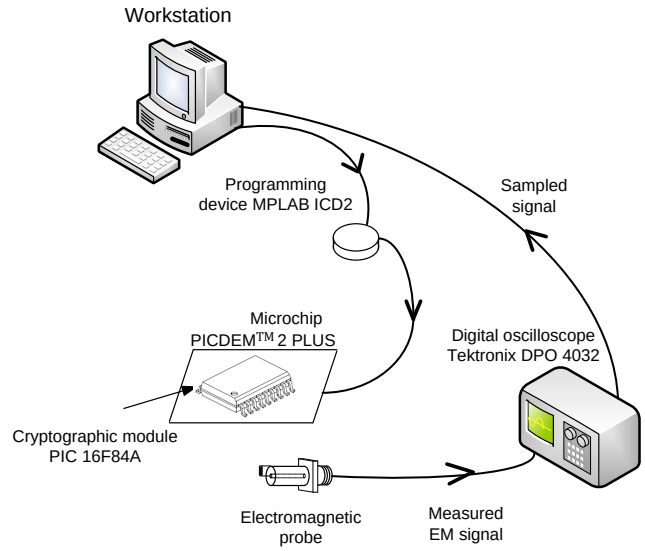


Fig. 3. Diagram of the testbed.

integrated circuits are composed of millions of transistors and connections, in which the changing currents are dependent on the transmitted data. These currents generate a variable electromagnetic field that can be measured by the probes. The ways of EM radiation emitted by integrated circuits (IC) are the following:

- conductive emission - is reflected in the integrated circuit pins, respectively, in routes which are connected on pins. These routes may behave as antennas emitting radiation during a step change in current.
- Electric and magnetic near-field emissions - EM field is generated due to current loops in IC. The magnetic field component can be divided into two parts H1 and H2 as it is shown in figure 1 a). The field H1 is closed around the ground contact of printed circuit boards and H2 is generated by currents in the internal capacitors and closes in the area above the surface of the IC in the range of approximately 10 mm. The magnetic field H2 is significantly larger than the field H1.

The electric field is located in the vicinity of parts under power supply. The main source of the electric field are internal a conductive connection in the IC. Figure 1 b) shows the emission of the electric field caused by the clock signal. Most of the flow is concluded to the ground, but part of the flow is radiated into the environment.

Based on the assumption that the IC generates an electromagnetic field, it is possible to characterize the electromagnetic emission by measuring. These measurements are realized by electric and magnetic probes. Measurement with small magnetic probes are used to determine the size of near magnetic field. The advantage of these probes is that they can be placed as close as possible to the source of radiation and increase the measurement accuracy. If the probe is placed further away it is possible to detect the microprocessor clock signal. Useful EM signals, which are dependent on the processed data, can be captured in the areas of the processor and

```
1.R = m
2.for i = 0:(b - 1) {
3.         R = (R*R)mod(n)
4.         if (d(i)==1) {
5.              R=(R*m)mod(n)   }
6. }
7. return R
```

Fig. 4. Algoritmus square and multiply

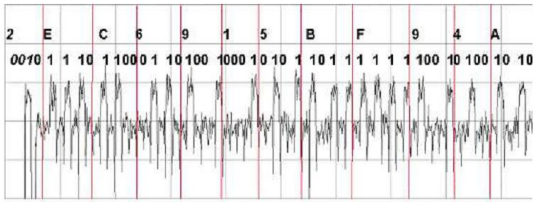


Fig. 5. Current consumption of square and multiply [13]

the memory of cryptosystem [11], [12].

Our measurements typically take place in this region where the signals may be considered as quasi-static. This allows to use the Biot-Savart law to describe the magnetic field $\vec{B}$:

$$d\vec{B} = \frac{\mu I \vec{dl} \times \hat{r}}{4\pi |\vec{r}|^2} \tag{2}$$

where I is the current carried on the conductor of infinitesimal length $\vec{dl}$, μ is the magnetic permeability and $\vec{r}$ is a vector specifying the distance between the current and the field point ($\hat{r} = \vec{r} / |\vec{r}|$).

Faraday's law can be used to express the voltage that will induce in the probe:

$$V_{emf} = -N\frac{d\phi}{dt} \tag{3}$$

$$d\phi = \int_{surface} \vec{B} \cdot d\vec{S} \tag{4}$$

where N is the number of turns in the coil and ϕ the magnetic flux. This equation clearly expresses that the closer we place the probe to the chip, the bigger the measured magnetic field is. These simple equations do not describe the exact behavior of the magnetic field because the field is data-dependent (that means dependent of the current intensity) and the orientation of the field directly depends on the orientation of the current. The processor will still process the same data (in a program loop) and we calculate the mean values of EM field to reduce this dependency (electronic noise).

If we assume that the bus may behave as an infinite wire, we can reduce the above cited Biot-Savart equation to the following expression:

$$\vec{B} = \frac{\mu I}{2\pi R}\hat{a_\varphi} \tag{5}$$

where R is the distance to the wire and $\hat{a_\varphi}$ is a unit vector azimuthally oriented with respect to the wire. It follows from these assumptions that the size of the induced voltage will be affected of probe position (angle) and microchip.

III. Simple Electromagnetic Analysis

This chapter will explain the principle of simple elektromagnetic analysis and will describe the various types. A simple power analysis (same like EM analysis II) was defined by Kocher [1] as follows: SPA is a technique that involves directly a interpreting power consumption measurements collected during cryptographic operations. In other words, the attacker tries to determine the secret key directly from the measured EM traces. This could make the simple analysis attack for potential attackers quite attractive technology, but they usually need detailed knowledge about the implemented algorithm and cryptographic device (module). In the extreme case, the attacker attempts to reveal the secret key based on one single measured EM trace. We can distinguish between single shot SPA attacks and multiple shot. From the name, it is clear that the attacker records only one EM trace in a single shot of SPA attacks and more EM traces in multiple shot. If there is only one measured waveform, it is necessary to use statistical methods to extract the useful signal. The advantage is the possibility to reduce the noise in measured traces when the attacker has more traces available. For both types of SPA attacks it is unconditionally necessary existence significant (direct or indirect) dependence of a secret key and EM trace.

A. Visual Inspections of EM Trace

Direct observation of traces is based on the following facts. All algorithms that run on cryptographic devices are performed successively in a defined sequence. Cryptographic algorithm consists of several functions (operations), which are translated into instructions supported by cryptographic module (microprocessor). For example, the core of AES algorithm is composed of these functions: key expansion, adding keys, nonlinear byte substitution rotation rows and matrix multiplication. These operations can be implemented in the microprocessor and in this case, the functions are implemented using a microprocessor supported instruction.

In most cases, the microprocessors have the instruction set, which includes arithmetic instructions (addition), logical instruction (XOR), instructions work with data (store, move), program branch instruction (jump or condition). Each instruction is working with a different number of bits or bytes and uses the different parts of the circuit such as an arithmetic logic unit, the internal or external memory (RAM or ROM) or input and output ports. These microprocessor components are physically separated and are different from functions and realization. For this reason, every instruction has typical EM trace which leads to the creation of characteristic EM pattern (fingerprint). The ability to distinguish between individual instruction in EM trace brings serious security threat when a sequence of instructions depends directly on a secret key. If specific instruction is processing during algorithm, when the key bit is 1 and different instruction is processed and if a key bit is 0, then it is possible to determine the secret key directly from the measured EM trace looking at the sequence

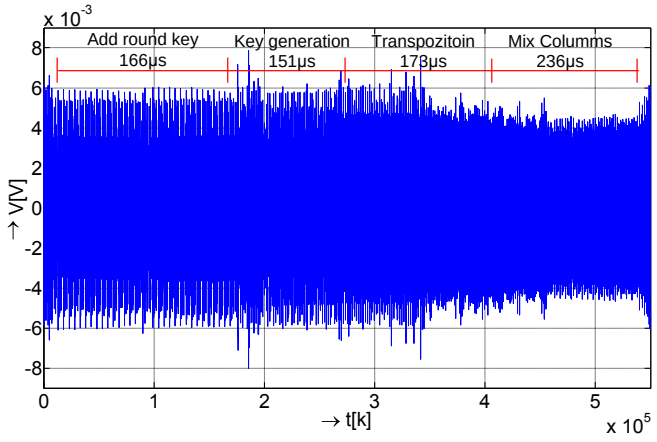


Fig. 6. EM trace of the first round.

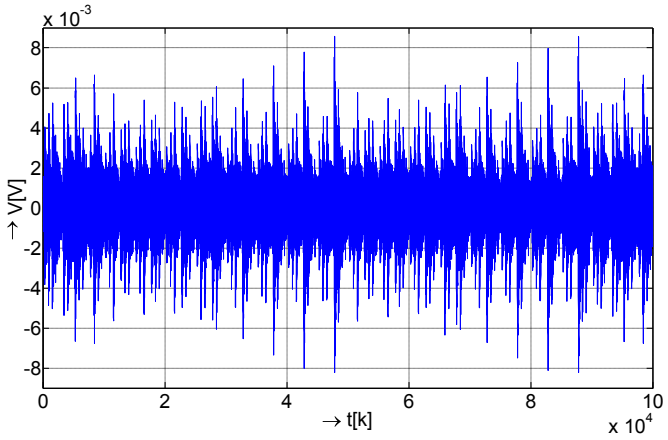


Fig. 7. EM trace of `Add Round Key`.

of performed instructions. A typical example of this SPA is attack to the implementation of an asymmetric algorithm RSA. Asymmetric RSA algorithm is based on a mathematical operation modular exponentiation. For the calculation of modular exponentiation there are more methods, but square and multiply algorithm are often used for the implementation in to the cryptographic modules. In this algorithm, each key bit (d) is processed sequentially (left-to-right) and is processed with a modular square operation followed by a conditional modular multiplication. The multiplication is only executed when the associated key bit is equal to one. Schema of algorithm is shown in figure 4. The attacker can easily determine from the EM trace (sequence of instructions) in which step was performed row 3 and in which 5 of algorithm. An example of current consumption square and multiply algorithm is shown in Figure 5. The attacker then easily determines the value of the secret key.

B. Template Based Attacks

Template based attacks use the fact that EM consumption is dependent on the currently processed data. Electromagnetic traces are characterized multidimensional normal distribution, which is fully defined by the vector of mean values and covariance matrix $(\mathbf{m}, \mathbf{C})$. This pair $(\mathbf{m}, \mathbf{C})$, is denoted as a template. The attacker assumes that he can characterize the device with the help of templates for certain sequences of instructions. For example, the attacker has full control over the same device on which he wants to perform attack. On this device, he starts a sequence of instructions for different input data d_i and a different key k_j and records the EM waveforms. Subsequently, the attacker groups corresponding sequences (d_i, k_j) and calculate the vector of mean values and covariance matrix of multivariate normal distribution. The result is obtained templates for all pairs data and keys $(d_i, k_j) : h_{d_i,k_j} = (\mathbf{m}, \mathbf{C})$. During the attack, the attacker uses these templates and just measured power consumption to determine the secret key of device as follows. At first, he measures the EM trace of device and the second step is the calculation of the probability density function of multivariate normal distribution $(\mathbf{m}, \mathbf{C})_{d_i,k_j}$ and the measured trace. In other words, he calculates the probabilities for the measured EM trace for all templates according to the following equation:

$$p(t; (\mathbf{m}, \mathbf{C})_{d_i,k_j}) = \frac{exp(-\frac{1}{2} \cdot (\mathbf{t} - \mathbf{m})' \cdot \mathbf{C}^{-1} \cdot (\mathbf{t} - \mathbf{m}))}{\sqrt{(2 \cdot \pi)^T \cdot det(\mathbf{C})}}. \quad (6)$$

Probabilities indicate how good the templates match measured trace. Fully intuitively, the maximum probability should correspond to the correct template. Each template is associated with a secret key therefore the attacker can determine the secret key. This method is based on the theory which is described in [14].

C. Collision Attacks

Collision Attacks are based on the fact that the attacker is able to observe the EM consumption for two encryption runs with two different inputs d_i and d_i and the unknown key k_j . In a collision, the attacker exploits the fact that in two encryption runs a specific intermediate value v_i, j can be equal:$v_j = f(d_i, k_j) = f(d_i^*, k_j)$. Intermedia1e value collides if an intrermedia1e value in one encryption run is equal to the intrermedia1e value the other encryption run. The most important knowledge is that for two inputs d_i and d_i^* a collision cannot occur for all key values but only for a certain subset of keys. Each collision allows to reduce the search space for the key. If several collisions can be realized, the key can be identified.

IV. Experimental measurements

The testbed focused on the measuring direct emissions was built to realize SEMA using Visual Inspections of EM Trace (section III-A). Diagram of the testbed is shown in figure 3 and was designed from the following devices:

- cryptographic module PIC16F84 microcontroller,
- workstation with installed software MPLAB,
- electromagnetic probe for sensing near EM field,
- ICD2 programing device,
- development board PICDEM 2 PLUS,
- oscilloscope Tektronix DPO-4032 with a maximum sampling frequency of 2.5GSa/s.

