MATHEMATICS AND NATURAL SCIENCE

Proceedings of the Fifth International Scientific Conference – FMNS2013
12 – 16 June 2013

Faculty of Mathematics and Natural Science

VOLUME 2

COMPUTER SYSTEMS AND ENGINEERING

Dedicated to the 10th anniversary of Department of Computer Systems and Technology

South-West University “Neofit Rilski”
Blagoevgrad

Fifth International Scientific Conference – FMNS2013
South-West University,
Faculty of Mathematics and Natural Science
12 – 16 June 2013

ORGANIZING COMMITTEE:

Honorary Chairman:
Prof. Ivan Mirchev, DSc, Rector of the SOUTH-WEST UNIVERSITY "NEOFIT RILSKI"

Chairman: *Assoc. Prof. Stefan Stefanov, PhD, Dean of the Faculty of Mathematics&Natural Sciences*

Members:
Iliya Gyudzhenov, South-West University "Neofit Rilski", Bulgaria
Ivan Trenchev, South-West University "Neofit Rilski", Bulgaria
Ivanka Stankova, South-West University "Neofit Rilski", Bulgaria
Konstantin Tufekchiev, South-West University "Neofit Rilski", Bulgaria
Luben Mihov, South-West University "Neofit Rilski", Bulgaria
Mitko Stoev, South-West University "Neofit Rilski", Bulgaria
Stanko Shtrakov, South-West University "Neofit Rilski", Bulgaria
Valentin Hristov, South-West University "Neofit Rilski", Bulgaria
Grigor Iliev, South-West University "Neofit Rilski", Bulgaria
Vasilisa Pavlova, Regional Educatioinal Inspectorate-Blagoevgrad, Bulgaria

PROGRAM COMMITTEE:

Honorary Chairman: *Prof. Kiril Chimev, DSc*

COMPUTER SYSTEMS AND ENGINEERING

Members:
Albrecht Zur, University of Kiel, Germany
Aleksey Bubenchikov, Tomsk State University, Russia
Boris Tudjarov, TU- Sofia, Bulgaria
Dimitar Dimitrov, South-West University "Neofit Rilski", Bulgaria
Hubert Roth, University of Siegen, Germany
Janos Botzheim, Tokyo Metropolitan University, Japan
Kiril Boyanov, Bulgarian Academy of Sciences, Bulgaria
Miglena Doncheva, University of Dornbirn, Austria
Naoyuki Kubota, Tokyo Metropolitan University, Japan
Paul Borza, Transilvania University of Brasov, Romania
Shigeru Aomura, Tokyo Metropolitan University, Japan

The content of the Proceedings of the International Conference FMNS'2013 will be assigned to two of the EBSCO Publishing Data Bases: Academic Search Complete and Computers & Applied Sciences Complete

ISSN 1314-0272

Information Evolution and Man

Kiril Boyanov
IICT-BAS, Sofia, Bulgaria

1. INTRODUCTION

The increasing volume of information flow and the social networks lead to significant alteration in our perceptions followed by a leap into more disordered and unstructured conclusions which a human being takes. Our minds get accustomed to working with partial information and separate facts without them being linked to each other. As a result we find more difficulties when coping with larger works and large-scale compositions which require time and attention. When reading we gradually lose our ability to concentrate and remember images and ideas or to find meaning and patterns in relatively random elements. The social networks weaken and in time lead to a total loss of some useful habits which we have previously established.

The use of social networks as a basis for spreading information is growing exponentially. The largest so far social network – Facebook has more than 650 million active users registered between 2004 and 2010 [1]. According to the statistics each user is connected to another 130, and creates 90 posts including feeds, notes, photos and links to other sources each month. Users spend more than 700 billion minutes in Facebook [2].

Throughout the human history of social development the access to more information has practically allowed us to increase our knowledge. The introduction of writing is part of this process, and yet it has also acted as a limit to independent reasoning. Through writing we can store information and enforce our memory. Ever since the time of Platon has it been recognised that memory should be used as a mean to increase knowledge and to enhance structural thinking. The use of writing, as a form of “external memory” is widespread in today’s society.

2. WAYS TO TRANSFER INFORMATION (SPEECH, SOUND, IMAGE)

People have initially communicated with each other through discussions, by bringing up memories and forwarding basic information, stories and events from one generation to another. With the birth of writing we start storing information and find the ability to structure it.

It should be noted that a flow of information which is transmitted via speech is relatively limited. The volume of information which can be transferred by speaking can easily be proven as limited [3].

2.1. Speech transfer

If we consider one of the ways of information transfer – the speech – some rough calculation can be made. Each character is coded with 6 bits (binary). If we assume that in average, a word consists of 5 characters, one needs 60 bits for two words. Man can talk no faster than 3-4 words per second, which means that we can assume the upper boundary of 200 bit/sec as the one used by humans for information exchange (having 8 bits for coding and 4 words – 160 bits/sec, with compression – up to 4 bits and 4 words – 80 bits/sec).

The possibilities of the human brain for immediate use of character information, is huge. Let assume that a talented actor can memorize about 200 pages text, which he can repeat, after learning it by heart. According the standards, 1 page has 66 characters in a line and 30 lines per page – all together – 1980 characters. When coding 1 character with 8 bits we got 1980 x 8 =~16 Kb per page.

With maximum speed of reading of 200 bits/sec, the time for reading of those 200 pages is:

$(200*16*10^3)/200 = 16*10^3 = \sim 16*10^3$ sec = ~ 4.44 hours

The volume of transferred information is about 400 KB. In fact (actually) a man reads a page for some 90 sec, i.e. with coding of 8 bits per character = ~176 bits/sec, when we have 6 bits per character = ~ 132 bits/sec. So, an upper boundary of 200 bits/sec. can be accepted.

2.2. Sound transfer

Let us consider a piece of music. We suggest (for simplicity) the Minute Waltz of Chopin, which is played by good pianists for 1 minute.

The piano has 85 keys and for the coding of each one, we assign 1 bit (on, off). For the strength of the sound, from the weakest (pianissimo) to the strongest (fortissimo), we assign 10 bits. This scale has 1024 grades, enough for a good master.

For Chopin's waltz if we use 50 keys (out of 85), 50 bits will be needed in addition to the 10 bits for the volume, which comes altogether to 60 bits.

In the musical score, one can count 730 notes (in general, in case we regard the chords as one position). In such case, the speed of transfer will be:

(730*60) / 60 = ~ 730 bits/sec

Or a bit more, in case we include notes with longer duration.

We can make the conclusion that there is 3 to 4 times bigger speed for transferring information, in case we use sound (tune). If we compare a good musician to an actor, the former has to memorize several time bigger information than the latter (for some 3-6 hours) , maybe even more, when regarding the musical score of big musical compositions like symphonies, requiems, etc. It is not our task or intention to compare the brain abilities of the actor and the musician. The conclusion is linked to the fact, that using more musical tunes leads to transfer of more information.

The volume of the transferred information for 4.4 hours is = 4.4 * 3600 * 730 = 11 563 200 b, which is approximately 1.43 MB – 4 times bigger volume.

We can think that a thunderstorm or sea waves will be “described” with higher information speed (bits/sec) and correctness if using sound than speech.

If we look at some Eastern languages (Japanese, Chinese), we shall notice that some words express concepts and we can conclude that for the time, that European languages transfer some 200 bits/sec, the ancient languages transfer bigger quantity bits (i.e. more information if we measure the quantity). It is curious to know whether the ancient languages, preceding in terms of history the European, are more perfect in terms of information transfer. Or the elaboration of those languages was aimed at transferring more information for a shorter period of time.

For example the speed of communication can be improved more by overloading the words with several meanings. Chinese language is a good example on this: ma = mother, horse and question. Also notation of words can be improved by using reduced instruction set, also like in Chinese: <mother> = <woman> + <horse> <house> = <roof> + <pig>

A natural obstruction is that using more tunes leads to more possibilities for errors (i.e. wrong understanding of the expressions).

2.3. Image transfer

Transferring information by image is faster and more effective. Watching modern monitors, our eye accepts for 1 second several hundred thousand bits (in a quality image, there are several mega pixels and not all shades are being percept). This imposed the cinema, TV and other image devices as the faster source of big volume of information. They are also the most informative, in terms of acceptance and processing by the human brain.

Until the present moment, the education and acceptance of new facts and knowledge was linked to oral explanation and visual materials. Knowledge was gained also from books. In both cases, the sent and available information lets human brain to process it. Depending on the

intellectual abilities of the person, the processing and rationalization of the information was quicker or slower, but there was the option of explanations, the visual materials or the written information was available to the learner. Modern tools allow even better quality of visualization by image projection but this approach also allows control of time, so that the percept information can be realized. One can state that the process of information transfer was faster than the process of its processing and man had enough time to grasp and realize the presented information. With the mass introduction of TV, computers with significant abilities for visualization, the flow of information has increased significantly and the need for faster processing and realization of that information is evident. The resurrection of interactive methods for education allows the process of transfer of information to go in parallel with the one of its realization. It is clear that to explain to child what is “cat” is faster with picture than by oral explanation.

The continuous information flow sometimes requires swift reaction by a person, depending on the situation – as in emergencies or when fast and effective decisions are required in areas, still controlled by man – transport, emergency operations, industrial processes, etc. This implies that modern man has to increase his abilities not only for faster understanding and grasping of information but also for its faster processing. Both requirements assume getting more abilities and skills through new approaches.

The development or perfection of human senses – can be achieved by proper training and education: quick image recognition, effective filtering of background information, increased ability for sight and hearing. It is clear that individual abilities of each person should be taken into account. The fact, that abilities are ever improved by system training and using various approaches shows that using that regular work can lead to improved individual qualities in accordance to the demanded particular requirements.

One can see two scenarios here: creation of abilities by purposeful education of people – i.e. creation of “intelligent commandos”. The other scenario is using gene engineering – creating “cultivated modern societies”. Both approaches do not provide good forcasts. Even now, Internet divides society to those, seeking fun and strong emotions and the ones seeking knowledge. The first group will soon form not very well educated class or group, which we can call “user”. The second group we can place at the so called “educated elite” (or intelligent society). This will lead invevitabely to division of society and a future destructible conflict can be expected in either near future or later on, taking into consideration national characteristics. In short – one might expect a digital division of society and the question “When destructible social conflicts will begin?” remains. They will get bigger and stronger also due to the increasing gap between rich and poor.

The second scenario of improving the qualities and skills of people, by changing the gene material does not lead to good forecast either. Human

senses can not improve endlessly and there will be a moment, when a de-deformation of organs will occur, having unforeseen consequences. Whatever improvement is carried out on a particular organism, there is a limit – it is clear that 100 meters can not be run for 1 second.

The faster processing of information supposes the progress of abstract thinking and the potential for physiological and social generalization of the processes. Undoubtedly for people with various tendencies in certain societies, using certain approaches can lead to solving complex abstract or practical tasks. For others, there can be significant success in summarizing real humanitarian situations or the creation of pieces of art. The first group can work well in the field of technology in the name of mankind's prosperity, while the second will be leading for their spiritual enlightening.

One can present the hypothesis that the human organism was and will be developing in the direction of increasing its abilities for maximal perception and fastest processing of information.

Let us consider the possible boundaries for speed of transferred information. According to some examples from university classes [4], during the use of light in the micron scope (1.3 microns), where the attenuation is almost a constant, for example for $\Delta\lambda$ * $0.17*10^{-6}$, we have

$$\lambda \,.\, f = c; \frac{df}{d\lambda} = -\frac{c}{\lambda^2}; \Delta f = \frac{c\Delta\lambda}{\lambda^2} \tag{1}$$

$$i.e. \Delta f = \frac{3\,.\,10^8\,.0{,}17\,.\,10^{-6}}{(1{,}3\,.\,10^{-6})^2} = 30\,.\,3.10^4 \; or \; 30\,THz$$

Using Shannon's formula for the speed of information transfer [5] we get:

$$S = \Delta f \ln\left(1+\frac{S}{N}\right) \approx 30\,.\,10^{12}\ \ln\left(1+10^6\right) \approx \tag{2}$$

$$\approx 30\,.\,10^{12}\,.\,200 \approx 600\,.\,10^{12} \approx 0{,}6\ Pb/s,$$

Having a ratio signal/noise = 1 000 000 = 10^6.

Even if we consider electromagnetic radiation with shorter waves, the speed of transmission will be limited to tens Pb/s. Is there a limit of the speed theoretically? As S/N is limited, the increase of Δf is also limited; *c* is constant, so theoretically it is hardly possible to achieve speed of several Exab/s.

Processing of information. Let us consider the possibilities of computer processing. Modern speeds of processing are in the range of PFlops/s with the tendency of achieving ExaFlops/s. Reaching the next order will be difficult due to technological and power problems. Energy

losses (power consumption + cooling) can be unsuitable from environmental point of view.

The problem can be solved by the introduction of new principles of computing – for example – quantum computing, molecular computers using other principles of computing, though some restrictions can arise.

This raises the question of perceiving of the results of the processed information and its use in terms of expedience. In certain cases, human brain can be used to take decisions in real time, even when using computer systems, which he must get going. This means that his reaction won't be in time – i.e. there won't be the necessary result, hence it is not expedient.

3. MAN AND THE DIGITAL WORLD

As far as human's intellect is related to the brain's capacity, the relationship between its development and the introduction of new technology stands as a question of high importance. Some papers already describe technical approaches that allow faster introduction of information and also ways to use it more rational when managing real systems [6][7][8][9].