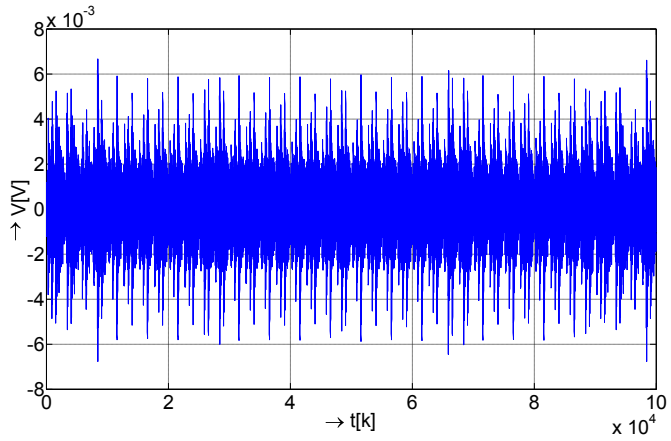


Fig. 8. The reference EM trace T_{ref}

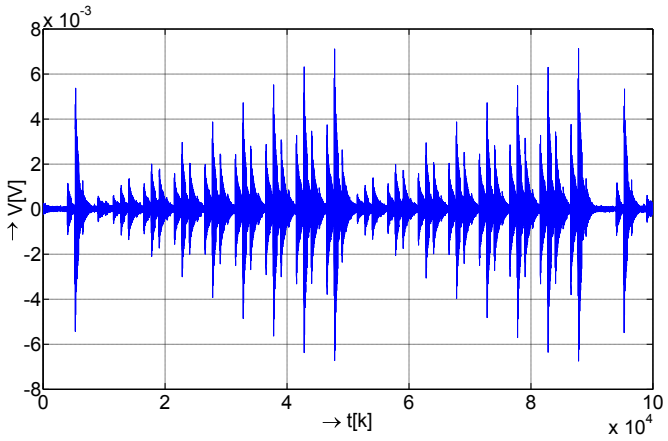


Fig. 9. The differential EM trace.

Encryption algorithm AES was implemented to the cryptographic module PIC16f84A. The algorithm was created by Edim Permadim [15] but it was necessary to take a few adjustments for measurement. For example the synchronization signal was inserted to simplify synchronization with oscilloscope. Figure 2 shows the total EM trace of AES algorithm stored by oscilloscope. Ten rounds of AES are clearly visible and the attacker can concentrate only the interesting parts on.

We analyzed EM trace of the whole AES algorithm and we focused only analyzing operations `Add Round Key`, because in initializing phase this operation works with original secret key. This operation performs the logical operation XOR with the block of plaintext **A** and the block of secret key $\mathbf{K_{sec}}$ and saves the result to the block **S**. In the original form, the AES algorithm works with the length of data blocks of 128 bits (4×4 matrix). Operations `Add Round Key` can be written as follows:

$$\mathbf{S} = \mathbf{A} \otimes \mathbf{K_{sec}}. \tag{7}$$

Figure 6 shows the EM trace of the AES first rounds. The raw contour of the individual phases are visible but more precise identification should be done at the level of individual instructions. The algorithm begins with an initialization phase `Add Round Key` and this operation takes 166 microseconds. The following operation is `Sub keys Generation`, which is executed every each cycle because insufficiency of storage space is available on a microprocessor. This operation takes 151 microseconds. The next operations are byte substitution and rotation and take 151 microseconds. The final operation is the `Mix Column`, which is quite demanding and takes 236 microseconds. The total duration of one round implemented AES algorithm is 726 microseconds.

Suppose the secret key is byte expressed $K = \{n, n, n, n, n, n, n, n\}$ for $0 \leq n \geq 256$. From the mathematical perspective each byte is a group of eight elements containing two groups of elements (specific number of 1 and 0). The number of all secret keys i of possible combinations

TABLE I
PERMUTATION OF SECRET KEY DEPENDING ON THE HAMMING WEIGHT

Hamming weight w of secret key (max 8)	Permutation i of secret key (theoretical max 256)
1	8
2	28
3	56
4	70
5	64
6	28
7	8
8	1

is given by the permutation with repetition:

$$i_{m_1,m_2,\ldots,m_k} = \frac{m!}{m_1! \cdot m_2! \cdot \cdots \cdot m_k!}. \tag{8}$$

The number of non-zero bits in the key can be described with Hamming weight w $0 \leq w \geq 8$. If the attacker knows the secret key Hamming weight, the number of all possible variants can be reduced according to (8). Table I shows the number of key combinations according to the (8) depending on the Hamming weight. The table shows that the knowledge of key Hamming weight will significantly reduce the number of possible secret key. In the worst case ($w = 4$) it would be chosen from 70 possible values from theoretical 256. This number corresponds to 30% of total number secret key.

Secret key $\mathbf{K_{sec}}$ was filled with various data manually in our experiment and the data was set randomly. Data had value from 01h to FFh, where Hamming weight w of the next element is always greater one compared to the previous element. For example the value of the first secret key word $k_{0,0}$ was 01h (B'00000001') then $w(k_{0,0}) = 1$. The following element in the matrix has a value 03h (B'00000011') than Hamming weight of the last element of $w(k_{0,1}) = 2$ and the last element $k_{3,3}$ takes the value FFh (B'11111111'), were $w(k_{1,3}) = 8$. The matrix of secret key $\mathbf{K_{sec}}$ look as follows (hexadecimal notation):

$$\mathbf{K_{sec}} = \begin{pmatrix} 01 & 03 & 07 & 0F \\ 1F & 3F & 7F & FF \\ 01 & 03 & 07 & 0F \\ 1F & 3F & 7F & FF \end{pmatrix}.$$

Hamming weight of the secret key can be determined by realization of two measurement of EM traces. The authors follow the own work focused on power side channel [16], [17], [18], [19], [20]. The method is following: the attacker measures the reference EM trace T_{ref}, which corresponds to the operation `Add Round Key` where the values of key and state are zero. It is necessary for the attacker to have full control over the same device on which he wants to perform attack. Measured reference EM trace T_{ref} is displayed in figure 8. No significant peaks are visible on trace because the cryptographic module works with no data. After that, the attacker measures EM traces of cryptographic module corresponding to the `Add Round Key`. This trace is shown in the figure 7. During the second measurement, the microprocessor works with data according to the rules described above therefore peaks were observed on trace. The peaks corresponding to data processing are very evident but Hamming weight is not entirely clear for lower values. The best way to improve readability is to calculate differential signal as a simple subtraction of trace in this two measurements, i.e. trace of T_{ref} and measured EM trace. The result of this simple operation is the waveform shown in figure 9. The figure shows peaks corresponding to work with data. Very important is that the increasing of the Hamming weight of the secret key 1 to 8 is clearly visible. In this case, the Hamming weight of secret key equals 72.

The numerical evaluation of measured data could be summarized again with table I, because the HW is successively equal to values $1, 2, 3, 4, 5, 6, 7, 8$. It is obvious that table contains results only for the first half of the key because the second half is the same. From the table it is evident that the knowledge of key Hamming weight reduced the number of possible keys. We do not assume determination of the whole secret key (in our key 128 bits length) in one time moment but we assume determination of secret key successively by bytes like in SEMA and DEMA. In this case this method allow reduction from the number of possible keys from 2048 to 263 and in the worst case for $w = 4$ it corresponds to 56. If it is not possible to determinate the secret key by bytes, this method allows to reduce the number of possible key for brute force attack from $3.40 \cdot 10^38$ to $1.58 \cdot 10^20$ for 128 bits length key. In the worst case for Hamming weight $w = 4$ and it corresponds to $3.32 \cdot 10^29$.

V. Conclusion

The article describes the main principle and methods of simple electromagnetic analysis. The introductory chapters describe specific SPA attack used visual inspection of EM traces, template based attack and collision attack. Another aim of the article was the practical realization of SEMA which is focused on AES implementation. The visual inspection of EM trace of AES is performed step by step and the result is the determination of secret key Hamming weight.

We analyzed the EM trace of the operations `Add Round Key` in initializing phase because in this time the algorithm works with original secret key. Hamming weight of secret key was determined by realization of two measurements of EM traces and then subtracting waveforms. The first trace corresponds to the operation `Add Round Key` where the values of key and state are zero and the second corresponds to the operation `Add Round Key` where the values of key equal secret key and state are random. During the second measurement, the microprocessor performs the date with operation XOR, therefore peaks were observed on trace. The Hamming weight of the secret key 1 to 8 was clearly visible and in this case, the Hamming weight of secret key equaled 72. In this case this method allows reduction from the number of possible keys and it depended on the fact if the attacker is able to test thee key by bytes or whole.

References

[1] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *CRYPTO '99: Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*. London, UK: Springer-Verlag, 1999, pp. 388–397.

[2] W. V. Eck and N. Laborato, "Electromagnetic radiation from video display units: An eavesdropping risk?" *Computers & Security*, vol. 4, pp. 269–286, 1985.

[3] M. G. Kuhn and R. J. Anderson, "Soft tempest: Hidden data transmission using electromagnetic emanations," in *Proc. 2nd Workshop on Information Hiding*. Springer-Verlag, 1998, pp. 124–142.

[4] K. Gandolfi, D. Naccache, C. Paar, K. G, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," 2001.

[5] J.-J. Quisquater and D. Samyde, "Electromagnetic analysis (ema): Measures and counter-measures for smart cards," in *Smart Card Programming and Security*, ser. Lecture Notes in Computer Science, I. Attali and T. Jensen, Eds. Springer Berlin / Heidelberg, 2001, vol. 2140, pp. 200–210, 10.1007/3-540-45418-7_17. [Online]. Available: http://dx.doi.org/10.1007/3-540-45418-7_17

[6] D. Agrawal, B. Archambeault, J. Rao, and P. Rohatgi, "The EM Side Channel(s)," 2003, pp. 29–45. [Online]. Available: http://dx.doi.org/10.1007/3-540-36400-5_4

[7] Çetin Kaya Koç, P. Rothatgi, W. Schindler, and C. D. Walter, Eds., *Cryptographic Engineering*, 2009.

[8] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in *CHES '01: Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems*. London, UK: Springer-Verlag, 2001, pp. 251–261.

[9] B. Struif, "Use of biometrics for user verification in electronic signature smartcards," in *Smart Card Programming and Security*, I. Attali and T. Jensen, Eds., no. 2140, Berlin, 2001. [Online]. Available: 2140/21400220.htm

[10] M. Alioto, L. Giancane, G. Scotti, and A. Trifiletti, "Leakage power analysis attacks: A novel class of attacks to nanometer cryptographic circuits," *Circuits and Systems I: Regular Papers, IEEE Transactions on*, vol. 57, no. 2, pp. 355 –367, feb. 2010.

[11] E. Peeters, F.-X. Standaert, and J.-J. Quisquater, "Power and electromagnetic analysis: Improved model, consequences and comparisons," *Integration, the VLSI Journal*, vol. 40, no. 1, pp. 52 – 60, 2007, embedded Cryptographic Hardware. [Online]. Available: http://www.sciencedirect.com/science/article/B6V1M-4J3NWY2-1/2/0197aa6143d75a8303ace31403077841

[12] T. Ostermann, W. Gut, C. Bacher, and B. Deutschmann, "Measures to reduce the electromagnetic emission of a soc," in *VLSI-SOC*, 2003, pp. 31–.

[13] M. Joye and F. Olivier, "Side-channel analysis," in *Encyclopedia of Cryptography and Security (2nd Ed.)*, 2011, pp. 1198–1204.

[14] S. M. Kay, *Fundamentals of Statistical Signal Processing, Volume I: Estimation Theory (v. 1)*, 1st ed. Prentice Hall, Apr. 1993. [Online]. Available: http://www.worldcat.org/isbn/0133457117

[15] E. Permadim. (2010, Dec.) Pic microcontoller math library methods. [Online]. Available: http://www.piclist.com/techref/microchip/math/index.htm

[16] Z. Martinasek, T. Macha, and P. Stancikk, "Power side channel information measurement," in *Research in telecommunication technologies RTT2010*, September 2010.

[17] Z. Martinasek, T. Petrik, and P. Stancik, "Conditions affecting the measurement of power analysis," in *Research in telecommunication technologies RTT2011*, September 2011.

[18] Z. Martinasek and P. Machu, "New side channel in cryptography," in *Proceedings of the 17th Conference Student EEICT 2011*, April 2011.
[19] Z. Martinasek, T. Macha, and V. Zeman, "Classifier of power side channel," in *Proceedings of NIMT2010*, September 2010.
[20] Z. Martinasek, T. Macha, O. Raso, J. Martinasek, and P. Silhavy, "Optimization of differential power analysis," *PRZEGLAD ELEKTROTECHNICZNY*, vol. 87, no. 12, pp. 140 – 144, 2011. [Online]. Available: http://pe.org.pl/articles/2011/12a/28.pdf

Zdenek Martinasek received BSc at the Department of Telecommunications at the Faculty of Electrical Engineering and Communication at Brno University of Technology in 2006. He received Ing. (MSc) at the same department in 2008. Now he is a PhD student at the same faculty. He also helps to cover pedagogically Master's program course. The area of his professional interests is cryptography,side channel analysis, sensors and modern data communication.

Vaclav Zeman received MSc. (Ing) at Faculty of Electrical Engineering and Communication at Brno University of Technology in 1991. He received Ph.D. at the Department of Telecommunications the at same Faculty in 2003. Now is the Associate Professor (doc. 2005) Faculty of Electrical Engineering and Communication at Brno University of Technology. He publishes in the cryptology area and communication systems area. Now, he is a lecturer and he deals with cryptology and information system security.

Krisztina Trasy was born in 1988 and she is last year MSc student of Department of Garden and Open Space Design, Faculty of Landscape Architecture, Corvinus University of Budapest.

A Voltage Gain-Controlled Modified CFOA And Its Application in Electronically Tunable Four-Mode All-Pass Filter Design

Norbert Herencsar, Jaroslav Koton, Abhirup Lahiri, Bilgin Metin, and Kamil Vrba

***Abstract*—This paper presents a new active building block (ABB) called voltage gain-controlled modified current feedback amplifier (VGC-MCFOA) based on bipolar junction transistor technology. The versatility of the new ABB is demonstrated in new first-order all-pass filter structure design employing single VGC-MCFOA, single grounded capacitor, and three resistors. Introduced circuit provides all four possible transfer functions at the same configuration, namely current-mode, transimpedance-mode, transadmittance-mode, and voltage-mode. The pole frequency of the circuit can be easily tuned by means of DC bias currents. The theoretical results are verified by SPICE simulations based on bipolar transistor arrays AT&T ALA400-CBIC-R process parameters.**

***Keywords*—Voltage gain-controlled modified CFOA, MCFOA, electronically tunable filter, four-mode circuit, all-pass filter.**

I. Introduction

After the second-generation current conveyor (CCII) was introduced by Sedra and Smith in 1970 [1], it became the most versatile active building block (ABB) used for analog signal processing and the is basic ABB of many other active elements such as the composite current conveyor [2] done by an interconnection of two CCIIs, which was recently introduced as modified current feedback operational amplifier (MCFOA) [3]–[7] or the conventional CFOA [8] (CCII followed by unity gain voltage buffer - UGVB). It should be noted that, the MCFOA is different from the conventional CFOA defined in [8], since the W terminal current of the MCFOA is copied to the Y terminal in the opposite direction. However, it is well known that the Y-terminal current of the conventional CFOA is equal to zero. Short list of additional CCII-based ABBs is the following: the second-generation current-controlled conveyor (CCCII) [9], where the intrinsic resistance of X-terminal can be tuned, the differential difference CC (DDCC) [10] and its more versatile derivative the so-called universal current conveyor (UCC) [11]–[14], the dual-X CCII (DXCCII) [15], which is an interconnection of CCII and inverting CCII in which the Y-terminal is joined, the current differencing buffered amplifier (CDBA) [16] employing current differencing unit (CDU) based on two CCIIs and UGVB, or the universal voltage conveyor (UVC) [17] based on two CCIIs and differential UGVB.

Recently the further research has been focused on CCII-based ABBs employing operational transconductance amplifier (OTA) [18] at their output stage. Probably the most known active element from this group is the current differencing transconductance amplifier (CDTA) [19], but other versatile elements such as the current-conveyor transconductance amplifier (CCTA) [20], where CCII is followed by an OTA, the differential-input buffered and transconductance amplifier (DBTA) [21] in which an interconnection of two CCIIs are followed by UGVB and OTA, the current follower transconductance amplifier (CFTA) [22], which employs a CCII with grounded Y-terminal and an OTA, the current backward transconductance amplifier (CBTA) [23], which is a specific interconnection of CCII and OTA, or the z-copy current-controlled current inverting transconductance amplifier (ZC-CCCITA) [24] have also received considerable attention.

For easy tunability of the circuit parameters using electrical signals by either voltage and/or current and to increase the universality of the conventional CCII, the electronically-tunable CCII (ECCII) [25], [26], programmable current amplifier (PCA) [27], K-gain CCII [28], the voltage and current gain CCII (VCG-CCII) [29], and the variable gain current conveyor (VGCCII) [30] were introduced.

In this paper we present a novel ABB called voltage gain-controlled modified current-feedback operational amplifier (VGC-MCFOA). The VGC-MCFOA joins the voltage gain control feature of the VCG-CCII in the conventional MCFOA [3]–[7]. To demonstrate the usefulness of the VGC-MCFOA, a new first-order all-pass filter (AFP) structure is proposed, which operates in current-mode (CM), transimpedance-mode (TIM), transadmittance-mode (TAM), and voltage-mode (VM), respectively. To prove the theoretical analysis, SPICE simulations based on bipolar transistor arrays AT&T ALA400-CBIC-R process parameters are given.

II. Circuit Description

The voltage gain-controlled modified current feedback operational amplifier (VGC-MCFOA) is a five-terminal ABB and its circuit symbol is shown in Fig. 1(a). Compared to the conventional MCFOA presented in [3]–[7], its voltage transfer

N. Herencsar, J. Koton, and K. Vrba are with the Department of Telecommunications, Faculty of Electrical Engineering and Communication, Brno University of Technology, Purkynova 118, 612 00 Brno, Czech Republic (phone: +420-541149190; fax: +420-541149192; e-mails: {herencsn, koton, vrbak}@feec.vutbr.cz; web: http://publicationslist.org/herencsar).

A. Lahiri is with the 36-B, J and K Pocket, Dilshad Garden, Delhi-110095, India (e-mail: lahiriabhirup@yahoo.com; http://www.publicationslist.org/lahiriabhirup).

B. Metin is with the Department of Management Information Systems, Bogazici University, Hisar Campus, 34342 Bebek-Istanbul, Turkey (e-mail: bilgin.metin@boun.edu.tr; http://www.mis.boun.edu.tr/metin/).

Manuscript received October XX, 2012; revised Month DD, YYYY.

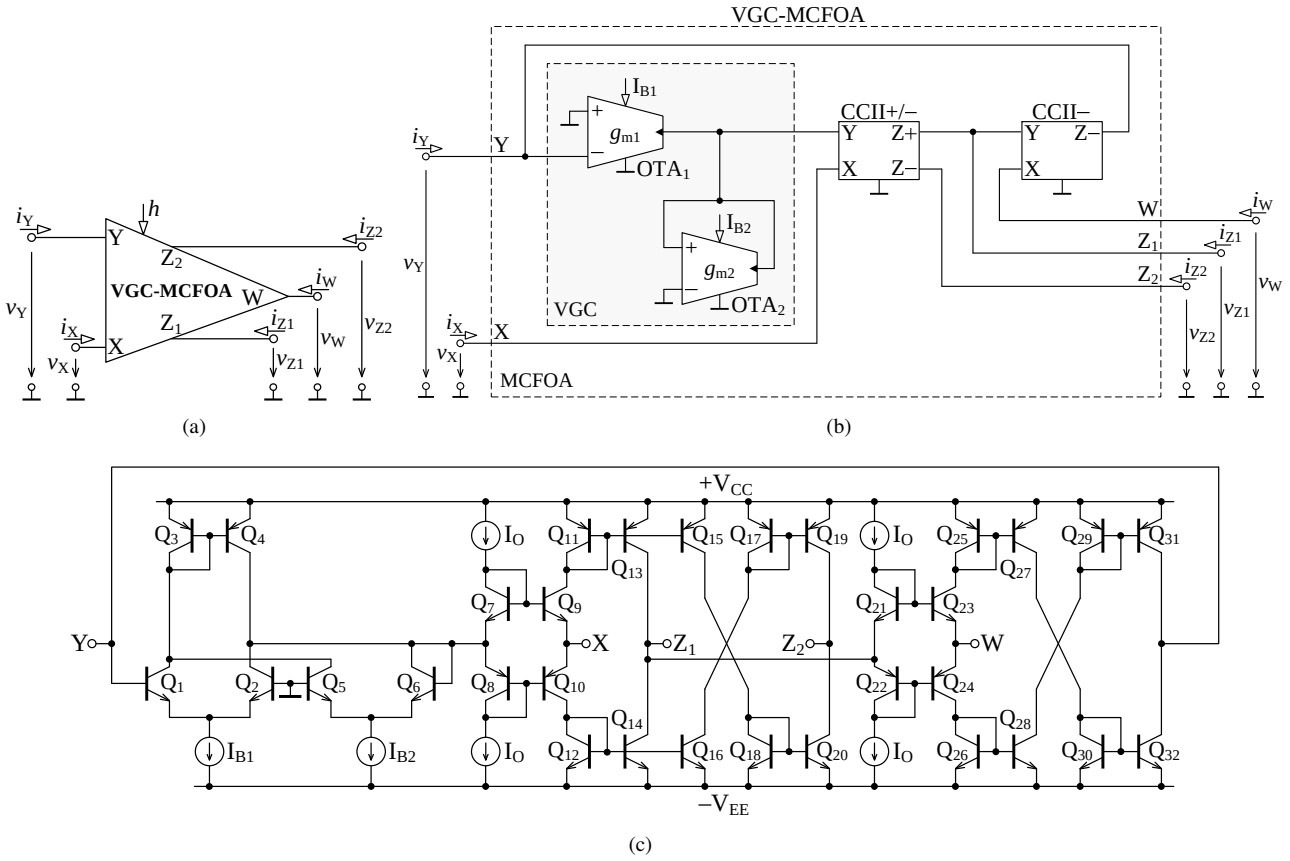


Fig. 1. Bipolar implementation of VGC-MCFOA

from the Y to X terminal can be easily electronically tuned by means of the voltage gain h. Hence, the relations between the individual terminals of the VGC-MCFOA can be described by the following hybrid matrix:

$$\begin{bmatrix} i_{\mathrm{Y}} \\ v_{\mathrm{X}} \\ i_{\mathrm{Z1}} \\ i_{\mathrm{Z2}} \\ v_{\mathrm{W}} \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & -\alpha_1 \\ h\beta_1 & 0 & 0 & 0 & 0 \\ 0 & \alpha_2 & 0 & 0 & 0 \\ 0 & -\alpha_3 & 0 & 0 & 0 \\ 0 & 0 & \beta_2 & 0 & 0 \end{bmatrix} \begin{bmatrix} v_{\mathrm{Y}} \\ i_{\mathrm{X}} \\ v_{\mathrm{Z1}} \\ v_{\mathrm{Z2}} \\ i_{\mathrm{W}} \end{bmatrix}. \quad (1)$$

The frequency-dependent non-ideal current gains α_j for $j = \{1,2,3\}$ and voltage gains β_k for $k = \{1,2\}$ are ideally equal to unity. Using a single-pole model [4], they can be defined as:

$$\alpha_j(s) = \frac{\alpha_{oj}}{1 + s\tau_{\alpha_j}}, \quad (2)$$

$$\beta_k(s) = \frac{\beta_{ok}}{1 + s\tau_{\beta_k}}, \quad (3)$$

where α_{oj} and β_{ok} are DC current and voltage gains of the element, respectively. The bandwidths $1/\tau_{\alpha_j}$ and $1/\tau_{\beta_k}$ on the order of a few gigarad/s in current technologies are ideally equal to infinity. At low and medium frequencies i.e., $f \ll (1/(2\pi))\times \min\{1/\tau_{\alpha_j}, 1/\tau_{\beta_k}\}$, Eqs. (2) and (3) turn to:

$$\alpha_j(s) \cong \alpha_{oj} = 1 - \varepsilon_{\alpha_{ij}}, \quad (4)$$

$$\beta_k(s) \cong \beta_{ok} = 1 - \varepsilon_{\beta_{vk}}, \quad (5)$$

where $\varepsilon_{\alpha_{ij}}$ and $\varepsilon_{\beta_{vk}}$ are the current and voltage tracking errors, whereas $|\varepsilon_{\alpha_{ij}}| \ll 1$ and $|\varepsilon_{\beta_{vk}}| \ll 1$, respectively.

The basic idea for implementation of the proposed VGC-MCFOA is shown in Fig. 1(b), where the OTA_1 and OTA_2 are used to control the voltage gain h and two CCII+/– represent the conventional MCFOA. Subsequently, the bipolar implementation of the VGC-MCFOA is shown in Fig. 1(c). The voltage gain control stage is formed by two simple differential pair amplifiers (transistors Q_1–Q_6) and transistors Q_7–Q_{32} form the two CCII+/– based MCFOA, respectively. Here it is worth mentioning that the voltage gain control of VCG-CCII [29] was implemented using the same technique. For the implementation in Fig. 1(b) the voltage gain h can be expressed as:

$$h = \frac{g_{m_{1,2}}}{g_{m_{5,6}}}, \quad (6)$$

where $g_{m_{1,2}} = \frac{I_{\mathrm{B1}}}{2V_{\mathrm{T}}}$ and $g_{m_{5,6}} = \frac{I_{\mathrm{B2}}}{2V_{\mathrm{T}}}$. Here, the V_{T} is the thermal voltage (approximately 26 mV at 27°C) and the I_{B1} and I_{B2} are control currents adjusting the transconductances $g_{m_{1,2}}$ and $g_{m_{5,6}}$, respectively. Therefore, the voltage gain h in (6) can be given as:

$$h = \frac{I_{\mathrm{B1}}}{I_{\mathrm{B2}}}. \quad (7)$$

From (7) it is obvious that the proposed VGC-MCFOA can be easily adjusted electronically by either I_{B1} and/or I_{B2} currents.