This is obviously a process that is limited in the long run, a question that can now be left for a solution. It is associated with certain paradoxes – is there a limit to the knowledge one can gain and can one reach this limit. If there is no limit to a person's potential knowledge then this knowledge will constantly grow up to a level, providing human's consciousness a new way of being. How will this development affect the group of people who are directly involved with physical labour and cannot reach the minimum intelligence level? Will we reach to a rift between the two groups or will we search for a mutually beneficial solution – a matter of research under certain assumptions, which is both technological as well as philosophical. The more likely scenario is that conflicts will arise, since earth's resources will be depleted, and people with higher intellectual standing will be able to deal with certain diseases, the cures of which will be out of grasp for the other group. But without this other group the food issue should be viewed in a whole different perspective. What will this society be – one of highly developed intellectuals who will use modern technology to supply their basic necessities, or will we inevitably pass through a global conflict leading to an uncertain outcome about the preservation of our civilization?

4. PROCESSING INFORMATION. COMPUTER-MAN

If we assume that there is a given connection between a human's and a computer's methods of processing information, we can roughly derive the

following parallels. Durring the administration of the different activities in the computer systems, a certain part of the RAM is kept for the preservation of the base supervising program (SP).

Looking into the development of the computer systems, the supervising program has taken from 10% to 20 % of the RAM. What is more, in order to use the full capacity of the computer, there is a continuous exchange between the RAM and the external memory. Let us assume that roughly 20% of the memory preserved for administration provides for the use of the rest of the RAM in a wide variety of tasks.

It should be noted that an increasing complexity of tasks corresponds to an increasing need for a larger quantity of SP and RAM. A parallel with the human brain can be made. The number of neurons is regarded to be around 10^{11} [10] and the number of connections is around 10^{14} (synopsis). According to research [11], [12], out of approximately 86 billion neurons, 69 billion are located in the brain and 16.3 billion find place in the cortex. It is possible that these 16.3 billion perform functions similar to the SP.

We will focus with more detail into the supervising program which usually takes place in a protected part of the RAM.

The SP aims to ensure functionality of the computer system by using RAM and external memory. The RAM hosts the data that is to be processed. Whether it will be hosted it pages intended to solve certain task in a multi-program mode, or whether batch-processing will be performed is an issue related to the performance of the computer system, and naturally its organization and architecture. In any case, however, SP aims also to ensure completion of the programs and their interactions with the environment (peripherals). We take it clear that the SP cannot pro-create new features within itself, but rather the system programmer or designer will add any amendments if needed. I.e. once confined, the SP cannot be modified during the execution of a specific task. Corrections can only be made in a certain time intervals depending on the requirements and functionality set by the designer. Figuratively speaking, the SP cannot cultivate and acquire new skills.

In the human brain, things look way more different. A fixed portion of the brain cells have a task of managing operations of the other cells, whilst constantly introducing them with new information subject to storage and processing.

The work process in the brain differs from the relationship SP-RAM (in the computer system) as a certain minimum of initial functions should be introduced which would serve to accumulate information in the brain cells. This process begins its development with the birth of a human being when he/she starts to percept and sense. Part of the information is stored, but at the same time is processed by those brain cells responsible for carrying out the connections. It is thus that we start accumulating a certain volume of

information in our brain which can be perceived through sight, hearing, touch, smell, and any other form of sensing known to the human body. This is a volume of information that constantly increases but managing the links between this information is carried out by the corresponding CPB (Control Program of the brain), which occupies part of the brain cells. An interesting fact [10] is that each neuron can carry out 7000 connections (synopsis). Within time, the data accumulated from the external environment grows more and more, resulting in a need for an improved supervising system so that better processing of this information can be achieved. This respectively leads to improving a human's organism actions in his/her environment. In such respect we can establish similarities with a computer system carrying out tasks for real-time processes.

In the same way that these actions can be associated with food gathering, they can also be associated with obtaining new knowledge about the surrounding environment. Such knowledge may improve a human's survival skills and/or may contribute for acquiring useful information in respect to his/her activities. In other words, we derive at a process where the volume of information is increased and at the same time the CPB is improved. Unlike a computer system, however, this improvement in the CPB is obtained thanks to training and self-training due to the contact between different personalities, and also thanks to the accumulated volume of information which allows management capabilities to grow. I.e. an interesting feature is that the more information the human brain acquires, the more complicated it becomes to manage this information in respect to survival related activities or development of the human's skills and intelligence. Moreover, giving progress to the CPB by the creation of new neuron cells will further improve the functionality of the whole brain system.

That is to periphrases the hypothesis as follows: **the larger the volume of accumulated information and the improved quality and speed of its processing should lead to an extended life expectancy.**

There is another interesting feature in the case of computer systems. In this case, the SP and volume of memory for a certain generation is fixed and cannot be substantially altered, and only a next generation can be designed with better functionality, increased memory, increased volume of the SP, etc. However, in the case of a human being this is all performed through an internally-dependent process. I.e., improving CPB is related to the increased volume of information which a person must perceive. As observed – this volume increases over time, which leased to an even increased number of connections between the separate brain cells.

And having in mind that there are 100 billion cells with 86 billion neurons and around 16 billion connections all of which responsible for the brain's functionality, there will yet be portions of the memory, which could be utilized, i.e. we should be able to continue adopting new information. When

considering a rough estimate of around 10 GB RAM in the human brain and several GB of CPB, the human's potential is far from exhausted.

Since it is estimated that the total volume of the world's information at present is around several exabytes, then it is logical that the information used by one individual is considerably smaller, i.e. $K_{app} << 1. \left(K_{app} = \frac{V_{eff}}{V} \right)$, where K_{app} - coefficient of applicability, V_{eff} - effective volume of used information, V - Volume of information.

5. INFORMATION AND EDUCATION

The access to a larger volume of information that allows individuals to expand their knowledge requires changes in the educational system. Within the educational field there have already been some studies developing new methods and approaches to education. Without considering the entirety of the field there are some interesting examples. Implementation of new techniques is evident in the training of tutors in the field of computer science due to the high applicability. Paper [13] discusses not only the demand of greater number of teachers but also the need to train them according to the technological developments.

The methods of education are the essence of the educational system. A greater percentage of academic graduates and practical trainees learn how to do the work they have studied for on the job rather than at university. On many instances this proves unsatisfactory for the employer which would require the educational providers to implement more focused and practical training. On one hand a future employee needs to be practically prepared in order to satisfy the requirements of the employer. On the other hand the limited study of basic theoretical theory makes it more difficult for professionals to acquire the new developments which would eventually be introduced in their field. A solution to this problem would be the constant improvement of one's knowledge and qualifications, or continuous education throughout one's lifetime.

The question then becomes what changes need to be introduced by the educational providers in order to implement such improvements. It is time to start making professional administrators aware of the development, needs and requirements of the different subjects thought in universities - a goal which depends on many things in order to be realised. For instance the people writing educational policies are not necessarily prepared professionally for the job or might not have the financial motivation. On the one hand the usually long term of employment of the heads of the university departments gives a guarantee to the public that traditions and best

practices will be observed. On the other hand this academic conservatism is harmful to the quickly developing digital field of education and does not allow for an account to be made of the realities of the spiritual and public life. Special attention should be given to economic and computer science universities which provide education in some of the vastly changing fields.

The introduction of computer technology is dynamically taking place in almost all aspects of modern education – starting with natural sciences, through humanities and social sciences and even including arts [14]. Although this technology brings many advantages throughout its wide range of applications, there are also some certain drawbacks.

An important element which restricts some of these disadvantages but is yet absent in our educational system is the code of ethics. The implication of such field is crucial in order to address a few existing ethical problems:

- Protection of copyrights from plagiarism;
- Sharing materials related to narcotics, alcohol, porn etc, via the computer networks;
- Control over the sites of educational institutions which should assess if any ethical code is actually conducted;
- Unbiased assessments of students, teachers, etc.

6. MAN AND DIGITAL SOCIETY

The Internet has changed the political and social realities, creating new opportunities for communication between people, expanding our horizons. The social networks and electronic media have set the roots of forming a “digital society” where the voice of social formations is increasingly being heard and recognised. The birth of this “digital society” implies a development of newly established communication, networking and literacy. This new literacy, in turn, includes active communication and an involvement of all participant members. In reality this should involve a combination of both the technical and social skills of the participants in this society. Just as our current traditional literacy and skills open the doors to the working and social processes, so should the “digital literacy” and “digital skills” provide certain abilities and confidence to become an active member of the “digital society”. The in-depth studies and implementations of computer and communication technology can expand our knowledge and skills from a childhood age improving the quality of the “digital society”.

The use of mobile communication and mobile technology has significantly improved our access to information at any time. Within the already established cyber space the access to information is related to two important (user) aspects.

The first aspect is the behaviour of the users. It can be recognised, for example, that when we use roads, public transport, driving, etc. we keep compliance with certain requirements and standards of behaviour. This implies that we achieve a certain level of literacy. In the “digital society”, one should in the same way establish certain behaviour and habits. Literature [15] identifies several important areas of behaviour which users of the “digital society” have to keep in compliance with: etiquette, communication, education, access, trade, responsibility, rights, safety and security. Other authors [16] suggest four key areas: digital compliance, digital ethics, digital sensibility and digital participation.

The second aspect is related to cyber threats and their relationship to the user’s behaviour in the digital society. The exponential growth of the use of Internet in economic, public and social areas has led to a tremendous increase in cyber attacks and threats. The existing firewalls are not always well-proofed requiring more responsibility and considerable efforts on the side of security experts [17].

7. PRIVACY OF INFORMATION

Protecting information is becoming a more and more serious problem. With the internet era and the expanding volumes of data uploaded online it is a challenge to find new preventive methods. In retrospect, one would find comparable dangers to privacy of information even before the invention of the computer. For example, even though the type of security used on social security cards and key-cards is not even comparable to the sophisticated protection used for online social networks the risks and dangers are alike. Computer systems, local network and internet in general have differences in vulnerability to breaches, but the types of the problems posed are similar.

The greatest danger to social network users is the breach (loss) of private information. According to [2] security of information researchers have estimated that up to July 2010, the private information of more than 100 million Facebook users is publicly accessible through the search engines. Several other threats are posed such as identity theft, debit and credit cards fraud and the like. The so called "hackers" attach social networks for one or more of the following reasons:

- The large number of users
- Abundance of private information that might be used for different purposes
- Easy access the such networks
- The high level of trust amongst users
- The variety of links to different applications allows more than one attack to be made

- Opportunity for spreading viruses

The increasing number of ways to breach the privacy of information requires serious protection.

The traditional protective methods such as cryptography, security protocols and insurance are no longer sufficient. The main goal of researchers is to perform the necessary analysis of protocols and methods of protection of privacy of information and to suggest entirely new approaches and a paradigm adequate to the new security requirements [18].

8. CONCLUSIONS

The rapidly growing flow of information via the Internet and other sources sets enormous challenges and stress in our lives. It is only natural that this will influence both positively and negatively human and society. Appropriate measures and programs should be introduced as soon as possible. These should be embraced by all age groups, starting as early as preschool, otherwise the consequences might evolve to be hard to predict.

9. REFERENCES

[1] Carlson, N. Facebook Has More Than 600 Million Users, Goldman Tells Clients, Business Insider, Online January 15, 2011, Available at: http://www.businessinsider.com/facebook-has-more-than-600-million-users-goldman-tells-clients-2011-1.

[2] Saeed A, Th. M. Chen, O. Alzubi, Malicious and Spam Posts in Online Social Networks, Computer, September 2011, p. 23.

[3] K. Boyanov, “On the Measurement of Quantity of Information on Speech, Sound and Image, and their Link with the Information Processing”, Proceedings of Joint Informational Conference on Human-Centered Computer Environments [HCCE 2012], March, 2012, Aizu-Wakamatsu, Japan.

[4] A. Tanenbaum, Computer Network, 4th Edition, 2003, Prentice Hall, Ch.2, §2.2.

[5] C. E. Shannon (January 1949). “Communication in the presence of noise” (PDF). Proc. Institute of Radio Engineers vol. 37 (1): 10-21.

[6] A. Schmidt and E. Churchill, “Interaction beyond the Keyboard”, Computer, April 2012 p. 21.

[7] H. Gellersen and F. Block, “Novel Interactions on the Keyboard”, Computer, April 2012 p. 36.

[8] A. Riener. “Gestural Interaction in Vehicular Applications”, Computer, Appril 2012, p. 42.

[9] M. Begudouin and all “Multisurface interaction in the WILO Room”, Computer, April 2012.
[10] Draclman D., “Do we have brain to spare?”, Neurology 64(12)p 2004-5.
[11] Williams R., Herrup K., “The control of neuron number”, Annual Review of Neuro science 12, p. 423-53.
[12] Azevedo F., Carvalho L., Grinberg L., et al “Equal numbers of neuronal and noneuronal cells make the human brain an isometrically scalet-up primate brain.” The Journal of Comparative Neurology 513(5), April 2009.
[13] M. Guzdial, “Learning How to Prepare Computer Science High School Teachers”, Computer, October 2011, p. 95.
[14] N. Holmes., “Digital Machinery and Analog Brains”, Computer, October 2011, p. 100.
[15] Ribble M., Bailey G., Ross T., Digital Citizenship Addressing Appropriate Technology Behavior, Learning& Leading with Technology, September 2004, vol. 32, No 1, pp 6-11.
[16] Yang H., Oh K., A Study of the Digital Citizenship. The International Journal of Policy Studies, Korean Association for Public Studies, 2011.
[17] Боянов Л., Зл. Минчев, К. Боянов, Някои киберзаплахи в дигиталното общество, Автоматика и Информатика, кн. 3, 2012.
[18] R. Rodrigo, P. Najera, J. Lopezi, Securing the Internet Things, Computer, September 2011, p. 51.