III. Proposed All-Pass Filter

A. Ideal Case Study

The proposed four-mode APF is shown in Fig. 2. Considering the ideal VGC-MCFOA (i.e. α_j and β_k are unity), based on the input selected two following cases can be considered:

$Case\ I$: If $I_{in1} = I_{in2} = I_{in}$, $V_{in} = 0$ (grounded), and assuming $R_2 = R_3 = R$, then we can obtain the following transfer functions (TFs):

$$T_{\mathrm{CM}}(s) = \frac{I_{out}}{I_{in}} = \frac{sCR_1 - h}{sCR_1 + h} = \frac{I_{\mathrm{B2}}sCR_1 - I_{\mathrm{B1}}}{I_{\mathrm{B2}}sCR_1 + I_{\mathrm{B1}}}, \quad (8)$$

$$T_{\mathrm{TIM}}(s) = \frac{V_{out}}{I_{in}} = R \cdot \frac{sCR_1 - h}{sCR_1 + h} = R \cdot \frac{I_{\mathrm{B2}}sCR_1 - I_{\mathrm{B1}}}{I_{\mathrm{B2}}sCR_1 + I_{\mathrm{B1}}}. \quad (9)$$

$Case\ II$: If the input of the APF is V_{in}, $I_{in1} = I_{in2} = 0$, and assuming $R_1 = R_2 = R$, then for the circuit the following TFs can be obtained:

$$T_{\mathrm{TAM}}(s) = \frac{I_{out}}{V_{in}} = -\frac{1}{R} \cdot \frac{sCR_3 - h}{sCR_3 + h} = -\frac{1}{R} \cdot \frac{I_{\mathrm{B2}}sCR_3 - I_{\mathrm{B1}}}{I_{\mathrm{B2}}sCR_3 + I_{\mathrm{B1}}}, \quad (10)$$

$$T_{\mathrm{VM}}(s) = \frac{V_{out}}{V_{in}} = -\frac{sCR_3 - h}{sCR_3 + h} = -\frac{I_{\mathrm{B2}}sCR_3 - I_{\mathrm{B1}}}{I_{\mathrm{B2}}sCR_3 + I_{\mathrm{B1}}}. \quad (11)$$

Thus, from Eqs. (8)–(11) it is seen that by suitable selection of input and output all four possible modes, i.e. current-, transimpedance-, transadmittance-, and voltage-mode first-order APF can be realized with the same circuit topology.

The phase responses of TFs in (8) and (9) are calculated as follows:

$$\varphi_{\mathrm{CM}}(\omega) = \varphi_{\mathrm{TIM}}(\omega) = 180^\circ - 2\mathrm{arctg}\left(\frac{1}{h} \cdot \omega CR_1\right) = \\ = 180^\circ - 2\mathrm{arctg}\left(\frac{I_{\mathrm{B2}}}{I_{\mathrm{B1}}} \cdot \omega CR_1\right), \quad (12)$$

and phase responses of TFs in (10) and (11) are given as:

$$\varphi_{\mathrm{TAM}}(\omega) = \varphi_{\mathrm{VM}}(\omega) = -2\mathrm{arctg}\left(\frac{1}{h} \cdot \omega CR_3\right) = \\ = -2\mathrm{arctg}\left(\frac{I_{\mathrm{B2}}}{I_{\mathrm{B1}}} \cdot \omega CR_3\right). \quad (13)$$

Hence, the phases of TFs in (8) and (9) alter from 180° to 0° while according to (10) and (11) the phase shift change between 0° to –180°, respectively.

Consequently, the zero (ω_z) and pole (ω_p) frequencies of all four TFs can be found as:

$$\omega_{(\mathrm{CM,TIM})z} = \omega_{(\mathrm{CM,TIM})p} = h \cdot \frac{1}{CR_1} = \frac{I_{\mathrm{B1}}}{I_{\mathrm{B2}}} \cdot \frac{1}{CR_1}, \quad (14)$$

$$\omega_{(\mathrm{TAM,VM})z} = \omega_{(\mathrm{TAM,VM})p} = h \cdot \frac{1}{CR_3} = \frac{I_{\mathrm{B1}}}{I_{\mathrm{B2}}} \cdot \frac{1}{CR_3}. \quad (15)$$

From Eqs. (14) and (15) it is clearly seen that the pole/zero frequency values can be easily tuned by means of the bias currents I_{B1} and/or I_{B2}.

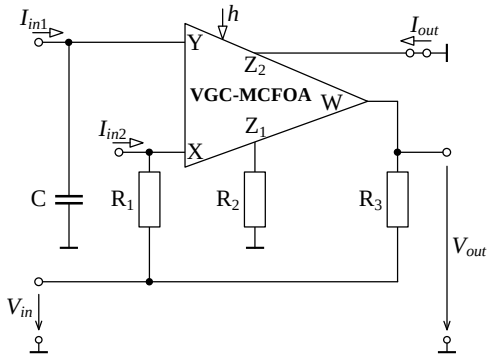


Fig. 2. Proposed electronically tunable all-pass filter using VGC-MCFOA

B. Non-Ideal Analysis

Taking into account non-idealities of the VGC-MCFOA, TFs (8) and (9) in $Case\ I$ of the filter convert to:

$$T_{\mathrm{CM}}(s) = \frac{I_{out}}{I_{in}} = \alpha_3 R_3 \cdot \frac{sCR_1 - \beta_1 h}{sCR_1R_3 + \alpha_1\alpha_2\beta_1\beta_2 hR_2} = \\ = \alpha_3 R_3 \cdot \frac{I_{\mathrm{B2}}sCR_1 - I_{\mathrm{B1}}\beta_1}{I_{\mathrm{B2}}sCR_1R_3 + I_{\mathrm{B1}}\alpha_1\alpha_2\beta_1\beta_2R_2}, \quad (16)$$

$$T_{\mathrm{TIM}}(s) = \frac{V_{out}}{I_{in}} = \frac{\alpha_2\beta_2R_2R_3 \cdot (sCR_1 - h\beta_1)}{sCR_1R_3 + \alpha_1\alpha_2\beta_1\beta_2hR_2} = \\ = \frac{\alpha_2\beta_2R_2R_3 \cdot (I_{\mathrm{B2}}sCR_1 - I_{\mathrm{B1}}\beta_1)}{I_{\mathrm{B2}}sCR_1R_3 + I_{\mathrm{B1}}\alpha_1\alpha_2\beta_1\beta_2R_2}, \quad (17)$$

and non-ideal phase responses from TFs (16) and (17) can be expressed as:

$$\varphi_{\mathrm{CM}}(\omega) = \varphi_{\mathrm{TIM}}(\omega) = 180^\circ - \mathrm{arctg}\left(\frac{I_{\mathrm{B2}}}{I_{\mathrm{B1}}} \cdot \frac{\omega CR_1}{\beta_1}\right) - \\ -\mathrm{arctg}\left(\frac{I_{\mathrm{B2}}}{I_{\mathrm{B1}}} \cdot \frac{\omega CR_1R_3}{\alpha_1\alpha_2\beta_1\beta_2R_2}\right). \quad (18)$$

The zero and pole frequencies in Eq. (14) change to:

$$\omega_{(\mathrm{CM,TIM})z} = \frac{I_{\mathrm{B1}}}{I_{\mathrm{B2}}} \cdot \frac{\beta_1}{CR_1},\ \omega_{(\mathrm{CM,TIM})p} = \frac{I_{\mathrm{B1}}}{I_{\mathrm{B2}}} \cdot \frac{\alpha_1\alpha_2\beta_1\beta_2R_2}{CR_1R_3}. \quad (19)$$

From Eq. (19), the active and passive sensitivities of zero and pole frequencies are given as:

$$S^{\omega_{(\mathrm{CM,TIM})z}}_{I_{\mathrm{B1}},\beta_1} = -S^{\omega_{(\mathrm{CM,TIM})z}}_{I_{\mathrm{B2}},C,R_1} = 1,\ S^{\omega_{(\mathrm{CM,TIM})z}}_{\alpha_1,\alpha_2,\alpha_3,\beta_2,R_2,R_3} = 0, \quad (20)$$

$$S^{\omega_{(\mathrm{CM,TIM})p}}_{I_{\mathrm{B1}},\alpha_1,\alpha_2,\beta_1,\beta_2,R_2} = -S^{\omega_{(\mathrm{CM,TIM})p}}_{I_{\mathrm{B2}},C,R_1,R_3} = 1,\ S^{\omega_{(\mathrm{CM,TIM})p}}_{\alpha_3} = 0, \quad (21)$$

and it is evident that the sensitivities of active parameters and passive components for $\omega_{(\mathrm{CM,TIM})z}$ and $\omega_{(\mathrm{CM,TIM})p}$ are at maximum unity in relative amplitude. The same study can also be done for the $Case\ II$ with similar results.

IV. Simulation Results

First, the proposed VGC-MCFOA in Fig. 1(c) has been further investigated in SPICE software. In the design the transistor model parameters NR100N (NPN) and PR100N (PNP) of bipolar arrays ALA400-CBIC-R from AT&T were used

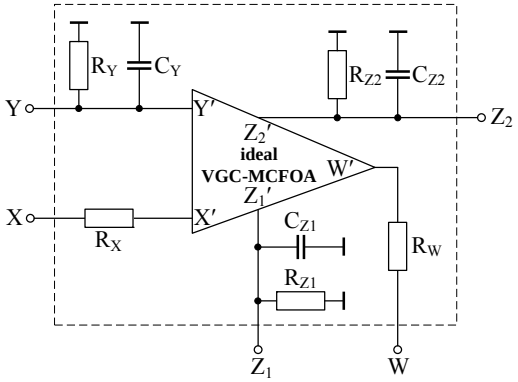


Fig. 3. Model of the VGC-MCFOA including parasitic elements

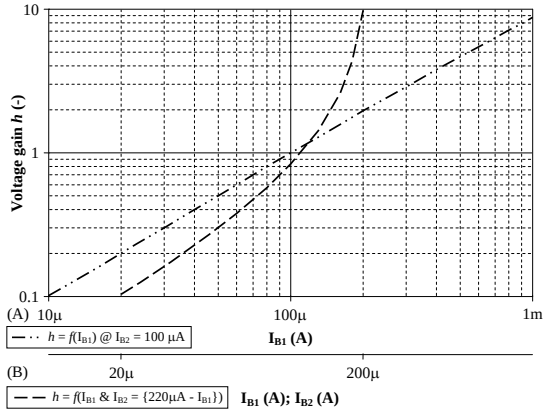


Fig. 4. Voltage gain h responses vs. applied bias currents

TABLE I
PARAMETERS OF VGC-MCFOA SHOWN IN FIG. 1(C) (NOTE: # AT $h = 1$)

Parameters	Values
$i_{\rm Y}/i_{\rm W}$ gain (α_1)	1.001
$v_{\rm X}/v_{\rm Y}$ gain (β_1)#	0.995
$i_{\rm Z1}/i_{\rm X}$ gain (α_2)	0.982
$i_{\rm Z2}/i_{\rm X}$ gain (α_3)	1.001
$v_{\rm W}/v_{\rm Z1}$ gain (β_2)	0.999
$i_{\rm Y}/i_{\rm W}$ $f_{-3\rm dB}$	49.16 MHz
$v_{\rm X}/v_{\rm Y}$ $f_{-3\rm dB}$#	108.15 MHz
$i_{\rm Z1}/i_{\rm X}$ $f_{-3\rm dB}$	89.22 MHz
$i_{\rm Z2}/i_{\rm X}$ $f_{-3\rm dB}$	67.34 MHz
$v_{\rm W}/v_{\rm Z1}$ $f_{-3\rm dB}$	879.47 MHz
$R_{\rm Y}$	55.35 kΩ
$C_{\rm Y}$	1.919 pF
$R_{\rm X}$	42.01 Ω
$R_{\rm W}$	36.96 Ω
$R_{\rm Z1}$	94.31 kΩ
$C_{\rm Z1}$	2.047 pF
$R_{\rm Z2}$	97.61 kΩ
$C_{\rm Z2}$	1.272 pF

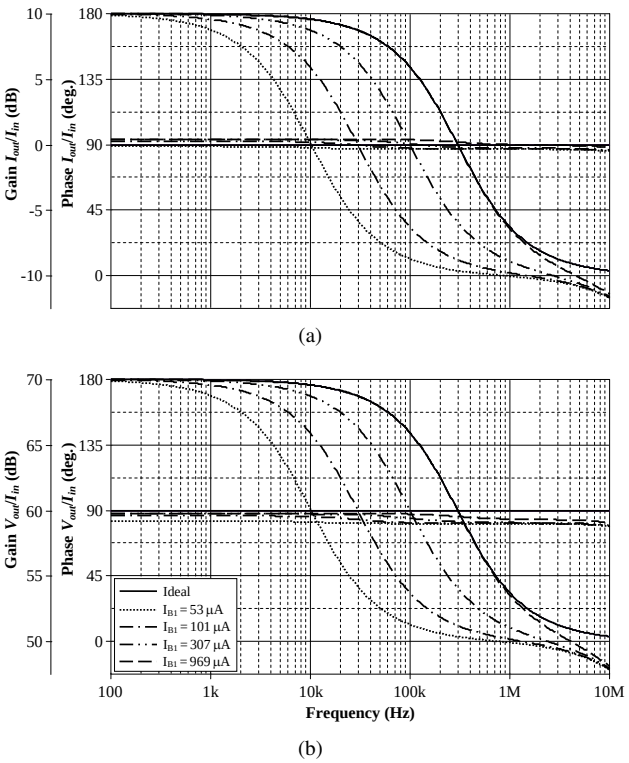


Fig. 5. Electronical tunability of the pole frequency by bias current $I_{\rm B1}$ based on case (A) at constant $I_{\rm B2} = 100$ μA: (a) current-mode, (b) transimpedance-mode first-order APF responses

[31]. The DC supply voltages are $+V_{\rm CC} = -V_{\rm EE} = 2.5$ V. Bias current $I_{\rm O}$ = 400 μA has been chosen and $I_{\rm B1}$, $I_{\rm B2}$ were set to 101 μA and 100 μA, respectively, to obtain voltage gain $h = 1$ precisely. The maximum values of terminal voltages and terminal currents without producing significant distortion were determined to be $\pm$106.7 mV and $\pm$16.23 mA, respectively. Evaluated DC current and voltage gains, $f_{-3\rm dB}$ frequencies of transfers, and values of the X and W terminal parasitic resistances (in series) and Z and Y terminal parasitic resistances and capacitances (in parallel) shown in Fig. 3 are given in Table I. The total power dissipation of the proposed VGC-MCFOA was found to be 23.1 mW.

Simulated voltage gain h responses between Y and X terminals is demonstrated in Fig. 4. In case of (A), the external bias current $I_{\rm B1}$ has been varied in large interval from 10 μA to 1 mA (equal to gain h = 0.1 to 10) at constant $I_{\rm B2} = 100$ μA. From Fig. 4 it can be clearly seen that due to the above mentioned non-idealities of the VGC-MCFOA, the obtained voltage gain is in reduced range 0.101÷8.71. Hence, to overcome the the large variation of control current $I_{\rm B1}$ and simultaneously obtain the same gain range i.e. h = 0.1 to 10, the control current $I_{\rm B1}$ has been varied in reduced interval from 20 μA to 200 μA together with $I_{\rm B2}$ according to Eq. $\{220$ μA$-I_{\rm B1}\}$. In this case (B), the obtained voltage gain is in range 0.102÷9.869, which is much closer to the theoretical one.

Using the bipolar implementation of the VGC-MCFOA the proposed APF from Fig. 2 has also been simulated in the SPICE software. The ideal and simulated gain and phase responses and electronical tunability of both current- and transimpedance-mode transfers based on case (A) discussed above i.e. by the bias current $I_{\rm B1}$ at constant $I_{\rm B2} = 100$ μA, are demonstrated in Fig. 5. In the simulations the passive element values were selected as $C = 5$ nF, $R_1 = R_2 = R_3 =$ 1 kΩ and the voltage gain h has been varied as h = {0.53; 1;

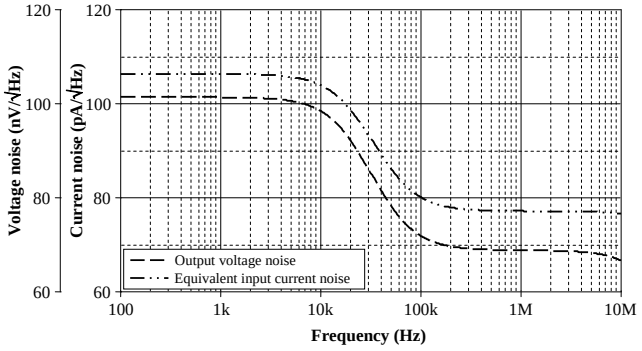


Fig. 6. Output and equivalent input noise variations vs. frequency at $h = 1$ ($f_0 = 29.9$ kHz) for the transimpedance-mode first-order APF response

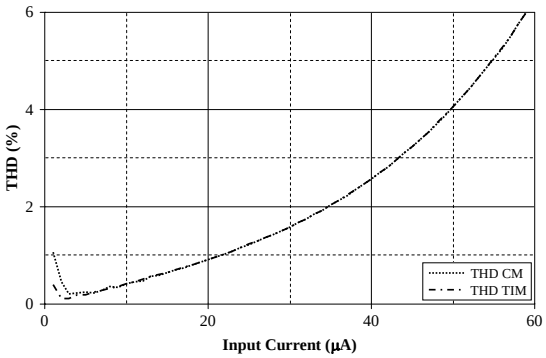


Fig. 7. THD variation of the proposed APF for both current- and transimpedance-mode responses against applied input current at $f_0 = 29.9$ kHz

2.95; 8.46} to set the pole frequency of the proposed circuit as $f_0 \approx \{10.2; 29.9; 100; 300\}$ kHz. Using the INOISE and ONOISE statements, the input and output noise behavior with respect to frequency has also been simulated, as it is shown in Fig. 6. The output noise and equivalent input noise at pole frequency ($f_0 \cong 29.9$ kHz) were found as 86.13 nV/$\sqrt{\text{Hz}}$ and 93.38 pA/$\sqrt{\text{Hz}}$, respectively. The THD variation for both responses with respect to amplitude of the applied sinusoidal input current at pole frequency of 29.9 kHz (filter parameter: $I_{\text{B1}} = 101$ μA) is shown in Fig. 7. An input with the amplitude of 30 μA yields for both responses THD values of 1.59%. From the simulations it is evident that the gain and phase characteristics of the filter are in good agreement with theory and the deviations are caused by the non-idealities of the active element used.

V. Conclusion

In this paper, a novel ABB called voltage gain-controlled MCFOA, which joins the voltage gain control feature of the voltage and current gain CCII in the conventional MCFOA. The usefulness of the tunable feature in the introduced VGC-MCFOA is demonstrated in four-mode first-order all-pass filter design. Since the capacitor in the circuit is grounded, the proposed filter is attractive for integration. The pole frequency can successfully be tuned in wide frequency range by means of external bias currents. The SPICE simulations confirm the theoretical assumptions.

Acknowledgment

Ing. Norbert Herencsár, Ph.D. was supported by the project CZ.1.07/2.3.00/30.0039 of Brno University of Technology. Research described in this paper was also in part supported by the project SIX CZ.1.05/2.1.00/03.0072 from the operational program Research and Development for Innovation, BUT Fund No. FEKT–S–11–15, and Czech Science Foundation projects under No. P102/11/P489, P102/10/P561, P102/09/1681.

A preliminary version of this paper has been presented at the 13th Int. Conf. on Optimization of Electrical and Electronic Equipment (OPTIM 2012) [32].

References

[1] A. S. Sedra and K. C. Smith, "A second-generation current conveyor and its applications," *IEEE Trans. Circuit Theory*, vol. 17, no. 1, pp. 132–134, 1970.

[2] K. C. Smith and A. S. Sedra, "Realization of the Chua family of new nonlinear network elements using the current conveyor," *IEEE Trans. Circuit Theory*, vol. 17, pp. 137–139, 1970.

[3] E. Yuce, "On the implementation of the floating simulators employing a single active device," *AEU–Int. J. Electron. and Commun.*, vol. 61, no. 7, pp. 453–458, 2007.

[4] E. Yuce and S. Minaei, "A modified CFOA and its applications to simulated inductors, capacitance multipliers, and analog filters," *IEEE Trans. Circuits and Systems—I*, vol. 55, no. 1, pp. 254–263, 2008.

[5] N. Herencsar, J. Koton, K. Vrba, and O. Cicekoglu, "Single UCC-N1B 0520 device as a modified CFOA and its application to voltage- and current-mode universal filters," In *Proc. of the Int. Conf. on Applied Electronics - APPEL 2009*, Pilsen, Czech Republic, pp. 127–130, 2009.

[6] N. Herencsar, J. Koton, and K. Vrba, "Voltage-mode universal filters employing single modified current feedback operational amplifier (MCFOA)," In *Proc. of the 6th Int. Conf. on Electrical and Electronics Engineering - ELECO 2009*, Bursa, Turkey, pp. 83–87, 2009.

[7] E. Yuce, "Fully integrable mixed-mode universal biquad with specific application of the CFOA," *AEU–Int. J. Electron. and Commun.*, vol. 64, no. 4, pp. 304–309, 2010.

[8] J. A. Svoboda, L. McGory, and S. Webb, "Applications of a commercially available current conveyor," *Int. J. Electronics*, vol. 70, pp. 159-164, 1991.

[9] A. Fabre, O. Saaid, F. Wiest, and C. Boucheron, "High frequency applications based on a new current controlled conveyor," *IEEE Trans. Circuits and Systems—I*, vol. 43, pp. 82–91, 1996.

[10] W. Chiu, S. I. Liu, H. W. Tsao, J. J. Chen, "CMOS differential difference current conveyors and their applications," *IEE Proceedings—Circuits, Devices and Systems*, vol. 144, no. 2, pp. 91–96, 1996.

[11] D. Becvar, K. Vrba, V. Zeman, and V. Musil, "Novel universal active block: a universal current conveyor," In *Proc. of the IEEE Int. Symposium on Circuits and Systems - ISCAS 2000*, Geneva, Switzerland, pp. 471–474, 2000.

[12] J. Cajka, T. Dostal, and K. Vrba, "General view on current conveyors," *Int. J. of Circuit Theory and Applications*, vol. 32, pp. 133–138, 2004.

[13] N. Herencsar and K. Vrba, "Current conveyors-based circuits using novel transformation method," *IEICE Electron. Express*, vol. 4, no. 21, pp. 650–656, 2007.

[14] J. Jerabek and K. Vrba, "SIMO type low-input and high-output impedance current- mode universal filter employing three universal current conveyors," *AEU–Int. J. Electron. and Commun.*, vol. 64, no. 6, pp. 588–593, 2010.

[15] A. Zeki and A. Toker, "The dual-X current conveyor (DXCCII): a new active device for tunable continuous-time filters," *Int. J. Electronics*, vol. 89, pp. 913–923, 2002.

[16] C. Acar and S. Ozoguz, "A new versatile building block: current differencing buffered amplifier suitable for analog signal processing filters," *Microelectron. J.*, vol. 30, pp. 157–160, 1999.

[17] J. Koton, N. Herencsar, and K. Vrba, "KHN-equivalent voltage-mode filters using universal voltage conveyors," *AEU–Int. J. Electron. and Commun.*, vol. 65, no. 2, pp. 154–160, 2011.

[18] R. L. Geiger and E. Sanchez-Sinencio, "Active filter design using operational transconductance amplifiers: A tutorial," *IEEE Circuits Devices Mag.*, vol. 1, pp. 20-32, 1985.

[19] D. Biolek, "CDTA - building block for current-mode analog signal processing," In *Proc. of the 16th European Conf. on Circuit Theory and Design - ECCTD 2003*, Krakow, Poland, pp. 397–400, 2003.
[20] R. Prokop and V. Musil, "Modular approach to design of modern circuit blocks for current signal processing and new device CCTA," In *Proc. of the Seventh IASTED Int. Conf. on Signal and Image Processing - SIP 2005*, Anaheim, USA, pp. 494–499, 2005.
[21] N. Herencsar, K. Vrba, J. Koton, and I. Lattenberg, "The conception of differential-input buffered and transconductance amplifier (DBTA) and its application," *IEICE Electron. Express*, vol. 6, pp. 329–334, 2009.
[22] N. Herencsar, J. Koton, and K. Vrba, "Realization of current-mode KHN-equivalent biquad using current follower transconductance amplifiers (CFTAs)," *IEICE Trans. Fundamentals*, vol. E93-A, no. 10, pp. 1816–1819, 2010.
[23] U. E. Ayten, M. Sagbas, N. Herencsar, and J. Koton, "Novel floating general element simulators using CBTA," *Radioengineering*, vol. 21, no. 1, pp. 11–19, 2012.
[24] N. Herencsar, A. Lahiri, J. Koton, K. Vrba, and B. Metin, "Realization of resistorless lossless positive and negative grounded inductor simulators using single ZC-CCCITA," *Radioengineering*, vol. 21, no. 1, pp. 264–272, 2012.
[25] W. Surakampontorn and P. Thitimajshima, "Integrable electronically tunable current conveyors," *IEE Proceedings—G*, vol. 135, no. 2, pp. 71–77, 1988.
[26] S. Minaei, O. K. Sayin, and H. Kuntman, "A new CMOS electronically tunable current conveyor and its application to current-mode filters," *IEEE Trans. Circuits and Systems—I*, vol. 53, pp. 1448–1457, 2006.
[27] N. Herencsar, A. Lahiri, K. Vrba, and J. Koton, "An electronically tunable current-mode quadrature oscillator using PCAs," *Int. J. Electronics*, vol. 99, no. 5, pp. 609–621, 2012.
[28] A. Fabre and N. Mimeche, "Class A/AB second-generation current conveyor with controlled current gain," *Electron. Lett.*, vol. 30, no. 16, pp. 1267–1268, 1994.
[29] A. De Marcellis, G. Ferri, N. C. Guerrini, G. Scotti, V. Stornelli, and A. Trifiletti, "The VCG-CCII: a novel building block and its application to capacitance multiplication," *Analog Integr. Circ. and Signal Process.*, vol. 58, no. 1, pp. 55–59, 2009.
[30] E. Yuce, K. Pal, and S. Minaei, "A high input impedance voltage-mode all-pass/notch filter using a single variable gain current conveyor," *J. Circuits, Systems, and Computers*, vol. 17, pp. 827–834, 2008.
[31] D. R. Frey, "Log-domain filtering: an approach to current mode filtering," *IEE Proceedings—Circuits, Devices and Systems*, vol. 140, no. 6, pp. 406–416, 1993.
[32] N. Herencsar, J. Koton, K. Vrba, A. Lahiri, and B. Metin, "Novel dual-mode electronically tunable all-pass filter using voltage gain-controlled MCFOA," In *Proc. of the 13th Int. Conf. on Optimization of Electrical and Electronic Equipment - OPTIM 2012*, Brasov, Romania, pp. 1199–1202, May 2012. DOI: 10.1109/OPTIM.2012.6231848