Multi-modal Perception for Human-friendly Robot Partners with Smart Phones based on Computational Intelligence

Naoyuki Kubota[*1], Yuichiro Toda[*1], Janos Botzheim[*1,2], and Boris Tudjarov[*3]

[1]*Tokyo Metropolitan University, Tokyo, Japan*

[2]*Szechenyi Istvan University, Gyor, Hungary*

[3]*Technical University of Sofia, Sofia, Bulgaria*

***Abstract**: This paper proposes an intelligent information processing method for multi-modal perception of a human-friendly robot partner based on various types of sensors built in a smart phone. First, we explain the hardware specification of a robot partner using a smart phone. Next, we propose an integration method of measurement data obtained by several sensors in the smart phone to estimate human interaction mode by computational intelligence techniques. Finally, we show several experimental results of the proposed method using the robot partner, and discuss the future direction.*

***Keywords:** Intelligent Robots, Sensor Fusion, Computational Intelligence, Natural Communication.*

1. INTRODUCTION

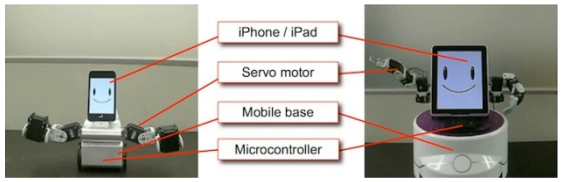
Recently, various types of smart phone and tablet PC have been developed, and their price is decreasing year by year [1]. Furthermore, the embedded system technology enables to miniaturize such a device and to integrate it with many sensors and other equipment. As a result, we can get a mechatronics device including many sensors, wireless communication systems, GPU and CPU composed of multiple cores with low price. Furthermore, elderly people unfamiliar with information home appliances also have easily started using tablet PC [2], because touch panels or touch interface have been popularized at ticket machines and information services in public areas. Therefore, we started the development project on on-table small size of human-friendly robot partners called iPhonoid and iPadrone based on smart phone or tablet PC to realize information support to elderly people. [3,4].

We can discuss three different styles of robot partners using a smart phone or tablet PC from the interactive point of view: physical robot partner, pocket robot partner, and virtual robot partner [5]. Each style of robot partners is different, but the interaction modes depend on each other, and we interact with the robot partner with the same knowledge on personal information, life logs, and interaction rules. In this paper, we propose a method of estimating human interaction modes based on computational intelligence techniques by using measurement data of sensors a smart phone or a tablet PC equipped with.

This paper is organized as follows. Section 2 explains the hardware specification of robot partners developed in this study. Section 3 proposes the methods of estimating human interaction mode and estimating human behaviors. Section 4 shows several experimental results of human-friendly robot partners. Finally, we summarize this paper, and discuss the future direction to realize human-friendly robot partners.

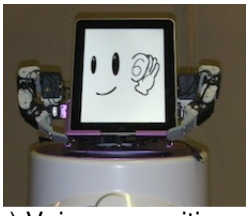
2. HUMAN FRIENDLY ROBOT PARTNERS

We have developed on-table small size of robot partners called iPhonoid and iPadrone (Figs.1 (a) and (b)). Since a smart phone is equipped with various sensors such as gyro, accelerometer, illumination sensor, touch interface, compass, two cameras, and microphone in addition to CPU and GPU, the robot base should have composed of actuators, motor drivers, and communication units at least. The mobile base is equipped in the bottom (Fig.1), but basically we don't use the mobile base on the table for safety's sake. In order to control the actuators of a robot partner from the smart phone or tablet PC, we can use wireless LAN and wireless PAN (Bluetooth) in addition to a wired serial communication. Basically, human detection, object detection, and voice recognition are done by the smart phone or tablet PC. Furthermore, touch interface is used as a direct communication method. When a person touches the right side on the display, the facial expression changes and voice recognition starts (Fig.2 (a)). Based on the perceptual information, the robot partner makes utterance with gestures (Fig.2 (b)).



(a) iPhonoid (b) iPadrone

Fig.1: Robot partners using a smart phone and a tablet PC.


(a) Voice recognition


(b) A gesture

Fig.2: Robot behaviors for social communication with people.

3. MULTI-MODAL PERCEPTION BASED ON SENSOR FUSION

3.1. Human Interaction Modes

In this paper, since we use the facial expression on the display for human interaction (see Figs. 1 and 2), the robot partner should estimate the human interaction mode: (a) the physical robot partner mode (attached to the robot base), (b) pocket robot partner mode (being removed from the robot base), or (c) other mode (on the table, in the bag, and so on). We use the values of acceleration, attitude, and luminance, and apply a fuzzy spiking neural network (FSNN) [6,7] using a simple spike response model with Gaussian membership functions to estimate the human interaction mode. A high pass filter is used to calculate the acceleration from data measured by the accelerometer. The attitude is calculated by measurement data of accelerometer, gyroscope, and digital compass. The luminance is calculated from the images measured by cameras.

The internal state $h_i(t)$ of the i-th spiking neuron at the discrete time t is calculated as follows:

$$h_i(t) = \tanh(h_i^{syn}(t) + h_i^{ext}(t) + h_i^{ref}(t)), \quad (1)$$

where $h_i^{syn}(t)$ includes the pulse outputs from other neurons, $h_i^{ref}(t)$ is used for representing the refractoriness of the neuron, $h_i^{ext}(t)$ is the input to the ith neuron from the external environment. The hyperbolic tangent function is used to avoid the bursting of neuronal fires.

The external input, $h_i^{ext}(t)$ is calculated based on Gaussian membership functions:

(2)

$$h_i^{ext}(t) = \prod_{j=1}^{M} v_{i,j} \,.\, exp\left(\frac{(x_j - a_{i,j})^2)}{b_{i,j}}\right)$$

Furthermore, $h_i^{syn}(t)$ indicates the output pulses from other neurons:

(3)

$$h_i^{syn}(t) = \sum_{j=1, j\neq i}^{N} w_{j,i} \,.\, h_j^{PSP}(t-1)$$

where $w_{j,i}$ is a weight coefficient from the *j*th to the *i*th neuron; $h_j^{PSP}(t)$ is the presynaptic action potential (PSP) approximately transmitted from the *j*th neuron at the discrete time *t*; *N* is the number of neurons. When the internal action potential of the *i*th neuron is larger than the predefined threshold, a pulse is outputted as follows:

(4)

$$p_i(t) = \begin{cases} if\ h_i(t) \geq q^{pui} \\ 0\ \ otherwise \end{cases}$$

where q^{pul} is a threshold for firing. Furthermore, *R* is subtracted from the refractoriness value as follows:

(5)

$$h_i^{ref}(t) = \begin{cases} \gamma^{ref}.\ h_i^{ref}(t-1) - R & if\ p_i(t-1) = 1 \\ \gamma^{ref}.h_i^{ref}\ (t-1) & otherwise \end{cases}$$

where γ^{ref} is a discount rate and *R*>0.

The spiking neurons are interconnected, and the presynaptic spike output is transmitted to the connected neuron according to the PSP with the weight connection. The PSP is calculated as follows:

(6)

$$h_i^{PSPf}(t) = \begin{cases} 1 & if\ p_i(t) = 1 \\ \gamma^{PSP}.h_i^{PSP}\ (t-1) & otherwise \end{cases}$$

where γ^{PSP} is the discount rate ($0<\gamma^{PSP}<1.0$). Therefore, the postsynaptic action potential is excitatory if the weight parameter $w_{j,i}$ is positive.

We apply (μ+λ)-Evolution Strategy (ES) for the improvement of the parameters of the Gaussian membership functions. In (μ+λ)-ES, μ and λ indicate the number of parents and the number of offspring produced in a single generation, respectively [8]. We use (μ+1)-ES to enhance the local hill-

climbing search as a continuous model of generations, which eliminates and generates one individual in a generation. (μ+1)-ES is considered as a steady-state genetic algorithm (SSGA) [9]. A candidate solution is composed of numerical parameters corresponding to the central value, the width, and the contribution of fuzzy membership functions:

(7) $$g_k = [\, g_{k,1}\ g_{k,2}\ g_{k,3}\ \ldots\ldots\ g_{k,i}] = [\, a_{k,1,1}\ b_{k,1,1}\ \mathbf{n}_{k,1,1}\ \ldots\ldots\ \mathbf{n}_{k,n,m}]$$

where n is the number of human interaction modes; m is the number of inputs; $l = n \cdot m$ is the chromosome length of the kth candidate solution. The fitness value of the kth candidate solution is calculated by the following equation:

(8) $$f_k = \sum_{i=1}^{n} f_{k,i}$$

where $f_{k,i}$ is the number of correct estimation rates of the ith human interaction mode. In (μ+1)-ES, only an existing solution is replaced with the candidate solution generated by crossover and mutation. We use elitist crossover and adaptive mutation. Elitist crossover randomly selects one individual, and generates an individual by combining genetic information between the selected individual and the best individual in order to obtain feasible solutions from the previous estimation result rapidly. Here we can use the local evaluation values of the human interaction estimation.

3.2. Multi-modal Interaction

The robot partner starts the multi-modal interaction after a smart phone is attached to the robot base. We use touch interface on the smart phone or tablet PC as the nearest interaction with a robot partner. The facial parts are displayed as icons for the touch interface in the display (Fig.2 (a)). Since the aim of this study is to realize information support to elderly people through the multi-modal interaction, the robot partner provides elderly people with their required information through the touch interface.

The ear icon is used for direct voice recognition because it is difficult to perform high performance of voice recognition in the daily communication with the robot partner. If the person touches the mouth icon, then the ear icon appears, and the voice recognition starts. The voice recognition is done by Nuance Mobile Developer Program (NMDP). NMDP is a self-service program for the developers of iOS and Android application. In this way, the total performance of multi-modal communication can be improved by combining several communication modalities of touch interface, voice recogni-

tion, and image processing. The conversation system is composed of (A) daily conversation mode, (B) information support mode, and (C) scenario conversation mode [4,5].

We use two cameras (front and rear cameras) the smart phone equipped with. Basically, we obtain time-series of images in RGB color space. In order to detect a human considered as a moving object, we use (1) gray scale conversion from the color image by YUV model, (2) differential extraction, (3) simple color extraction, and (4) ES [8] based on template matching for extracting a human shape from the background image.

The sequence of human hand positions can be used to extract a spatio-temporal pattern of human behaviors. Here two layers of spiking neural network (SNN) using a simple spike response model for human motion extraction are applied to reduce the computational cost. In the first layer, spiking neurons are used to extract the moving direction and other motions listed in Table 1. By using the change of position of a human face or hand, the neuron corresponding to its direction is fired. In the second layer, the excitatory presynaptic potential (EPSP) based on firing patterns is used to estimate human behaviors listed in Table 2. The human behaviors of (0) No people, (1) Approaching, and (2) Leaving are simply estimated by the change of human position and the size of template. The human behavior of (4) Sitting is estimated by the relative position from the robot. The human behavior of (5) Interacting is estimated by motion extraction, and the human behavior of (6) Touching is directly recognized by the touch interface of the robot face.

Tab. 1: Features used for motion extraction.

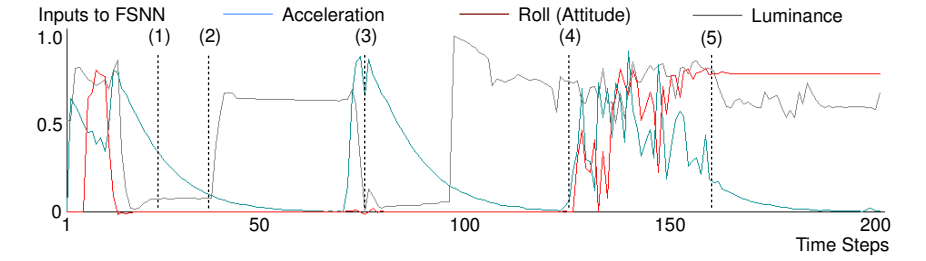
ID	Motion	ID	Motion	ID	Motion
0	no motion	6	d5 direction	12	area size
1	d0 direction	7	d6 direction	13	upper position
2	d1 direction	8	d7 direction	14	middle position
3	d2 direction	9	stoping	15	lower position
4	d3 direction	10	extending		
5	d4 direction	11	reducing		

Tab. 2: Human behaviours.

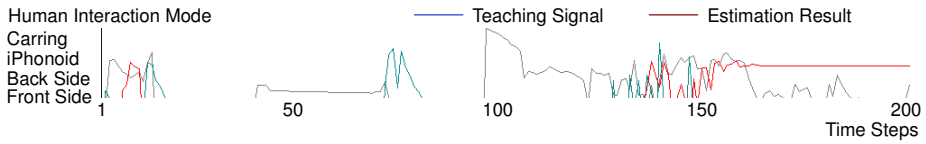
ID	Behavior	ID	Behavior
0	no people	4	sitting
1	approaching	5	interacting
2	leaving	6	touching
3	standing		

4. EXPERIMENTAL RESULTS

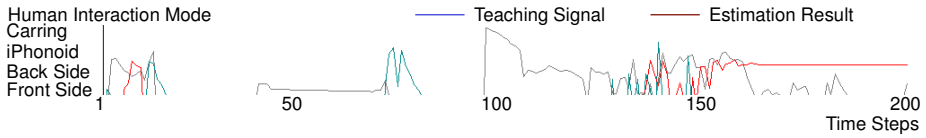
This section shows experimental results of the proposed method using a robot partner. The number of individuals of (μ+1)-ES for fuzzy inference is 100, and the number of evaluation (iteration) times is 5000. Figure 3 illustrates experimental results of the estimation of human interaction modes by the proposed method. We conducted off-line learning after obtaining teaching data beforehand. In the experimental result (Fig.3 (a)), the person put iPhone on the table with making the display prone ((1) in Fig.3 (a)). As a result, since the luminance was very low, the rear camera was activated ((2) in Fig.3 (a)). After several second, the person overturned the iPhone ((3) in Fig.3 (a)). Next, the person took the iPhone ((4) in Fig.3 (a)), and attached the iPhone to the robot's base ((5) in Fig.3 (a)). In the initialization of the fuzzy inference rules, we used the average and standard deviation of the input data of the teaching signals. Figure 3 (b) shows an estimation result using the initial values of the fuzzy inference rules before learning. After updating the fuzzy inference rules by (μ+1)-ES, the performance of the estimation of human interaction mode was improved (Fig.3 (c)).



(a) Inputs to FSNN



(b) An estimation result before learning

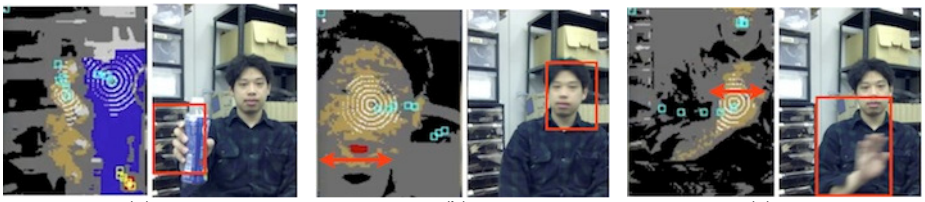


(c) An estimation result after learning

Fig. 3: Estimation results of human interaction mode.

Next, we present experimental results of human interaction. The image size of a camera is reduced to 120 x 160. The number of individuals (candidate templates) of (μ+1)-ES for the image processing is 100, and the num-

ber of evaluation (iteration) times for the image processing is 150. Figure 4 depicts the snapshots of attention range, human detection, human motion, and object detection. The result of image processing is shown in the left side, and the attention range is drawn by a red box in the right side. A person showed a bottle (a), and showed a hand gesture (c). Since the attention range is focused on the moving object, and the robot partner traced the movement of the bottle. After the person had put the bottle on the table, the robot partner paid attention to the human face. Next, the robot partner found the human hand gesture, and extracted its human hand motion pattern. In this way, the robot partner tried to pay attention to human motion and gestures to realize the interaction with a person.



(a) (b) (c)

Fig. 4: Snapshots of robot gestures.

5. SUMMARY

In this paper, we proposed a method of estimating human interaction mode using two cameras, accelerometer, and gyro. First, we explained the robot partners developed in this paper. Next, we proposed an estimation method of human interaction mode using a fuzzy spiking neural network based on a simple spike response model with Gaussian membership functions. Furthermore, we proposed a method of tuning fuzzy inference rules based on evolution strategy. In the experimental results, we showed, that the proposed method is able to estimate human interaction modes based on the iPhone's sensors.

As a future work, we intend to improve the learning performance according to human life logs, and propose an estimation method of more types of human interaction modes.

6. REFERENCES

[1] http://www.letsgodigital.org/en/23646/smartphone-price/
[2] http://green.tmcnet.com/news/2013/02/18/6929794.htm
[3] D. Tang, B. Yusuf, J. Botzheim, N. Kubota, and I. A. Sulistijono, "Robot Partner Development Using Emotional Model Based on Sen-

sor Network", Proc. (CD-ROM) of IEEE Conference on Control, Systems and Industrial Informatics (ICCSII 2012), pp. 196-201, 2012.
[4] N. Kubota, Y. Toda, "Multi-modal Communication for Human-friendly Robot Partners in Informationally Structured Space", IEEE Transaction on Systems, Man, and Cybernetics-Part C, vol. 42, no. 6, pp.1142-1151, 2012.
[5] N. Kubota, "Cognitive Development of Partner Robots Based on Interaction with People", Proc. (CD-ROM) of Joint 4th International Conference on Soft Computing and Intelligent Systems and International Symposium on Advanced Intelligent Systems, 2008.
[6] W. Gerstner, Spiking Neurons, In W. Maass and C. M. Bishop, editors, Pulsed Neural Networks, chapter 1, MIT Press, 1999, pp. 3-53.
[7] W. Gerstner, W. M. Kistler, Spiking Neuron Models, Cambridge University Press, 2002.
[8] H.-P. Schwefel, Numerical Optimization of Computer Models, John Wiley & Sons, New York, 1981.
[9] G. Syswerda, A Study of Reproduction in Generational and Steady-State Genetic Algorithms, In Foundations of Genetic Algorithms, Morgan Kaufmann Publishers, Inc., pp. 94-101, 1991.

A Survey of Intelligent Tutoring and Affect Recognition for Mobile Devices

Malinka Ivanova

Technical University of Sofia

***Abstract**: Intelligent tutoring is used to support a student through arrangements of adaptable learning paths. Some of intelligent tutoring systems are only interested in the cognitive state of a student; others combine the cognitive state with the affective situation to achieve the best efficacy in learning. Emotional mood could be recognized through one technique or combination of several methods.*

The aim of the paper is to explore the specificity of intelligent tutoring improved by emotions recognition and suitable for use on mobile devices. This will facilitate educators in their intention to realize mobile intelligent tutors.

***Keywords:** intelligent tutoring, affect recognition, facial expression recognition, mobile devices, mobile learning*

1. INTRODUCTION

The role of an intelligent tutor is to support learning of a student according to his individual specific characteristics and level of knowledge in a given domain. Intelligent tutors are used in several pedagogical scenarios like: problem solving, ensuring step-by-step guidance considering the way of student's thinking, learning by dialog, others, providing flexible learning paths. Their construction typically consists of four modules: *expert knowledge module* that describes knowledge in a given subject-matter domain; *student model module* contains information about student' background, behavior, achievement; *tutoring module* includes pedagogical strategies and instruction to students, and *user interface module* that ensures a flexible and interactive connection between the student and the computer tutor. Nowadays the construction of intelligent tutors is extended with modules for motivation improvement and student affect recognition. The reason for that is research showing that emotional state influences on learning, decision making and problem solving. Different techniques for affect recognition are implemented including: facial expression recognition, analysis of voice characteristics, analysis of text typing dynamics, self-evaluation via

emotional quiz, measuring the pressure on the chair, measuring the heart rhythms, etc. An intelligent tutoring system (ITS) can utilize one of these techniques or combination of several of them to receive needed information about the emotional state of a student.

Recently, researchers have been working intensively on Internet faster applications and ITSs mobile versions. This is dictated by the lifestyle of young people and advances in mobile technologies. Also, the problems of delay of signal in wireless networks and standardization are explored in [9], [10], [11] and it is proved that the signal delay is relatively small. Anyway, the created mobile versions of ITSs are a few with limited features.

The aim of this research is to recognize the main usage of mobile devices for learning, to figure the specific characteristics in design of mobile learning environments, to understand the face and facial expression recognition and its implementation in mobile devices in context of ITSs improvement. The explored provision of scientific achievements in the areas of ITSs, mobile technologies, learning design, and affect recognition will facilitate educators in their intention to put in practice mobile intelligent tutors.

2. MOBILE INTELLIGENT ENVIRONMENTS

The utilization of mobile technologies for ensuring an effective tutoring support and the tutor's role and tasks in mobile learning settings are discussed in [8]. Several tutoring methods are suggested after summarization of face-to-face classroom practice and eLearning instructional strategies. The theoretically built model Activation, Externalization, Focusing, Interpretations, Reflection and Information Processing (AEFIRIP) by Silander and Rytkönen, reflecting the specificity of mobile tutoring and learning is examined as a main pedagogical statement for implementation of a semi-automatic tool that facilitate mobile tutoring. The educational practices suitable for usage in mobile variant are classified in seven categories: (1) tutoring and guidance through sending sms, emails for help providing, writing in blogs, performing inquiry, tutoring by video phone calls, keeping tutoring dialogue, gathering the students' answers after learning tasks doing, gathering artefacts by students; (2) receiving students products, chat, one-to-many communication; (3) communication through real-time interaction, access to student's portfolio, access to students achievements; (4) evaluation / assessment through the results after tasks doing in specific learning situations; (5) positioning of students through pedagogical strategies that incorporate in themselves the possibilities of GPS; (6) simulation through access to simulators, examples, instructional games, demos, videos.

A detailed study about the performed informal learning activities in time of mobile devices usage shows that the main interactions are related to the exploitation of the mobile, connective and collaborative functionalities of

these devices [4]. The findings point that learners perform a wide variety of intentional and unintentional learning activities using mobile learning applications grouped in seven categories according to the functional architecture of Patten, Arnedillo Sanchez, and Tangney: (1) collaborative activities – information sharing and uploading through wiki, blog, forum, email and sms, skype VoIP; (2) location aware activities – using GPS, downloading contextual information; (3) data collection activities - recording audio notes, writing text, taking picture and video; (4) referential activities – looking for information to dictionaries, translators, e-books, course materials; (5) administrative activities – organizing calendar events and contacts; (6) interactive activities related to applications with information input and output in support of learning; (7) microworld applications (learning scenarios from the real practice) are not used in informal learning context.

3. DESIGN OF MOBILE ENVIRONMENTS

Koole and Ally are developed a theoretical model FRAME (Framework for the Rational Analysis of Mobile Education) that examines the processes in mobile learning and proposes a specification of strategies for mobile teaching and learning [12]. The model renders the reciprocal actions among mobile technologies, learner capabilities and socio-cultural background and guides the designers of mobile learning in their preparation of a mobile educational environment. They give prescriptions about design of: (1) learning content in form of learning objects for flexible lessons delivery, served according to the cognitive level of a given student and leading to the successful achievement of learning goals; (2) learning activities considering the different students' styles of learning and the different needs for instructional support; (3) teaching instructions that facilitate the mental processing, stimulate the attention and maintain the motivation, including sequences of instructions forcing students to apply their existing knowledge in problem solving or in real life situations, to analyze, to synthesize new knowledge, to evaluate, ensuring deep learning and storage in the long-term memory. The authors conclude that the focus in the design of a mobile learning environment has to be put on the "knowledge navigation paradigm" where the tutor plays a crucial role in assistance providing at selection and manipulation of prior information.

4. ITS FOR MOBILE DEVICES

A mobile version of a typical ITS designed according to the characteristics of mobile devises is presented in [2]. A geometry tutor from Carnegie Learning framework is used as bases for experimentation. This math tutor is

converted in the so called “Poor Man’s Eye Trackers” tutor in order for the user interfaces to be evaluated. Its interface is divided into several regions and every one of them is covered by an opaque layer which is removed through a mouse click by a student. In this way during the solving geometric problems, the students can work only with one region at a time. The intelligent tutor records the opened regions, the transition flows between regions and the time spent for each one student. The received data is analyzed and the regions with lower usage are re-designed in tabs. Authors consider that such solution will activate students for frequent usage of the converted in tabs regions.

Chen and Hsu present a solution of a personalized intelligent mobile system for improving English reading ability that consists of a mobile client application of English learning system, a remote server and an agent for data synchronization between client and server [3]. The results after experimentation point to several benefits of the proposed mobile system for learners like: reduction of cognitive overload because of the personal recommendation for English articles reading, promotion of English learning, comprehension and reading.

5. FACIAL EXPRESSION RECOGNITION

The face characteristics and its muscle motions are described with a set of parameters which is utilized for recognition of facial emotions. Several sets with such parameters are created, but the most used are the following two: the Facial Action Coding System (FACS) presented by Ekman and Friesen [7] and the set with Facial Animation parameters (FAPs) which is included the MPEG4 Synthetic/Natural Hybrid Coding (SNHC) standard. Anyway, the MPEG4 standard does not give information about some facial behavioural characteristics that differentiate the posed from spontaneous emotions. MPEG4 is applied for preparing animations of facial avatars, but it does not count the changes in surface texture like shape changes, bulges and wrinkles that are important for FACS action units description.

The differences between posed and spontaneous expressions are rooted in emotions appearance and their temporal characteristics (onset-apex-offset). Posed and spontaneous expressions can be recognized by the movement of given facial components and by their movement dynamics. Ekman talks also about micro facial expressions and squelched expressions [6]. Micro facial expressions are observed in the cases when people are trying to mask their real emotions. Their duration is very short about 1/25-1/15of a second, but they are complete expressions (they have onset, apex and offset). The squelched expressions begin their showing but they are immediately stopped and changed to other expression. The squelched expressions are uncompleted and their duration is longer than micro expres-

sions. At this moment several automatic recognition systems for micro expressions are developed, but still the meaning of micro facial expressions for educational society are not researched. Instead of that there are a wide range of good practices at implementation of facial expression recognition systems working with posed and spontaneous expressions, including in the area of ITSs.