Norbert Herencsar received the M.Sc. and Ph.D. degrees in Electronics & Communication and Teleinformatics from Brno University of Technology (BUT), Czech Republic, in 2006 and 2010, respectively. Currently, he is an Assistant Professor at the Department of Telecommunications, Faculty of Electrical Engineering and Communication, BUT. From September 2009 through February 2010 he was an Erasmus Exchange Student with the Department of Electrical and Electronic Engineering, Bogazici University, Istanbul, Turkey. His research interests include analog filters, current-mode circuits, tunable frequency filter design methods, and oscillators. He is an author or co-author of 25 research articles published in SCI-E international journals, 20 articles published in other journals, and 60 papers published in proceedings of international conferences. In 2011 and 2012, he received Rector Award in the University competition "Top 10 Excelence VUT" for the 9th and 9th most productive scientist at the BUT, category "Publications", respectively. Since 2008, Dr. Herencsar serves in the organizing and technical committee of the Int. Conf. on Telecommunications and Signal Processing (TSP). He is Senior Member of the IACSIT and Member of the IEEE, IAENG, and ACEEE.

Jaroslav Koton received the M.Sc. an Ph.D. degree in electrical engineering from the Brno University of Technology, Czech Republic, in 2006 and 2009, respectively. He is currently an Assistant Professor at the Department of Telecommunications of the Faculty of Electrical Engineering and Communication of Brno University of Technology, Czech Republic. His current research is focused on linear- and non-linear circuit designing methods with current or voltage conveyors, and current active elements. He is an author or co-author of about 125 research articles published in international journals or conference proceedings. Dr. Koton is a Member of IEEE and IACSIT.

Abhirup Lahiri received Bachelor of Engineering (B.E.) degree with the highest honors from the Division of Electronics and Communications, Netaji Subhas Institute of Technology (erstwhile, Delhi Institute of Technology), University of Delhi, India. His past research works include design of compact analog circuit solutions using novel voltage-mode and current-mode active elements. His current research interests include low-power and low-voltage analog circuit design and precision voltage and current reference generation. He has authored/co-authored more than thirty international journal/conference papers (including fifteen SCI/SCI-E publications) and has acted as a reviewer (by editor's invitation) for numerous international journals and conferences of repute. He served as a program committee member for the International Conference on Telecommunications and Signal Processing (TSP). He is an editorial board member of Radioengineering Journal for the years 2011-2012. His biography is included in Marquis Who's Who in the World 2011- (28th Edition).

Bilgin Metin received the B.Sc. degree in Electronics and Communication Engineering from Istanbul Technical University, Istanbul, Turkey in 1996 and the M.Sc. and Ph.D. degrees in Electrical and Electronics Engineering from Bogazici University, Istanbul, Turkey in 2001 and 2007 respectively. He is currently an Assistant Professor in the Management Information Systems Department of Bogazici University. His research interests include continuous time filters, analog signal processing applications, current-mode circuits, and information systems. He was given the best student paper award of ELECO'2002 conference in Turkey. He has over 25 articles in SCI and SCI-E indexed journals and 25 conference proceedings.

Kamil Vrba received the Ph.D. degree in Electrical Engineering in 1976, and the Prof. degree in 1997, both from the Technical University of Brno. Since 1990 he has been Head of the Department of Telecommunications, Faculty of Electrical Engineering and Computer Science, Brno University of Technology, Brno, Czech Republic. His research work is concentrated on problems concerned with accuracy of analog circuits and mutual conversion of analog and digital signals. In cooperation with AMI Semiconductor Czech, Ltd. (now ON Semiconductor Czech Republic, Ltd.) he has developed number of novel active function blocks for analog signal processing such as universal current conveyor (UCC), universal voltage conveyor (UVC), programmable current amplifier (PCA), digitally adjustable current amplifier (DACA), and others. He is an author or co-author of more than 700 research articles published in international journals or conference proceedings. Professor Vrba is a Member of IEEE and IEICE.

Schmitt Trigger with Controllable Hysteresis Using Current Conveyors

Jiri Misurec and Jaroslav Koton

***Abstract*—Active elements working in the current or mixed mode are still attractive for the design of analog functional blocks. The current conveyor (CC) was defined already in 1968. This paper deals with hysteresis comparators using second generation current conveyor. The comparator is basically a pulse circuit. In these circuits, the maximum rate of change in the output voltage is required during switching from one state to another. In comparators with operational amplifiers the switching time is given by the slew rate of the operational amplifier used, which is not too high. If a current conveyor is used, the time of switching the comparator gets shorter. The comparator is capable to operate at a higher frequency bands and if it is used, for example, in converters, a higher operating frequency can be reached. The connection of an inverting and a non-inverting comparator with adjustable hysteresis is shown as a practical implementation. Using the AD844, results of experimental measurements are presented that confirm the theoretical assumptions and the results of computer simulation.**

***Keywords*—Current conveyor, analog circuit design, hysteresis comparator.**

I. Introduction

The current conveyors as active elements are known since 1968 [1], when Smith and Sedra presented the first-generation current conveyor (CCI). Later on the the second- and third-generation current conveyors have been designed [2], [3]. These elements are now with advantage used in applications, where the wide bandwidth or current output response is necessary. Nowadays, different types of current conveyors are described that are mostly based on the CCII, e.g. current controlled CC (CCCII) [17], differential voltage CC (DVCC) [18], or electronically tunable CC (ECCII) [19], [20].

The application possibilities of current conveyors are mostly presented on linear circuit design, e.g. frequency filters [4]–[7] or immittace simulators [8]–[11]. However, the CCII can be used to implement other functional blocks, such as Schmitt trigger circuit, by creating a regenerative feedback that takes part of the output voltage from terminal Z and applies it to the Y terminal of the active element [12], [13]. Schmitt Triggers based on other active elements such as Current Through Transconductance Amplifier (CTTA) or Current Differencing Transconductance Amplifier (CDTA) can be found e.g. in [14], [15].

In this paper we use simple second-generation current conveyors to implement Schmitt trigger with inverting and non-inverting hysteresis loop. First basic circuit topology is described that is subsequently supplemented by and digital-to analog converter with reference input enabling digital control the value of hysteresis of the Schmitt trigger. The behavior of the proposed circuit is analyzed both by SPICE simulations and experimental measurements showing the performance of the Schmitt trigger.

J. Misurec and J. Koton are with the Department of Telecommunications, Brno University of Technology, Purkynova 118, 612 00 Brno, Czech Republic. Corresponding author: misurec@feec.vutbr.cz.

Manuscript received July 5, 2012; revised September 29, 2012.

II. Second-generation Current Conveyor and Its Implementation

Generally, in the second-generation of current conveyors, terminal Y is only a voltage terminal having infinite input impedance in theory. The X port is the current input and the current transfer from port X to port Y is zero, from X to Z it is unity. A three-port is involved here (see Fig. 1), the matrix representation of which is given by relations:

$$\begin{bmatrix} V_{\mathrm{X}} \\ I_{\mathrm{Y}} \\ I_{\mathrm{Z}} \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} I_{\mathrm{X}} \\ V_{\mathrm{Y}} \\ V_{\mathrm{Z}} \end{bmatrix}. \tag{1}$$

Its advantageous properties and application possibilities have grown with the development of circuits and systems in the current mode. Second-generation current conveyors have come to feature prominently in circuit structures of some commercially manufactured circuits. The AD844 circuit is a transimpedance amplifier (Analog Devices). In its internal structure there is a CCII+ second-generation current conveyor. A high-impedance outlet is important here, which is used as port z of the CCII+ conveyor. The internal connection of the circuit is shown in Fig. 2(a), the schematic symbol of the AD844 circuit in the PSpice program is in Fig. 2(b), and the ideal model is in Fig. 2(c).

It is evident from the equivalent circuit connection that its internal connection consists of two voltage followers and one current follower. Current I_{IN} flows via input resistance $\mathrm{R_{IN}}$ (the input resistance of low-impedance terminal is ca. 50 Ω). This current is detected by the current follower and transferred to the transimpedance terminal.

The current passage through the so-called transimpedance produces a voltage, which is conveyed to the compensation terminal. On this terminal the output current I_{Z} of the current conveyor is obtained too. For the sake of load separation

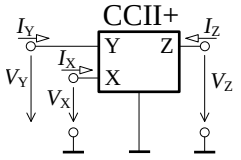


Fig. 1. Schematic symbol of CCII+ second-generation current conveyor

a voltage follower is included on the voltage output of transimpedance amplifier. However, in the case of current conveyor the voltage output is not made use of. The transimpedance models the impedance of output terminal Z and is formed by a parallel combination of resistance R_t (its magnitude is ca. 3 MΩ) and capacitance C_t (cca. 4.5 pF). The output impedance of the transimpedance terminal of this current source is high.

The output circuits of comparators are in the nature of pulse circuits and thus a maximum rate of change in the output voltage is usually required in comparison. This parameter has a direct influence on the switching time. In the classical comparator with operational amplifier the switching time is given by the slew rate of the operational amplifier used. In comparators with current conveyors the switching time should be substantially shorter.

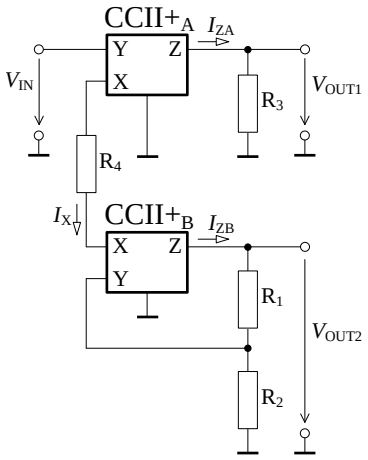


Fig. 3. Non-inverting and inverting hysteresis comparator with two CCII+s

III. Hysteresis comparator with CCII+

Similarly as in [12], transimpedance amplifiers AD844 [16] including CCII+ were used to implement the comparator. The schematic diagram of a hysteresis comparator implemented using two CCII+ conveyors is shown in Fig. 3.

From the connection of non-inverting hysteresis comparator with operational amplifier the equivalent connection of non-inverting or inverting hysteresis comparator with CCII+ can be derived. The connection given in Fig. 3 combines two possibilities. The circuit part containing the CCII+$_A$ current conveyor represents the non-inverting hysteresis comparator while the part containing the CCII+$_B$ current conveyor performs the function of an inverting hysteresis comparator. Then output voltage V_{OUT1} is the output of the non-inverting hysteresis comparator, and output voltage V_{OUT2} is the output of inverting hysteresis comparator.

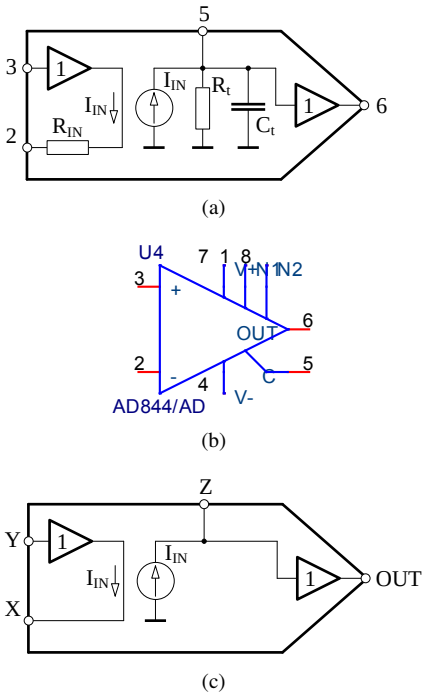


Fig. 2. (a) Internal connection of circuit AD844 [16], (b) symbol of circuit AD844 in PSpice program, (c) idealized model of circuit AD844

To describe the activity and determine the values of positive comparison voltage $+V_P$ and negative comparison voltage $-V_N$ of the comparator from Fig. 3 we will start from the knowledge of CCII+ in the AD844 circuit as given above. In this case the most important parameter of CCII+ is the magnitude of the transimpedance formed by a parallel connection of resistance R_t and capacitance C_t. These elements form the impedance of output terminal Z. The output resistance R_X of low-impedance terminal X also needs to be taken into consideration.