6. FACE RECOGNITION IN MOBILE DEVICES

A face recognition system for Motorola DROID phone is presented in [5] that has been developed after investigation and experimentation with several algorithms for colour segmentation and face detection. The findings point to the existence of limitations related to the incorrectness at color recognition, templates dependence, not good detection of people's faces from different ethnic groups. Other two algorithms Eigenface and Fisherface for face recognition are tested and the resulted rate for correct recognition is 84.3% for Eigenface and 94.0% for Fisherface.

Anand et al. report for a desktop application of eBook reader implementation with possibilities for facial expression recognition [1]. Several functions related to the display control can be manipulated by the facial expression. For example, when a person is frowning the UI will be changed, if his eyes are opened wide then the content is zooming out, if the head is nodded in right or in left, then the previews or next page will be turned, if the finger is on mouth then the audio will be muted. For facial expression recognition FACS is used in two phases – facial action units detection and inference of the output emotion based on detected active units. Other methods like Gabor filter, AdaBoost and Support Vector Machine are applied too. Authors are working on adaptation of this system to Android tablet device.

7. CONCLUSIONS

Intelligent tutoring for mobile devices makes its first progressive steps for ensuring high quality of learning giving ubiquitous access to knowledge when students are outside of classrooms (for example, distance education, informal learning). At the beginning stage are also applications combining the level of cognition and affective state of a student to provide appropriate learning object or path. There are several problems related to the design of new applications (media form, duration of learning objects, attention allocation, emotions' recognition) and adaptation of the existing desktop or web-based tutors to mobile versions. Further research is needed to outline the effective pedagogical strategies, cognitive issues and technical solutions.

8. REFERENCES

[1] Anand, B. et al. (2012) Beyond Touch: Natural Interactions Using Facial Expressions, The 9th Annual IEEE Consumer Communications and Networking Conference – Special Session Affective Computing for Future Consumer Electronics, pp. 255-259, http://cgit.nutn.edu.tw:8080/cgit/PaperDL/LZJ_120807051353.PDF

[2] Brown, Q. et al. (2008) The design of a mobile intelligent tutoring system, In Proceedings of the 9th International Conference on Intelligent Tutoring Systems 2008, https://www.cs.drexel.edu/~salvucci/publications/Brown-ITS08b.pdf

[3] Chen, C. M., Hsu, S. H. (2008) Personalized Intelligent Mobile Learning System for Supporting Effective English Learning. *Educational Technology & Society* 2008, 11 (3), pp. 153-180.

[4] Clough, G. et al. (2009) Informal Learning Evidence in Online Communities of Mobile Device Enthusiasts, *Mobile Learning: Transforming the Delivery of Education and Training*, Issues in Distance Education, Athabasca University Press, pp. 99–112.

[5] Dave, G. et al. (2010) Face Recognition in Mobile Phones, http://www.stanford.edu/class/ee368/Project_10/Reports/Sriadibhatla_Davo_Chao_FaceRecognition.pdf

[6] Ekman, P. (2003) Darwin, Deception, and Facial Expression. *Annals of the New York Academy of Sciences*, vol. 100, pp. 205-221, http://www.evenhappier.com/darwin.pdf

[7] Ekman, P., Friesen, W. (1978) Facial Action Coding System: A Technique for the Measurement of Facial Movement. *Consulting Psychologists Press*, Palo Alto, CA.

[8] Graham, K. (2010) The use of mobile communication technology for tutoring, http://ebookbrowse.com/the-use-of-mobile-communication-technology-for-tutoring-pdf-d421089279

[9] Hristov, V. (2009) Signaling Delay in Wireless Networks with Session Initiation Protocol over User Datagram Protocol, Proc. of the Conference FMNS'09, Blagoevgrad, 3-6 June, vol. 1, pp. 78-85.

[10] Hristov, V. (2009) Signaling Delay Using Session Initiation Protocol over Transmission Control Protocol in Wireless Networks, Proc. of the International Conference on Information Technologies (InfoTech-2009), September 17-20, 2009, Varna– St. St. Constantine and Elena, Bulgaria, pp. 82-87.

[11] Hristov, V. (2010) Session Initiation Protocol Interworking with Traditional Telephony and Signaling Delay Introduced by Internet, Proc. of the International Conference on Information Technologies (InfoTech-2010), September 16-17, Varna, Bulgaria, pp. 167- 172.

[12] Koole, M., Ally, M. (2006) Framework for the Rational Analysis of Mobile Education (FRAME) Model: Revising the ABCs of Educational Practices, auspace.athabascau.ca/bitstream/2149/612/1/01628461.pdf

FPGA Based Mixed-Signal Circuit Novel Testing Techniques

Sotirios Pouros[*], Vassilios Vassios[*], Dimitrios Papakostas[*], Valentin Hristov[**]

*[*1]Alexander Technological & Educational Institute of Thessaloniki, Greece*
[**]South-West University, Blagoevgrad, Bulgaria

***Abstract**: Electronic circuits fault detection techniques, especially on modern mixed-signal circuits, are evolved and customized around the world to meet the industry needs. The paper presents techniques used on fault detection in mixed signal circuits. Moreover, the paper involves standardized methods, along with current innovations for external testing like Design for Testability (DfT) and Built In Self Test (BIST) systems. Finally, the research team introduces a circuit implementation scheme using FPGA.*

***Keywords:** Fault Detection, Mixed Circuits, BIST, DfT*

1. INTRODUCTION

Using fault detection techniques on electronic component/devices, manufacturers can enhance the good, reliable quality and operation of their respected products before shipping the products to their potential customers and speeds up the fault diagnosis in components/devices which leads to a faster repair of the faulty component and ultimately less down time for the device/machine that uses these component/devices.[1-4]

Current research projects have also adapted the use of the power supply current IPS for producing a good/fault signature and a reference metric good/fault classification. [5-11]

Several fault testing methods and techniques are utilizing both the static and the mixed signal specifications of mixed signal circuits such as ADC's and DAC's to produce a good/fault signature/metric for comparison. A summary of these specifications and the related work will be presented. Finally, a circuit implementation scheme using FPGAs will be proposed.

[1] This research has been co-financed by the European Union (European Social Fund – ESF) and Greek national funds through the Operational Program "Education and Lifelong Learning" of the National Strategic Reference Framework (NSRF) - Research Funding Program: **ARCHIMEDES III**. Investing in knowledge society through the European Social Fund.

2. METHODOLOGY – TESTING SPECIFICATIONS

The testing specifications are presented in the following paragraphs. Mixed signal IC's, such as ADC's and DAC's have static and dynamic specifications which are used by researchers in order to produce the good/fault signature and/or the classification metric. A complete set of these specifications can be found also in the data books of different manufacturers. The main static and dynamic specifications will be described below. The specifications to be described are:

- Static: Differential Non Linearity (DNL),Integral Non Linearity (INL), Gain-Offset Error
- Dynamic: Configurable Logic Blocks (CLB), Signal to noise ratio (SNR), Total Harmonic Distortion (THD), Signal to noise and Distortion ratio (SINAD), Effective Number of bits (ENOB)

2.1. Static Specifications

- **Differential Non Linearity (DNL),** is the maximum deviation between two neighboring codes. Ideally, a change of one LSB in digital code corresponds to one LSB analog voltage signal change for DAC's and vice versa for ADC's [3].
- **Integral Non Linearity** is defined as the maximum deviation of the ADC/DAC transfer function of a straight line from start to end point. Two main methods are used, the end point method and the best straight line method.
- **Gain-Offset Error** is the transfer function of a DAC/ADC which can be expressed from the function D=GA+K where D is the Digital code, A the Analog signal value and K, G are the offset and the gain respectively (K, G are constants). The Gain Error is the deviation between the theoretical value of G (given by the manufacturer) and the actual value of the device expressed as a percentage difference between the values. It can also be expressed in mV or LSB's.

2.2. Dynamic Specifications

- **Signal to noise ratio (SNR)** is the ratio of the rms signal amplitude without the 5 first harmonics over the mean value of the square root sum of all other spectral components except the DC component.
- **Total Harmonic Distortion (THD)** is defined as the ratio of the rms value of the primary frequency over the mean value of the root sum squares of its harmonics
- **Signal to Noise and Distortion Ratio (SINAD)** is the ratio of the rms signal amplitude, including the 5 first harmonics, over the mean

value of the root sum square of all other spectral components without the DC component.

- **Effective Number of bits (ENOB)** is defined by the following equation (1):

$$ENOB = \frac{\sin AD - 1}{6,02} \quad (1)$$

There are more static and dynamic specifications for ADC's and DAC's but the above mentioned specifications were widely used by researchers to extract their respective metric [1,2,4].

3. TESTING METHODS

The testing methods to be described are the following:

3.1. Basic testing method

The emerged Build In Self Test (BIST) technique partially solves the issue of a complex testing scheme, since it is integrated inside the component at hand. BIST can significantly reduce the production cost but can be impractical in many cases due to the fact that the BIST is more complex than the tested component or/and it occupies a large area inside the component.[1]

All the methods rely on the basic concept behind these testing schemes which is the comparison of the output response (signature) of the "non-faulty" Circuit Under Test (CUT) to the "faulty" one.

The output voltage of a good CUT's VOUT provides the signature against which the signatures of the "faulty" ones will be compared and classified according to the respective match. If the signatures match the CUT then it is classified as "good" and if the signatures don't match then the CUT's are classified as "faulty" [5].

A signature provided by measuring the power supply current IPS [6] gave a new interesting aspect to the ongoing research.

3.2. Input Stimulus

Different input signals and patterns are used for driving the CUT in order to produce the output signature. These signals, range from pure sinusoidal [7] to more complex signals such as multitone signals [8], impulse response [9] and pseudo-random patterns [10]. In some schemes there is no direct input signal but a positive or negative feedback from the output which drives the CUT to oscillate (Oscillation BIST) [11].

3.3. Classification methods

The output response or/and the IPS waveform from a series of CUTs measurements/simulations (signature) will compose a data base which will be the basis of the good/faulty classification. The respective signature of the good CUT will be compared to the signature of the Device Under Test (DUT) and will be classified accordingly. In order to classify the DUTs, a metric is used which derives from the spectral analysis [12], RMS and the mean value of the signature [13]. SNR, SINAD, THD [14] and other mixed signal static and dynamic specifications are also used to produce the classification metric. At start, the Euclid distance was used to compare the signatures. Current implementations introduced the wavelet packet spectral analysis [15], the Malahanobis distance [16],[17] and the Voltera series [9] as a classification metric.

4. CONCLUSIONS – FUTURE WORK

This paper provides the foundations of the future work and it will guide the selection of the method to be implemented. The aim is to develop external testing devices which will take the current signatures of positive, negative and ground power supply lines of the DUT and classify the DUT accordingly.

The IPS of the CUT (positive, negative power supply lines and ground line) will be sampled by an external Analog to Digital Converter to the FPGA. The sampled data are led to a Digital Filter, positioned into the Signal Processing Unit, located inside the FPGA and used for antiallizing and denoising purposes. After the filtering, the sampled data are led to the second stage of the signal processing unit also located inside the FPGA, At this stage, the signal processing unit will perform the spectral analysis of the IPS signature using Fast Fourier Transformation (FFT) and Discrete Wavelet Transformation (DWT) algorithm to extract the energy of the signature. The rms and mean values of the IPS signature will be also calculated in the same unit. All these features will provide the necessary information to create a signature data base for comparing the “good” circuits against the measured CUTs for the good/fault classification.

The comparison will be executed after the CUT’s signature is extracted. Both signatures, good and the DUT’s will be compared with the help of a distance metric. The Malahanobis distance metric may be used, which is similar to the Euclid distance metric but more efficient as an algorithm. This comparison will lead to a good/fault classification.

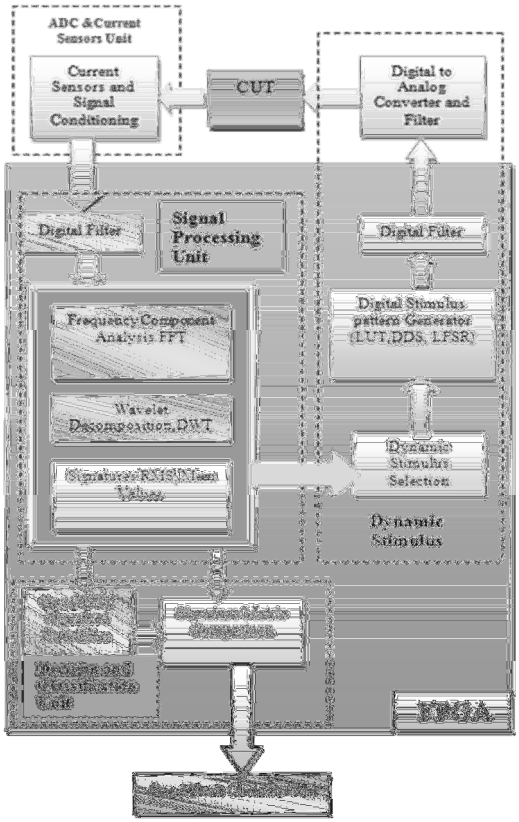


Fig. 1: Block Diagram of our future implementations.

The novelty that will be introduced is the Digital Stimulus Pattern Generator incorporated inside the FPGA. Its purpose is to apply the correct digital or analog signal (after a D/A conversion) to the CUT according to the specification of the CUT. When a CUT cannot be classified from the signature taken for a specific stimulus, then the pattern generator will create a new stimulus that will provide a new signature for comparison. This stimulus will be created by LUT's, DDS and LFSR. The Stimulus will be also user selectable depending on the CUT.

The A/D conversion of the current sampling and the D/A conversion for the CUT stimulus will be done externally and all the digital processing, filtering, frequency component analysis, metric extraction and final good/faulty classification will be implemented inside the FPGA. FPGA's can be significantly faster than any conventional DSP and they have parallel processing capabilities which can be very useful in simultaneous processing algorithms.

5. REFERENCES

[1] Lee D., Yoo K., Kim K., Han G., Kang S., (2004), "Code-Width Testing-Based Compact ADC BIST Circuit." IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—II: EXPRESS BRIEFS, VOL. 51, NO. 1.

[2] Olleta B. ,Jiang H., Chen D., Geiger R., (2009),"Methods of testing analog and mixed signal using dynamic element matching for source linearization", US Patent Number:7.587.647B2.

[3] Maxim Integrated, INL/DNL Measurements for High-Speed Analog-to-Digital Converters (ADCs), Available: http://www.maxim-ic.com/app-notes/index.mvp/id/283 (accessed February 20, 2013)

[4] Kester W., Bryant J., "Sampled Data Systems" Available: http://www.analog.com/static/imported-files/seminars_webcasts/ MixedSignal_Sect2.pdf (accessed February 20, 2013)

[5] Stroud C. , (2002), "A Designer's Guide to Build-In Self Test", New York: Kluwer Academic Publisher.

[6] Bell I., Sprinks S., Dasilva J., (1996), "Supply current test of analog and mixed-signal circuits", Proc. Inst. Elect. Eng.-Circuits Devices Syst., vol.143,no 6, pp 399-407.

[7] Park J., Abraham J., (2008), "Parallel Loopback Test of Mixed-Signal Circuits", Proc IEEE VLSI Test Symposium.

[8] Sindia S., Singh V., Agrawal V., (2009), "Multi-Tone Testing of Linear and Nonlinear AnalogCircuits using Polynomial Coefficients", Proc. Asian Test Symposium.

[9] Park J., Chung J., Abraham J., (2009), "LFSR-based performance chartacterizartion of nonlinear analog and mixed signal circuits", Proc. Asian Test Symposium.

[10] Marzocca C., Corsi F. , (2002), "Mixed-Signal Circuit Classification in a Pseudo-Random Testing Scheme", Journal of ElectronicTesting:Theory and Applications 18,333-342.

[11] Arabi K., Kaminska B., (1997), "Efficient and Accurate Testing of Analog-to-Digital Converters Using Oscillation-Test Method", ED&CT 97.

[12] Dimopoulos M., Spyronasios A., Papakostas D., Konstantinou D., Hatzopoulos A., (2010), "Circuit implementation of a supply current spectrum test method", IEEE Trans.Instrum.Meas., vol. 59, no,. 10, pp.2660-2670.

[13] Zwolinski M., Chalk C., Wilkins R., Suparjo S., (1996), "Analogue Circuit Test using RMS Supply Current Monitoring".

[14] Toner M., Roberts G., (1993), "A BIST scheme for an SNR test of a sigma-delta ADC", IEEE Int. Proc. Test. Conference

[15] Dimopoulos M., Spyronasios A., Papakostas D., Hatzopoulos A., (2010), ”Wavelet energy-based testing using supply current measurements”, IET Sci., Meas. Tech., vol. 4, no. 2, pp76-85.
[16] Dimopoulos M., Spyronasios A., Hatzopoulos A., (2011), ”Wavelet analysis for the detection of parametric and catastrophic faults in mixed-signal circuits”, IEEE Trans. Inst. Meas. vol. 60, no. 6.
[17] Kalpana P., Gunavathi K., (2007), ”A novel implicit parametric fault detection method for analog mixed signal circuits using wavelets” ICGST-PDCS Journal, vol. 7,Issue.1.

Vulnerability issues on research in WLAN encryption algorithms WEP WPA/WPA2 Personal

Lazaridis Ioannis, Pouros Sotirios, Veloudis Simeon

DEI College, Thessaloniki, Greece

Abstract: *This paper presents historic and new evidence that wireless encryption algorithms can be cracked or even bypassed which has been proved by other researchers. The paper presents a description of how WEP and WPA/WPA2 Personal encrypt data and how the passphrase is shared between the nodes of the network. Modern tools available on the internet have been evaluated, decomposed and tested to provide evidence on the reliability of passwords. A number of criteria are used to compare the tools and their efficiency.*

Keywords: *WLAN, security algorithms, encryption methods, passphrases, Backtrack, cracking tools*

1. INTRODUCTION

A wireless LAN (WLAN) is a network in which a user can connect to a local area network (LAN) through a wireless connection. Since most modern WLANs are based on IEEE 802.11 standards the term “Wi-Fi” is used as a synonym for “WLAN”. Nowadays, WLAN devices are commonly used by everyone, mostly because of the need to connect to the Internet. [1] At home, at work, even public places such as local café and shopping centers people are able to connect to the Internet via a Wi-Fi device connected to a Wi-Fi Access Point (AP).[2] The issue here is that almost nobody actually cares if the connection just established is safe or not. Most people have heard the terms authentication, encryption, WEP, WPA and WPA2 but only few knows how they work and even fewer knows how they can be cracked or even bypassed.

1.1. WEP

In WEP authentication a wireless device sends an authentication request to the access point which will reply with a 128 bit challenge in a clear text.[3] The client will sign that challenge with the shared secret key and send it back to the access point. The AP will decrypt the signed message (uses the same shared key as client did) and verifies the challenge sent. If the challenge matches, then the authentication has

succeeded and the client is able to access the WLAN. It must be noted that the same key is used for authentication and encryption so this kind of authentication is prone to man in the middle attacks (There is no way to distinguish if the subsequent messages are from a legitimate client or an impostor). The encryption process between an AP and a client WEP uses RC4 stream cipher. WEP uses 8-bit RC4 and operates on 8-bit values by creating an array with 256 8bit values for a lookup table. WEP also uses CRC (Cyclic Redundancy check) for data integrity. It performs a CRC checksum on the plaintext and generates a CRC value. Then that value is concatenated to the plaintext, thesecret key is concatenated to the Initialization Vector (IV) and given into theRC4. RC4 creates a keystream that is based on the secret key and the IV. The keystream and the CRC+plaintext message are XOR'ed. The result of that is called ciphertext. The same IV that was initiallyused is presented in clear text to the resultant ciphertext. The IV plus the ciphertext along with the frame headers are then transmitted over the air.

1.2. WPA

WPA includes dynamic key generation, an improved RC4 data encryption that uses TKIP and 802.1x authentication.[4] It can provide data protecting and ensure that only authorized users can access the WLAN. At this point, the importance of TKIP must be stated since it employs a pre-packet key, meaning that it automatically generates a new key (128 bit) for every packet. This means that static key attacks can not affect WPA. WPA has also replaced the cyclic redundancy check (CRC) that WEP uses as an integrity check since it didn't provide a strong data integrity guarantee. The integrity check algorithm used is called Michael or MIC which is stronger that CRC but as past researches has shown MIC has a flow because of its limitation to retrieve the keystream from short packets to use for re-injection or even spoofing. TKIP uses a master key which is distributed using 802.1x or PSK (in that case it derives a pairwise master key). Pairwise master key is used in order to get four other keys. These keys are used during the encryption. One of these four keys is called temporal key which is used to encrypt data over the WLAN. The temporal key is XORed with the MAC of the transmitter and then is mixed with a sequence number in order to produce a key that is used as input to the previous WEP algorithm. [5] It must be noted that by adding all these steps, the key becomes much more secure since now it depends on time and the transmitter's MAC. The source and the destination addresses are added along with the sequence number.MSDU stands for MAC Service Data Unit and MPDU stands for MAC Protocol Data Unit.

1.3. WPA2

Authentication in WPA2 is performed between the client and the access point by generating a 256-bit PSK from a plaintext passphrase (8-63 characters long).[6] The PSK in conjunction with the SSID and the SSID length form a mathematical basis for the PMK (Pair-wise Master key) to be used in key generation. In order to generate the key, there is a need of two handshakes, a four way handshake for PTK, GTK derivation and a group key handshake for GTK renewal. SinceWPA2encryption is compatible with TKIP and AES we will focus on AES. [7] For AES, the MIC is calculated using a 128-bit IV. The IV is encrypted with AES and TK in order to produce a 128-bit result. This result is XORed with the next 128 bits of data. The result of that XOR is then passed through the first two steps until all 128 blocks in the 802.11 payload are exhausted (AES uses groups of bits of a fixed length – called blocks). Finally the first 64 bits are used to produce the MIC.Since the MIC is created the counter mode algorithm encrypts the data and the MIC. It begins with a 128-bit counter preload similar to the MIC IV, but it uses a counter value initialised to one, instead of a data length resulting in another counter used to encrypt every single packet. In order to encrypt the data and the MIC,the counter has to be initialised (if it is the first time) otherwise the counter has to be incremented. Then, the first 128 bits are encrypted by using AES and TK in order to produce a 128-bit result. A XOR is performed on that result which is going to be used later. The first 128 bits of data produce the first encrypted block (128-bit). The same procedure is repeated until all 128-bit blocks have been encrypted. Then the counter is set to zero and it is encrypted using AES and XOR with MIC appending the result the encrypted frame.

2. METHODOLOGY

Technical Specifications:

Machine used: Samsung RV515

Processor: AMD Dual Core Processor E-450 (1.65GHz, 1MB L2 Cache)

Memory: 4GB DDR3 System Memory at 1066MHz (4GB x 1)

Graphics Adapter: AMD Radeon HD6470M

NIC: Alfa AWUS036H – 5 dB Antenna

[11]**O/S:** Backtrack 5 R3

2.1. WEP

Tab.1: RAM consumption in standby during injection and cracking.

	RAM/standby	RAM/injection	RAM/cracking
FERN	150 MB	840 MB	1.2 GB
Gerix	142.4 MB	178 MB	198 MB
Airdump-ng	139.2 MB	146 MB	148 MB

Tab. 2: CPU consumption in standby during injection and cracking.

	CPU/standby	CPU/injection	CPU/Cracking
FERN	30.6%-20.3%	100% x2	100% x2
Gerix	11.1%-24.6%	36.7%-50.0%	72.2%-99.9%
Airdump-ng	9.7%-25%	71.2% - 72.5%	48.5%- 30.0%

2.1.1. WEP encryption: 64 bit

Passphrase: 12345

Tab. 3: Time and IVs needed in order to crack the 12345 password.

	Time to decrypt	IVs needed
FERN	00:22,0	18,500
Gerix	00:20,6	8,500
Airdump-ng	00:14,5	8,000

Passphrase: 1234554321

Tab. 4: Time and IVs needed in order to crack the 1234554321 password.

	Time to decrypt/12000 Ivs	IVs needed
FERN	01:01,6	14,700
Gerix	02:02,6	11,000
Airdump-ng	01:57,1	11,900

2.1.2. WEP encryption: 128 bit

Passphrase: 1234567890123

Tab. 5: Time and IVs needed in order to crack the 1234554321 password.

	Time to decrypt/12000 Ivs	IVs needed
FERN	04:24,1	48.800
Gerix	03:10,5	39,200
Airdump-ng	03:03,2	32,500

Three tools were used to grab and replay ARP packets into the network. [8] This cause the network to send ARP replay packets, thus increasing the number of packets sent. After that WEP key was cracked by analysing cryptographic weaknesses in the packets that I have sniffed (the ARP packets).

2.2. WPA

Tab. 6: RAM and CPU consumption while cracking.

	RAM/cracking	CPU/Cracking
FERN	320 MB	100% 40%
Gerix	218 MB	100%-38%
Airdump-ng	204 MB	100%- 38%

Tab. 7: Time required to find the passphrase (Zealotsk) which is at the end of the dictionary.

	Time to find the passphrase
FERN	00:53,6
Gerix	00:52,1
Airdump-ng	00:52,0

Tab. 8: Time to find the passphrase (Zealotsk) which is at the middle of the dictionary.

	Time to find the passphrase
FERN	00:33.6
Gerix	00:34,2
Airdump-ng	00:33,3

A dictionary attack was performed, using the same three tools as WEP. The dictionary list used contains movie characters and 26,707 words. For the first test the last word of the dictionarywas chosen which was zealotsk (The sk was added at the end since at least 8 characters were required). For the second test the same word had been placed right at the middle of the list (position: 13353). [9] It must be mentioned that all of the tools were able to grab the WPA handshake in a matter of seconds (5-10) but it is not something that it can be measured precisely since it was always random. It is really important to understand that all these tools do not actually crack WPA, but they crack the WPA handshake protocol. Finally, these tools are able to use both .txt .lst files.

2.3. WPA2

Tab. 9: CPU consumption in standby during injection and cracking.

	RAM/cracking	CPU/Cracking
Reaver	531 MB	100% 100%

Tab.10: Time needed to crack PIN in seconds, minutes and hours.