Consider that the output voltage V_{OUT1} can acquire values $+V_{OUT\_SAT}$ or $-V_{OUT\_SAT}$, with the output voltage V_{OUT2} always acquiring the opposite values, i.e. $-V_{OUT\_SAT}$ and $+V_{OUT\_SAT}$. The outputs V_{OUT1} and V_{OUT2} are mutually complementary.

Consider that the output voltage V_{OUT2} of conveyor CCII+$_B$ has a maximum positive level, i.e. $V_{OUT2} = +V_{OUT\_SAT}$, in which case the voltage $+V_P$ on port Y of current conveyor CCII+$_B$ is given by the relation:

$$+V_P = +V_{OUT\_SAT}\frac{R_2}{R_1+R_2} = +V_{OUT\_SAT}\beta. \qquad (2)$$

If on the contrary there is on the output of conveyor CCII+$_B$ a minimum negative level, $V_{OUT2} = -V_{OUT\_SAT}$, then the voltage on port Y of this conveyor is:

$$-V_N = -V_{OUT\_SAT}\frac{R_2}{R_1+R_2} = -V_{OUT\_SAT}\beta. \qquad (3)$$

By the definition of current conveyor CCII+ it holds that $V_X = V_Y$, so that the voltage on port Y will be repeated also on port X of CCII+$_B$. Therefore, the current flowing into terminal X can be expressed as:

$$I_X = \frac{V_{IN} - V_{OUTSAT}\beta}{2R_X + R_4}. \qquad (4)$$

From the conveyor definition it further follows that the output current of conveyor CCII+$_A$ is $I_{ZA} = I_X$, and the output current of conveyor CCII+$_B$ is $I_{ZB} = -I_X$. The output voltage

of conveyor CCII+$_{\rm A}$ is then given by the relation:

$$V_{\rm ZA} = V_{\rm OUT1} = \frac{V_{\rm IN} - V_{\rm OUT\_SAT}\beta}{2R_{\rm X} + R_4} \frac{R_{\rm t}}{1 + sR_{\rm t}C_{\rm t}} \qquad (5)$$

and the output voltage of conveyor CCII+$_{\rm B}$ is:

$$V_{\rm ZB} = V_{\rm OUT2} = -\frac{V_{\rm IN} - V_{\rm OUT\_SAT}\beta}{2R_{\rm X} + R_4} \frac{R_{\rm t}}{1 + sR_{\rm t}C_{\rm t}}, \qquad (6)$$

where $s = {\rm j}\omega$, whereas ω is the angular frequency. Simplified relations can be obtained in the form of

$$V_{\rm ZA} = V_{\rm OUT1} = \frac{R_{\rm t}}{2R_{\rm X} + R_4} \left(V_{\rm IN} \mp V_{\rm OUT\_SAT}\beta\right), \qquad (7)$$

$$V_{\rm ZB} = V_{\rm OUT2} = -\frac{R_{\rm t}}{2R_{\rm X} + R_4} \left(V_{\rm IN} \mp V_{\rm OUT\_SAT}\beta\right), \qquad (8)$$

where the negative sign "–"and positive sign "+"within the parentheses denote the state of comparator output voltages $V_{\rm OUT1}$ and $V_{\rm OUT2}$. If $V_{\rm OUT1} = -V_{\rm OUT\_SAT}$, then $V_{\rm OUT2} = +V_{\rm OUT\_SAT}$, and if $V_{\rm OUT1} = +V_{\rm OUT\_SAT}$ then $V_{\rm OUT2} = -V_{\rm OUT\_SAT}$.

After switching the conveyor outputs to the values $V_{\rm OUT1} = -V_{\rm OUT\_SAT}$ and $V_{\rm OUT2} = +V_{\rm OUT\_SAT}$ the input voltage $V_{\rm IN}$ must drop below the value $-V_{\rm OUT\_SAT}\beta$. The comparator hysteresis is defined as the difference between the positive and the negative comparison level of input voltage and is thus given by the relation:

$$h = +V_{\rm P} - (-V_{\rm N}) = +V_{\rm OUT\_SAT}\beta - (-V_{\rm OUT\_SAT}\beta) = \\ = 2\beta V_{\rm OUT\_SAT}. \qquad (9)$$

IV. Computer Simulation of Hysteresis Comparator with CCII+

The operation of the comparator from Fig. 3 was tested in computer simulation. In the MicroCap simulation program the model of the AD844AD circuit will be used. The circuit parameters set for the simulation were: supply voltage $V_{\rm CC} = \pm 15$ V, saturation voltage $V_{\rm OUT\_SAT} = 10$ V, the resistance values chosen are $R_1 = R_2 = 10$ kΩ, consequently $\beta = 0.5$, $R_3 = 20$ kΩ, and $R_4 = 1$ kΩ. The calculated value of comparison voltage is $+V_{\rm P} = 5$ V and the comparator hysteresis is then $h = 10$. For the chosen $V_{\rm IN} = 10$ V the output current magnitudes of the two current conveyors are $I_{\rm ZA} = 4.5$ mA and $I_{\rm ZB} = -4.5$ mA.

Simulation results are given for non-inverting comparator in Fig. 4(a), and for inverting comparator in Fig. 4(b). Arrowheads in the waveforms follow the direction of the change in input voltage $V_{\rm IN}$. As can be seen, the circuit performs the expected function. The circuit part containing the CCII+$_{\rm B}$ fulfills the function of inverting hysteresis comparator, the part with CCII+$_{\rm A}$ performs the function of non-inverting hysteresis comparator.

V. Digital Control of Hysteresis and Experimental Measurements

For the digital control of hysteresis magnitude the comparator connection including a CCII+ was proposed as given in Fig. 5. The initial basic connection given in Fig. 3 was complemented with a multiplier with digital-to-analog converter AD7533 [21], operational amplifier LM741 (which is connected as a voltage follower), and a third CCII+ current conveyor AD844. Voltage from the divider R_1-R_2 is conveyed to the multiplier, where it is multiplied by the value of a 10-bit input word *D*, which sets the hysteresis magnitude. Therefore, it is necessary to multiply the relations (2), (3) and (9) by the value *D*. The value *D* expresses the binary fraction value of 10-bit digital input word DAC; examples of calculating *D* for some of the combinations are given in Table I. In the comparator connection implemented, hysteresis can be set in an interval $h = 0$ V to $h = 12.125$ V, in dependence on the set combination of 10-bit digital word *D*.

The measured waveforms for the control word $D = 1111111111$ is given in Fig. 6. For this value of the number *D* the maximum value of comparator hysteresis is obtained, $h = 12.125$ V. For $D = 1000000000$ the waveform is shown in Fig. 7 while for $D = 0000000001$ it is shown in

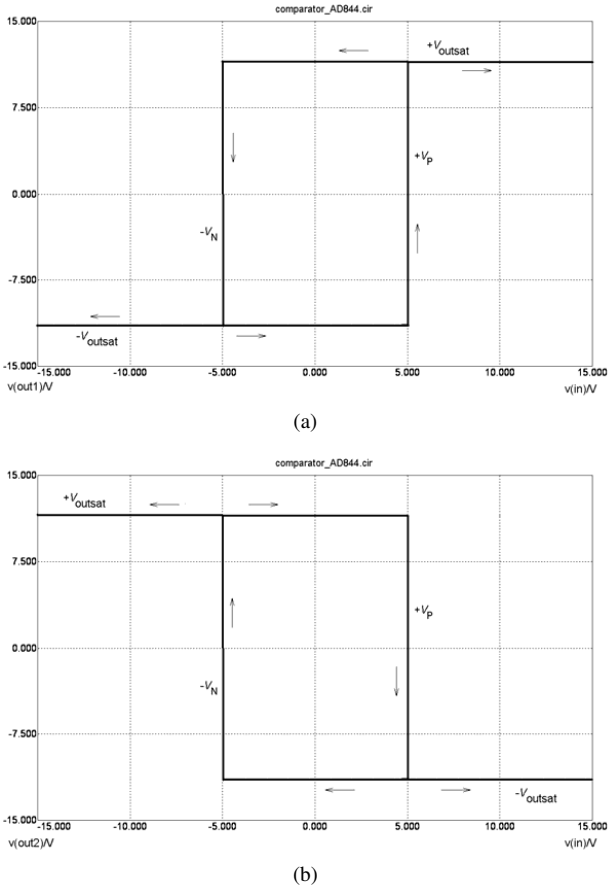


Fig. 4. (a) non-inverting, (b) inverting waveform of hysteresis characteristic of comparator from Fig. 3

TABLE I
BINARY FRACTION REPRESENTATION OF SOME COMBINATIONS OF 10-BIT DAC INPUT DIGITAL INPUT BINARY FRACTION VALUE

Digital input (MSB → LSB)	Binary fraction value
1111111111	1023/1024
1000000001	513/1024
1000000000	512/1024
0111111111	511/1024
0000000001	1/1024
0000000000	0/1024

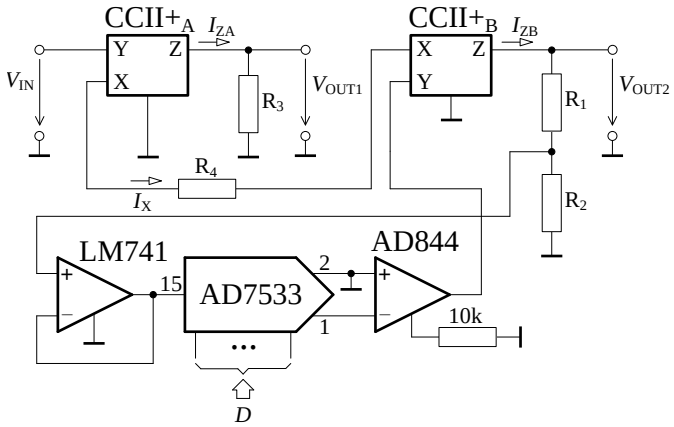
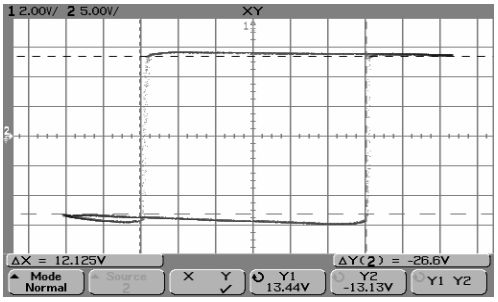
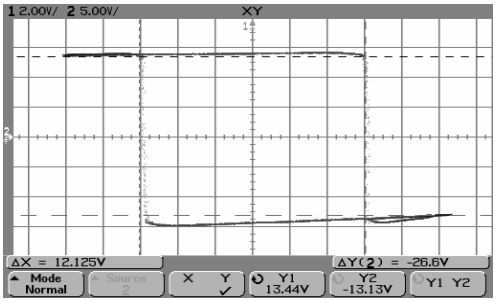


Fig. 5. Design schematic of comparators with variable hysteresis

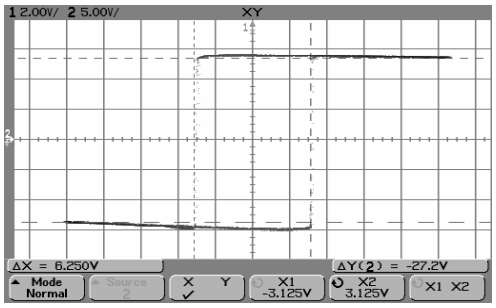


(a)

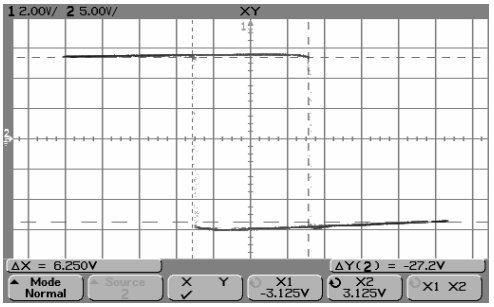


(b)

Fig. 6. Hysteresis loop for $D = 1111111111$, (a) non-inverting comparator (b) inverting comparator

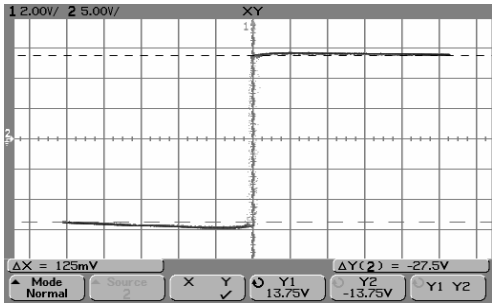


(a)

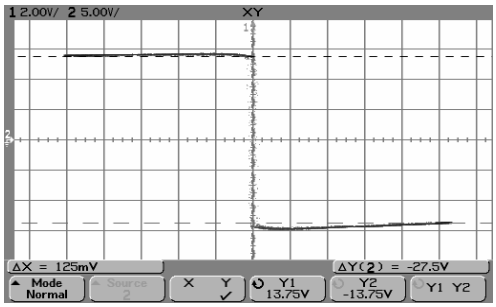


(b)

Fig. 7. Hysteresis loop for $D = 1000000000$, (a) non-inverting comparator (b) inverting comparator



(a)

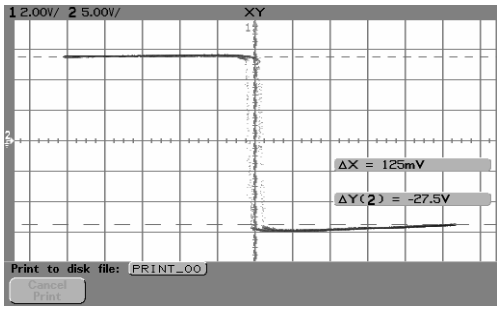


(b)

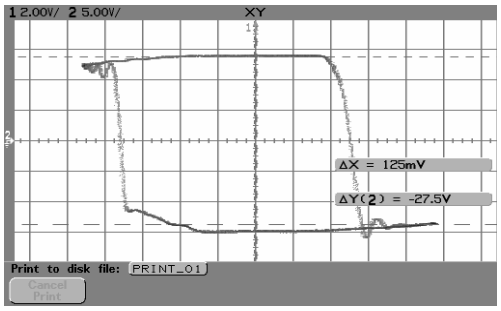
Fig. 8. Hysteresis loop for $D = 0000000001$, (a) non-inverting comparator (b) inverting comparator

Fig. 8. The value of hysteresis h in the comparator is given by the parameter of ΔX cursors in the left bottom corner while the parameter ΔY in the right bottom corner gives the value of $2V_{\mathrm{OUT\_SAT}}$. The testing input signal was a sinusoidal waveform of frequency 2.2 kHz.