Seconds to crack the PIN	Minutes to crack the PIN	Hours to crack the PIN
31861	531.016666667	8.874509091

Since a Dictionary attack was already demonstrated for WPA, it was decided that another tool is going to be used which is called Reaver. [10] The main concept is to brute-force attack the AP itself, attempting every single possible combination in order to find the AP's 8 digit PIN number and get all the credentials of the AP. This makes it a lot of easier than a simple brute force attack, in case a dictionary attack is useless, since AP's WPS pin uses only numeric characters. This means 10^8 (100,000,000) possible combinations, but since the last digit of the pin is a checksum value, which can be calculated based on the previous 7 digits, that key length is reduced to 10^7 (10,000,000) possible values. It took 8.8 hours to crack the PIN and get the passphrase. Based on an [12] online password calculator a simple brute force attack in a complex passphrase of 8 characters would take approximately 10800 years. Finally, we have to realise that even if the passphrase is changed by a legitimate user we are able to find it once again but now without waiting 5 to 10 hours since we have the PIN number. A test was performed every time the passphrase was changed, but after 4 seconds the reaver tool was able to find the new passphrase since the PIN number was applied to it.

3. CONCLUSIONS

This research has proven that even with a low processing power and free software, it is possible for someone to bypass/crack every security protocol in matter of hours or even minutes. The latest security protocol (WPA2) was introduced back in 2004; it is obvious that wireless LAN is not as safe as they are supposed to be since the security mechanisms they use are out of date.

4. REFERENCES

[1] Pahlavan, Kaveh; Krishnamurthy, Prashant (2009). Networking Fundamentals – Wide, Local and Personal Area Communications. Wiley.
[2] Wale Soyinka, (2010) Wireless Network Administration. USA: McGraw-Hill
[3] WIFI-Fi Alliance: Organization. Official industry association web site.
[4] SA Standards Board. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Communications Magazine, IEEE, 2007
[5] Ciampa, Mark (2006). CWNA Guide to Wireless LANS. Networking. Thomson
[6] Wolter Lemstra , Vic Hayes , John Groenewegen , (2010)The Innovation Journey of Wi-Fi: The Road To Global Success, Cambridge University Press)
[7] Bulk, Frank.(27/1/2006) Learn the basics of WPA2 Wi-Fi security. Network Computing http://www.informationweek.com/story/showArticle.jhtml?articleID=17710533 (accessed March 18, 2013)
[8] Vivek Ramachandran, (2011) Backtrack 5 Wireless Penetration Testing. Birmingham, UK: Pactk Publishing Ltd.
[9] Viehbock, Stefan (26 December 2011). Brute forcing Wi-Fi Protected Setup
[10] Reaver tool website - http://www.tacnetsol.com/products (accessed March 18,2013)
[11] BackTrack Linux – Penetration Testing Distribution http://www.backtrack-linux.org (accessed March 18, 2013)
[12] Password Calculator - http://lastbit.com (accessed March 18, 2013)

Experimental studies of the web server defenses against TCP SYN Flood attacks

Nina Sinyagina, Stela Ruseva

Faculty of Mathematics and Informatics

Sofia University St. Kliment Ohridski

Abstract: *DDoS attacks are accomplished by the combined actions of variety of program components available on Internet hosts. A system for protecting against DDoS attacks was developed. DDoS attacks launched by SYN floods can be very problematic for servers that are not properly configured to handle them.*

A system for protection Ruslan has been developed, aiming at overcoming the DDoS attacks. It changes parameters of the OS core and basic configuration files. The system contains additional modules. It has a stable performance under real conditions - DDoS attacks. Its ability to keep the performance of the web server has been proved.

A survey of the problem and the long-term mechanisms of defense against attacks was made.

Keywords: *Network Security, Distributed Denial of Service (DDoS) attack, defense system.*

1. DESCRIPTION OF THE PROBLEM

The attack leading to the impossilbility to get information or to get computer systems function without being overlodded is called DoS - (Denial of Service). This kind of attack hamper or fully block the leagal users responses to services. A protective system, aiming at defending a web server against DDoS attacks has been developed. The system changes some parametres of the OS as well as basic configuration files and contains additional modules. Basic elements of the protective Ruslan system are the parametres of the OS core, the TCP/IP stack and the script[1-4] for iptables.

The configuration of the HTTP server used for the study is:
Processor: Intel Core i3-2120 CPU, 3.30 GHz, 3M Cache
Processor speed: 3.30 GHz
RAM memory: 8 GB

Network adapter: 3Com Typhoon (3CR990-TX-97) at MMIO 0xecf80000, 00:01:03:e6:65:e9

OS: CentOS Linux release 6.0 ; Linux version 2.6.32-71.29.1.el6.i686

gcc version 4.4.4 20100726

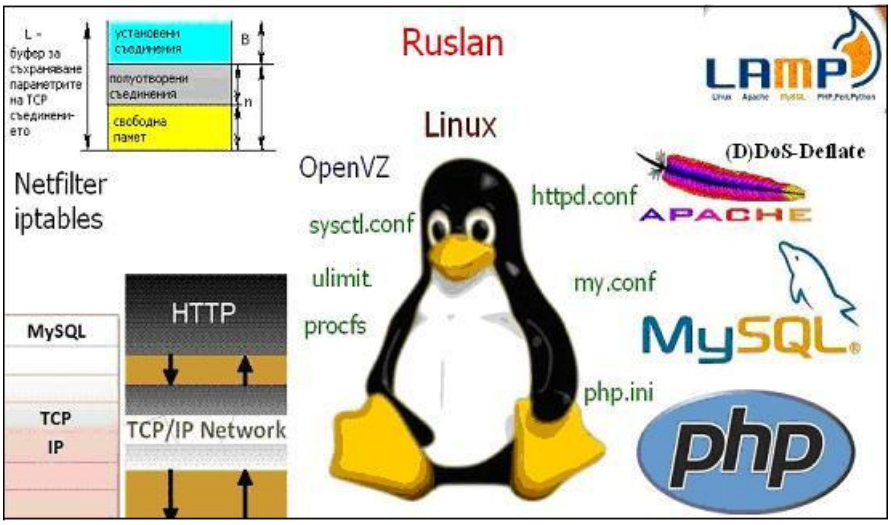


Fig. 1: Ruslan protective system against DDoS attacks.

The following command shows the default parametres of the TCP/IP stack variables as well as those of the netfilter (standart network filter for OS GNU/Linux):

cat /etc/sysctl.conf

The size of the table for the number of simultaneous connections through:

net.ipv4.netfilter.ip_conntrack_max = 1515072

The protection against arp table overflowof the network interface (Neighbour table overflow):

net.ipv4.neigh.default.gc_thresh1 = 2048
net.ipv4.neigh.default.gc_thresh2 = 4096
net.ipv4.neigh.default.gc_thresh3 = 8192
net.ipv4.tcp_mtu_probing = 1

Maximum number of simultaneous connections to the socket:

net.core.somaxconn = 4096

TCP keepalive is virtually swtched off:

net.ipv4.tcp_keepalive_time=1

The number of the packets keepalve which will be sent by the server before closing the connection is:

net.ipv4.tcp_keepalive_probes=1
net.ipv4.tcp_keepalive_intvl = 10

Decreasing the time to refuse the connection by default is 5 days, which is too much.
net.ipv4.netfilter.ip_conntrack_tcp_timeout_established = 28800

The buffer dimentions by default for receiving and sending data through sockets are set to 256 KB:
net.core.rmem_default = 262144
net.core.wmem_default = 262144

Maximum size of packet backlocks:
net.core.netdev_max_backlog = 8192

The maximum size of the TPC buffers is increased to 16MB:
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216

The minimum, standart and maximum size of the autoconfiguration limits for TCP and UDP buffers in bytes is increased:
net.ipv4.tcp_rmem = “8192 87380 8388608”
net.ipv4.tcp_wmem = “8192 65536 8388608”

net.ipv4.udp_rmem_min = 16384
net.ipv4.udp_wmem_min = 16384

net.ipv4.tcp_mem = “8388608 12582912 16777216”
net.ipv4.udp_mem = “8388608 12582912 16777216”

Priority for start of swapping (from 0 to 100):
vm.swappiness = 70

The backlock of the half-open connections is increased
net.ipv4.tcp_max_syn_backlog=4096

The parametre tcp_synack_retries controls the numler of the retranslations[5] in OS GNU/Linux. It is 5 by default, which means deleating of a

half-open connection in 3 minutes. The transmission is set to be realised up to the third second and the full time for saving of the half-open connections in the backlock is fixed to 9 seconds:

net.ipv4.tcp_synack_retries=1

The timeout for FIN wait until final close of socket:

net.ipv4.tcp_fin_timeout = 10

Permission to support a large scale window for TCP protocol (according to RFC1323 – a highperformance protocol):

net.ipv4.tcp_window_scaling = 1

Increase of the number of the accessible network ports:

net.ipv4.ip_local_port_range = “16384 61000”

To avoid the peculiarities when decreasing the size of the sliding window (because of transmitting packets for a second time) for a single connection, the size of the window for all other connections with this host has to be decreased:

net.ipv4.route.flush=1

Cashing of the status ssthresh (slow start threshold limit) for the other connections:

net.ipv4.tcp_no_metrics_save = 1

Changing the congestion control dlgorithm:

net.ipv4.tcp_congestion_control=htcp

The core is set not to answer a broadcast ping. Each ICMP message, answering a broadcast or a group address is ignored. There has to be written:

net.ipv4.icmp_echo_ignore_broadcasts = 1

TCP syncookies are used(against TCP SYN packet flooding):

net.ipv4.tcp_syncookies = 1

To mislead programs of nmap type, which can identify a OS by the network stack characteristics, the TTL size by default of 64 has to be changed and number 128 has to be written in the file ip_default_ttl:

net.ipv4. ip_default_ttl = 128

Selective acknowledgements are banned, RFC2018 (net.ipv4.tcp_sack):

net.ipv4.tcp_sack=0

How often a connection , closed by the defender has to be killed is determined by:
net.ipv4.tcp_orphan_retries=1

The rp_filter is switched on (IPsrc verification, defense against IP spoofing):
net.ipv4.conf.all. rp_filter=1

Packets with impossible addresses to get logged have to be refused:
net.ipv4.conf.all. log_martians =1

Protection against bogus responses to broadcast requsts written in a log file:
net.ipv4.icmp_ignore_bogus_error_responses = 1

ICMP Redirect is switched off:
net.ipv4.conf.all.send_redirects=0
net.ipv4.conf.all.accept_redirects=0

Routing, defined by the IPsrc source, is switched off:
net.ipv4.conf.all.accept_source_route=0

Multicast dispatch support is switched off:
net.ipv4.conf.all.mc_forwarding=0

2. EXPERIMENT DESCRIPTION

A number of experiments have been made to evaluate the deny of service by (or without) using Ruslan protective system when flooding a a web server with TCP SYN packets.

To guarantee the neatness of the experiment, a version for connection without intermediate routers has been chosen because the administrator of each intermediate router sets rules to filtrate their networks by themselves, which could influence results.

In the experiment, by using a 16 port switch web server, 15 machines were connected in a local network, which were used simultaneously as attacking machines and as clients . The switch model is Cisco Linksys SR2016T-EU 16-Port 10/100/1000 Gigabit Switch (SR2016T-EU).

The 16 ports switch over at the rate of 32 Gbps. The channel capacity is 23,8 million packets per second.

Configuration of hosts(clients and attacking) interacting with the HTTP server:

Processor: Intel® Celeron® 2.00 GHz
Processor speed: 2.00 GHz
RAM memory: 512 MB
Network asaptor: 100Mb/s Ethernet
OC: CentOS Linux release 6.0; Linux version 2.6.32-71.29.1.el6.i686
gcc version 4.4.4 20100726 (Red Hat 4.4.4-13)

. . . . . .

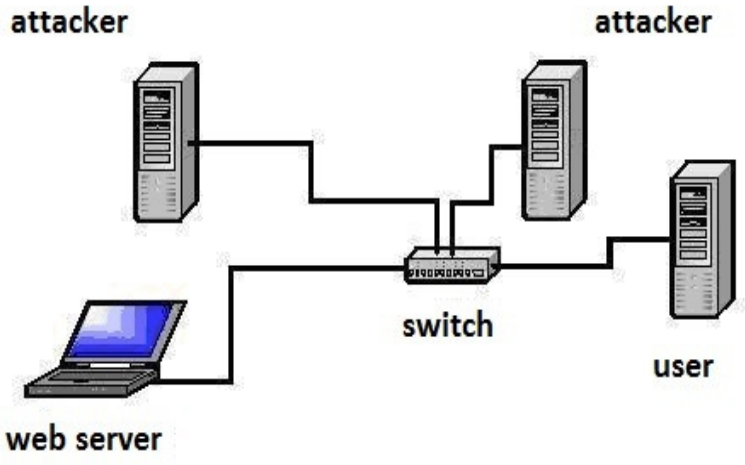


Fig. 2: Topology of the experimental network.

The IPTraf program, which was started on the web server, is used to measure the input and output traffic in packets/ sec. The registered through IPTraf traffic трафик pulsates, so, the tables indicate average values.

The computers, alleged to be attacking hosts generate TCP SYN packets, which simulate SYN flooding. A program used for the purpose sends packets to the web server without the defence of Ruslan system from a single host. The web server registers 47 thousand packets per second and manages to respond to only 11 thousand packets per second. This proves that the system has resource to respond to less than a quarter of the received requests. When two hosts attack, the resource is drained again. The system registers 32 thousand and responds to 7 thousand packets. It

is obvious the resources are drained and this shows that there is TCP SYN flooding (DDoS attack).

3. EXPERIMENTAL RESULTS

It is experimentally proved that the server fails when attacked by 7 hosts but when Ruslan is used it functions even if it is attackes by all 15 machines.

Tab. 1: Generated input and output traffic at the web server without Ruslan defence system.