With increasing frequency of the input signal the magnitude of the hysteresis value changes. The waveforms of output signal of inverting comparator at input signal frequency 5.5 kHz and D set to 0000000001 is given in Fig. 9(a) while Fig. 9(b) gives the waveform for input frequency 650 kHz. The two waveforms can be compared with the oscillograms given in Fig. 8(b). For the above value of input word D the hysteresis should be $h = 125$ mV but the actual hysteresis value is 300 mV. If the input signal frequency increases, the



(a)



(b)

Fig. 9. Hysteresis loop of inverting comparator for $D = 0000000001$, (a) frequency $f = 5.5$ kHz (b) frequency $f = 650$ kHz

hysteresis loop gets more extended and the dynamic properties of current conveyors come to be fully shown. At the time of switching, noticeable overshooting can be observed on the waveforms. This has a considerable effect on comparator precision, showing in the utilizable frequency band of comparator with AD844.

VI. Conclusion

The paper presents the solution of a voltage comparator with current conveyors CCII+. A theoretical analysis and computer simulation were performed and a digitally controlled inverting and non-inverting comparator has been proposed. The comparator has some pulse circuit elements and therefore a maximum rate of output voltage change is usually required. Measuring on an experimental specimen shows the results obtained. The values of hysteresis *h* measured for three chosen combinations of *D*, i.e. full extent of *h*, half the extent of *h*, and the least value of *h*, were compared with calculated values. The deviation from these values was cca. 3% for individual values of *D*. In the connection given, there is evidently a drop in voltage, obviously due to the AD7533 multiplier. Measuring the comparator without multiplier did not exhibit this error. Thus the good functionality of the comparator was verified and the advantage of the current mode was shown. Further work will focus on obtaining a higher operating frequency.

References

[1] K. C. Smith and A. Smith, "The Current Conveyor: a New Circuit Building Block,"*IEEE Proc.*, Vol. 56, pp. 1368-1369, 1968.

[2] A. Sedra and K. C. Smith, "A second-generation current conveyor and its application,"*IEEE Trans. Circuit Theory*, Vol. 17, pp. 132-134, 1970.

[3] A. Fabre, "Third-generation current conveyor: a new helpful active element,"*Electronics Letters*, Vol. 31, No. 5, pp. 338-339, 1995.

[4] M. Sagbas, K. Fidanboylu, and M. C. Bayram, "Triple-input Single-output Voltage-mode Multifunction Filter Using Only Two Current Conveyors", *Trans. Engineering, Computing and Technology*, Vol. 4, pp. 105-108, 2005.

[5] S. Minaei, O. K. Sayin, and H. Kuntman, "A new CMOS electronically tunable current conveyor and its application to current-mode filters", *Tran. Circuits and Systems I*, Vol. 53, pp. 1448-1457, 2006.

[6] S. A. Mahmoud, M. A. Hashiesh, and A. M. Soliman, "Digitally controlled fully differential current conveyor: CMOS realization and applications", in *Proc. IEEE Int. Symp. Circuits and Systems - ISCAS*, Vol. 2, pp. 1622-1625, 2005.

[7] P. Prommee, M. Somdunyakanok, and S. Toomsawasdi, "CMOS-based current-controlled DDCC and its applications", in *Proc. IEEE Int. Symp. Circuits and Systems - ISCAS*, pp. 1045-1048, 2010.

[8] S. Ozoguz and A. Acar, "On the realization of floating immittance function simulators using current conveyors", *Int. J. Electronics*, Vol. 85, No. 4, pp. 463-475, 1998.

[9] U. Cam, O. Cicekoglu, and H. Kuntman, "Universal series and parallel immittance simulators using four terminals floating nullors,"*Analog Integrated Circuit and Signal Processing*, Vol. 25, No. 1, pp. 5966, 2000.

[10] E. Arslan, B. Metin, C. Cakir, O. Cicekoglu, "A novel grounded lossless inductance simulator with CCI", in *Proc. Int. XII. Turkish Symposium on Artificial Inteligence and Neural Networks*, 2003.

[11] E. Yuce, S. Minaei, and O. Cicekoglu, "A novel grounded inductor realization using a minimum number of active and passive components", *ETRI Journal*, Vol. 27, pp. 427 - 432, 2005.

[12] S. Bima, A. Khan, S. Roy, and K. Dey, "Programmable Hysteresis Comparator Circuits using Current Conveyor,"*J. Instrum. Soc. India*, No. 32, pp.85-93, 1997.

[13] S. Del Re, A. De Marcellis, G. Ferri, and V. Stornelli, "Low voltage integrated astable multivibrator based on a single CCII", in *Proc. Research in Mincroelectronics and Electronics Conference*, pp. 177-180, 2007.

[14] P. Silapan and M. Siripruchyanun, "A Simple Current-mode Schmitt Trigger Employing Only Single MO-CTTA", in *Proc. 6th Int. Conf. Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology - ECTI-CON*, Vol. 01, pp. 556-559, 2009.

[15] P. Silapan and M. Siripruchyanun, "Fully and electronically controllable current-mode Schmitt triggers employing only single MO-CCCDTA and their applications ", *Analog Integr Circ Sig Process*, doi: 10.1007/s10470-010-9593-2, Vol. 68, pp. 111-128, 2011.

[16] Datasheet AD844: 60 MHz 2000V/μs Monolithic Op Amp, Analog Devices, Rev. F. 2009.

[17] A. Fabre, O. Saaid, F. Wiest, and C. Baucheron, High frequency applications based on a new current controlled conveyor, *IEEE Trans. Circuits Syst.-I*, Vol. 43, No. 2, pp. 82-90, 1996.

[18] H.O. Elwan and A.M. Soliman, Novel CMOS differential voltage current conveyor and its applications, *IEE Proc. Circuits, Devices, Systems*, Vol. 144, No. 3, pp. 195-200, 1997.

[19] S. Minaei, O.K. Sayin, and H. Kuntman, A new CMOS electronically tunable current conveyor and its application to current-mode filters, *IEEE Trans. Circuits Systems I*, Vol. 53, No. 7, p. 1448-1457, 2006.

[20] W. Surakampontorn and K. Kumwachara, CMOS-based electronically tunable current conveyor, *Electronics Letters*, Vol. 28, No. 14, pp. 1316-1317, 1992.

[21] Datasheet AD7533: CMOS low cost 10-bit multiplying DAC, Analog Devices, Rec. C, 2007.

Jiri Misurec MSc. (1985), Ph.D. (1991), Ass. Prof. (2007) is with the Brno University of Technology, Dept. of Teleinformatics, Czech Republic. He gives lectures in and leads the exercise for the subject "Analog technique"and gives lectures in the course "Digital Signal Processing". His research interest is focused on the area of analog technique, converters, especially on converters working both in voltage and current mode. Now he is interested in generalization of sensitivity analysis of transfer functions. This should be used for comparison of newly developed applications. In the latest he also cooperates with a number of companies on implementation of fundamental research results into practice.

Jaroslav Koton received the M.Sc. an Ph.D. degree in electrical engineering from the Brno University of Technology, Czech Republic, in 2006 and 2009, respectively. He is currently an Assistant Professor at the Department of Telecommunications of the Faculty of Electrical Engineering and Communication of Brno University of Technology, Czech Republic. His current research is focused on linear and non-linear circuit designing methods with current or voltage conveyors, and current active elements. He is an author or co-author of about 85 research articles published in international journals or conference proceedings. Dr. Koton is a Member of IEEE and IACSIT.

36th INTERNATIONAL CONFERENCE ON TELECOMMUNICATIONS AND SIGNAL PROCESSING

tsp 2013

IEEE

CZECHINVEST Investment and Business Development Agency

JULY 2-4, 2013, ROME, ITALY

The 2013 36th International Conference on Telecommunications and Signal Processing (TSP), will be held during ***July 2-4, 2013, Rome, Italy.***

The TSP 2013 conference is organized for, but not limited to, young academics, researchers and developers from different branches of telecommunication technology and signal processing. The aim of the conference is to bring together both novice and experienced scientists and developers, to meet new colleagues, collect new ideas and establish new cooperation between research groups.

TOPICS

Telecommunications:

- Information Systems
- Network Services
- Network Technologies
- Telecommunication Systems
- Modelling, Simulation and Measurement

Signal Processing:

- Analog Signal Processing
- Audio, Speech and Language Processing
- Biomedical Signal Processing
- Digital Signal Processing
- Image and Video Signal Processing

PROCEEDINGS

The conference proceedings will be indexed and abstracted in the ***IEEE Xplore, SCOPUS, Conference Proceedings Citation Index (CPCI) of Thomson Reuters***, ***DBLP***, *and* ***Google Scholar***. ***After the conference, selected papers will be published in special issues of international journals.***

IMPORTANT DATES

Paper Submission: *February 11, 2013*

Notification of Acceptance: *March 25, 2013*

Authors' Registration: *May 13, 2013*

CONTACTS

E-mail: tsp@feec.vutbr.cz

Web: http://tsp.vutbr.cz/

INDEXED BY

IEEE Xplore® DIGITAL LIBRARY

dblp .uni-trier.de Computer Science Bibliography

Google scholar

ISI PROCEEDINGS

SciVerse Scopus

IN COOPERATION WITH

ASSZISZTENCIA

Origo Services

ORGANISED BY

DEPARTMENT OF Telecommunications

West Pomeranian University of Technology Szczecin

Department of Telecommunications

STU FEI

UFE

8th International Conference on Electrical and Electronics Engineering

ELECO 2013

Bursa – Turkey

First Call for Papers

Aim and Scope

ELECO is organized as international conferences in odd numbered years and as national conferences in even numbered years. As such ELECO 2013 is the 8th international conference, with participants coming from various countries, presenting papers from the rich spectrum of electrical and electronics engineering. ELECO 2013 is jointly organized by Uludag University, Bursa; Istanbul Technical University (ITU); and the Chamber of Turkish Electrical Engineers (EMO), Bursa Section.
The Conference aims to provide a forum for electrical engineers and scientists in academia and industry, to present their works and to share their experiences in the area of electrical and electronics engineering.
Your contributions, presenting original work, are expected in the form of regular papers, special session papers.
Proposals from potential Special Session organizers are also expected by the same deadline, addressing more specific topics within the general scope of the conference.
From the broad scope of the technical program it was probably the largest international electrical and electronics engineering conference ever held in Turkey.

Topics

- Energy sources and power markets
- Electric power systems
- Electrical machines and drives
- Power electronics and applications
- Electrical materials and High voltage techniques
- Electronics
- Circuits and systems
- Signal processing
- Electromagnetics, microwave, antennas and propagation
- Optoelectronics
- Communication theory and systems
- Biomedical electronics
- Sensors and instrumentation
- Control theory and applications
- Mechatronics
- Robotics and automation systems
- Intelligent systems

Contact and Information

EMO Chamber of Turkish Electrical Engineers - Bursa Section
Bursa Akademik Odalar Birligi Yerleskesi (BAOB) Odunluk Mah. Akademi Cad. No. 8
16040 Bursa, Turkey
Telephone: +90 (224) 451 12 12
Fax: +90 (224) 451 98 99
E-mail: eleco@emo.org.tr

www.eleco.org.tr

ISSN 1805-5443