Number of attacking machines	Input traffic, packets/sec	Output traffic, packets/sec
1	47000	11000
2	32000	7000
3	30000	6000
4	28000	5000
5	25000	4000
6	22000	3000
7	17000	1000
8	10000	900

Tab. 2: Generated input and output traffic at the web server with Ruslan defence system.

Number of attacking machines	Input traffic, packets/sec	Output traffic, packets/sec
1	25000	5500
2	19000	3600
3	17000	3500
4	16000	3400
5	14500	2500
6	13000	1550
7	9800	1200
8	9400	1100
9	8600	900
10	8000	850

4. CONCLUSIONS

As a result of the studies and the analysis made, there can be drawn the following conclusions:

1. An experimental evaluation has been made of the denial of service with/without the use of Ruslan defending system against DDoS attacks due to web servers flooding with TCP SYN packets.

2. The steady work of Ruslan under a real DdoS attack was experimentally proven. Its ability to keep the working capacity of the web server was confirmed.

3. Ruslan manages to keep the capacity of the web server at maximum flooding with false requests to the attacked system, related to the channel capacity and hardwere devices. Without the help of Ruslan the web server fails to serve the clients even at much lower levels of input flow of requests.

5. REFERENCES

[1] CERT. “TCP SYN Flooding and IP Spoofing Attacks.” CERT Advisory CA-1996-21. http://www.cert.org/advisories/CA-1996-21.html

[2] Ipsysctl-tutorial, Oskar Andreasson, http://www.frozentux.net/documents/ ipsysctl- tutorial/

[3] RFC 4614 Duke, M., Braden, R., Eddy, W., Blanton, E. A Roadmap for Transmission Control Protocol (TCP) Specification Documents, 2006

[4] Slavov Z., and V. Hristov, BUILDING AN UNIVERSAL NETWORK SECURITY MODEL, Proc. of the Conference ELECTRONICS ET’2006, Sozopol, September 20-22, 2006, pp. 3- 8.

[5] V. Hristov, SIMULATION OF TRANSMISSION CONTROL PROTOCOL Proc. of the Conference SCICE’05, Sofia, 2005, pp. 74-78.

Simulation of aggregation mechanism with fragments retransmission

Valentin Hristov*, Bzar k. Hussan, Firas Ibrahim***, Gergana Kalpachka***

**South-west University "Neofit Rilski"- Blagoevgrad, Bulgaria*
***Hawler Polytechnic College "Erbil Technical Institute"-Erbil, Iraq*
****University Of Tabuk- Tabuk, Kingdom Saudi Arabia,*

1. INTRODUCTION

Modern wireless computer networks offer more high-speed data transmission in the physical layer (PHY) and using highly efficient protocols in the Media Access Control layer (MAC)to access the communication medium.

High-speed of physical layer does not lead directly to increased efficiency of the MAC layer. The reason is that increasing speed leads to faster transmission of the MAC part (in frame), but the transmission time of PHY header and the backoff time of avoiding conflicts has not decreased substantially. For example, the new 802.11n standard offers speeds up to 600 Mbps and improvements in the MAC. Transmission time of PHY header, however, is 48 μs. The maximum size of frame is limited to 7955 B. Thus, at a speed 150 Mbps, the time for transmitting user data is 424 μs, which means the proportion of transmission time for the header in frame is more than 10%. It is known that even under the best conditions, the efficiency of MAC layer (MAC_Layer_Speed/ PHY_Layer_Speed) in 802.11n fall from 42% at a speed of 54Mbps to only 10% at speed of 432Mbps [9].

Appropriate solution to overcome this phenomenon in high-speed wireless networks is the use of mechanisms for aggregating packets.

Most studies of mechanisms for aggregating packets using models in which traffic has a Poisson or Bernoulli distribution. These models cannot capture the strong correlative nature of actual network traffic and the sequence of wrong packets (burst error).

The aim of this paper is to propose a simulator of aggregation mechanism with fragments retransmission, taking into account time-varying radio channel characteristics and their strong relation with errors.

2. MODIFIED MECHANISM FOR AGGREGATION WITH FRAGMENTS RETRANSMISSION

In the aggregation mechanism with fragment retransmission -AFR, multiple packets are aggregated into one large frame to be sent. Using technology of fragmentation, whereby if the packets are larger than a threshold, they are split into fragments that are re-transmitted in case of loss, rather than retransmitting of whole aggregated frames.

In order to AFR mechanism would improve delays in aggregation in the literature [2] is proposed aggregation to do with utilization above a certain threshold. In low intensity of arrival packets in the buffer, respectively utilization ($\rho = \lambda/\mu$) below this threshold, aggregation is not done, and each new arrival packet formed frame.

In AFR mechanism, the MAC frame consists of a header and body (Fig. 1). All fields of the MAC header remain unchanged, only three new fields added - size of fragment, number of fragment and reserved field.

The body of frame contains the headers of fragments and the bodies of fragments and control field for checking the corresponding fragment (FCS-Fragment Check Sequences). Each header fragment consists of six fields: ID of the packet (PID), length of the package (pLEN), start position (startPos), offset field (offset), reserved for future use fields and FCS. StartPos is used to indicate the position of body fragment in the frame and offset (offset) is used to record the position of this fragment in the packet.

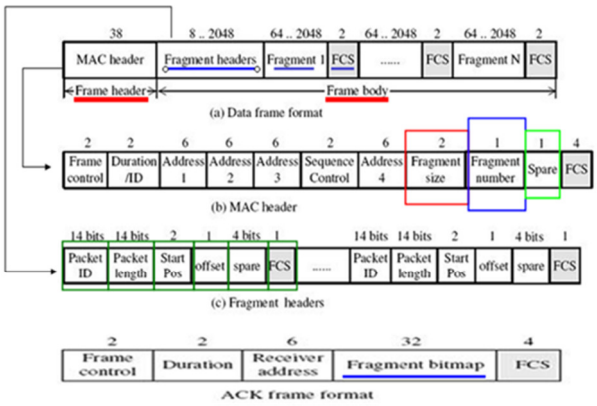


Fig. 1: A-AFR Frame formats.

3. SIMULATION MODEL

The A-AFR mechanism and more precisely the transmitter assigns unique identifier (ID) to each fragment in the aggregated frame (Fig.1). In the receiver side fragments of a packet are concatenated according to their IDs. After the transmission of aggregated frame, constituent fragments temporarily buffered while the acknowledgement frame (ACK frame) arrives back to the transmitter. This happens with some delay (see feedback in Fig. 2). In case that a positive acknowledgment (ACK) arrives for given fragment, this fragment will be removed from the retransmission buffer (waiting buffer). If the acknowledgement arrives negative (NACK) – the fragment will be transmitted again.

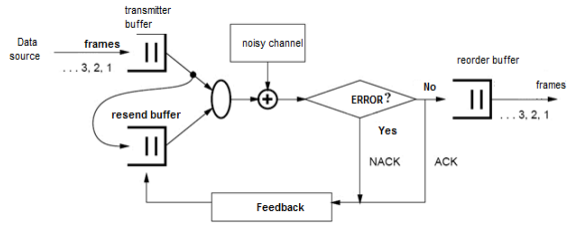


Fig. 2: Packets transmission over wireless network.

Although the transmitter sends fragments of packets in the correct order, the order of the fragments into the receiver may be broken due to the occurrence of errors, respectively retransmission. So correctly received fragments have to wait in a buffer until the lost fragments (with the missing IDs) are received correctly. The buffer for re/sequencing is located in the receiver. Once all fragments of an aggregated frame arrive, they are released from resequencing buffer (in the correct order) and packets are forwarded to the upper levels.

Fig. 3 shows the various delays that fragments of packets undergo in their transmission across a wireless network using the A-AFR protocol. Total delay- Tt is the delay for packets transport, including the delivery delay- Td and the delay in the transmitter queue also called queuing delay- Tq. The delay Tt is the time elapsed since the first transmission (of fragments) of the packet until the moment in which this packet leaves resequencing buffer. The delay in the transmitter queue (Tq) is defined as the elapsed time from the arrival of packets in the buffer to the first attempt of transmission. Delivery delay (Td) includes delay of retransmission and delay of rearranging. The retransmission delay is defined as the time elapsed since the first transmission of the fragment until it successfully arrives at the receiver. Delay for rearrangement of packet fragments (resequencing delay) is equal

to the time that the packet waits until all its fragments arrive in resequencing buffer.

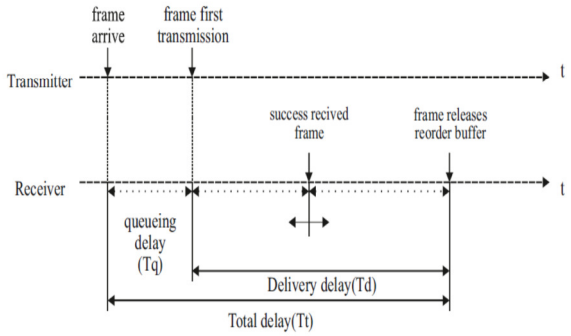


Fig. 3: Timeline of transmission process.

The generation of the input stream in the model is achieved by ON-OFF process. Modeling of time-varying radio channel is also used ON-OFF process.

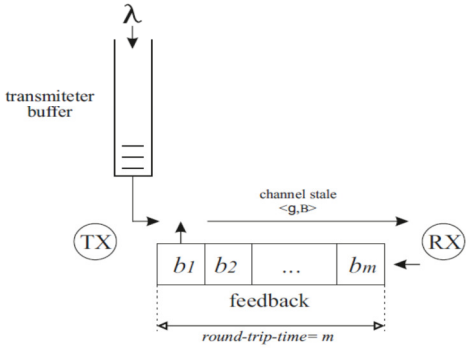


Fig. 4: Queuing system.

In the queuing system we assume that a fragment is transmitted per slot (the time in model is slotted). The time in which an information comes for the status of the fragments of an aggregated frame (round-trip-time) is equal to m slot (Fig. 4), where *m>1*. This means that the available packets in the buffer are fragmented, aggregated and transmitted, but will not leave the queuing system before waiting at least m slots.

The arriving of fragments of packets in the buffer of transmitter is described by:

- Intensity of the arrival packets - λ.
- Average number of packets in one aggregated frame –p.
- Average number of 128B fragments in a packet - L.

The last parameter characterizes the process of fragmentation of packets, i.e. the average number of fragments aggregated in one frame is A = p.L.

New arrival packet is immediately transmitted [9] only when the buffer is empty as well as there is no request for retransmission of fragment/s of earlier transmitted packet. This is because retransmission of the fragments has a higher priority than fragmentation, aggregation and transmission of newly arrived packets.

The sent data from the transmitter reaches the receiver on radio channel in which there is interference which can lead to loss of fragments. In the proposed model this error prone channel is also modeled by ON-OFF generator (process with two states) and is described by parameters:

- Error probability of the channel also called channel error probability- ε;
- Average error burst length (length of the sequence of lost fragments due to the packet error)- B.

The receiver responds with a positive or negative acknowledgment (ACK / NACK) depending on whether the fragment was received without errors or with errors. After the round-trip-time, i.e. after m slots the transmitter gets feedback (ACK/ NACK) and then starts transmission of a new aggregated frame or retransmission of lost fragment/s (for which is arrived a negative acknowledgement - NACK). Corresponding flags - *bi (i = 1, 2, ... m)* are used to model the result of transmission in *mi* slot, where *bi = 1* - means that the transmission of *i*-th fragment is not successfully and its retransmission is necessary, otherwise i.e. *bi = 0* and the transmission is successfully.

In the proposed model is assumed that no errors occur in transmission of acknowledgements (ACK / NACK), i.e. all acknowledgements arrive to the transmitter.

General Purpose Simulation System (GPSS) has been chosen to create simulator for evolution of the A-AFR mechanism. The proposed modeling approach reflects the requirements and limitations of the GPSS language environment and accurately describes the parameters and the processes in the wireless network.

4. CONCLUSION

In this paper simulation model and GPSS simulator of aggregation mechanism with fragments retransmission have been developed in order to

examine performance of the adaptive mechanism for aggregation with retransmission of fragments.

5. REFERENCES

[1] N. Ghazisaidi, M. Maier and C. Assi, "Fiber-Wireless (FiWi) Access Networks: A Survey", IEEE Communications Magazine, February 2009, pp 160-167.

[2] J. Xie and X. Wang, "A Survey of Mobility Management in Hybrid Wireless Mesh Networks", IEEE Network, November/December 2008, pp 34-44.

[3] J. Hong and K. Sohraby, "On Modeling, Analysis, and Optimization of Packet Aggregation Systems", IEEE Transactions on Communications, vol. 58, no. 2, February 2010, pp 660-668.

[4] L. Taneva, " Intelligent Module for Data Exchange using CAN Interface", CEMA'09, 8-10 October 2009, Sofia, Proceedings p.102-104.

[5] R. Jain, C. So-In and A. Tamimi, "Level Modeling Of IEEE 802.16e Mobile Wimax Networks: Key Issues", IEEE Wireless Communications, October 2008, pp 73-79

[6] V. Hristov, , B. Tudzharov, Adaptive mechanism with aggregation and fragment retransmission for highspeed wireless networks, Bulgarian Journal of Engineering Design, No 7, February 2011, pp. 15-22 (in Bulgarian).

Investigation of aggregation with fragments retransmission with losses in wireless networks

Valentin Hristov*, Firas Ibrahim, Bzar k. Hussan***, Kiril Slavkov******

**South-west University "Neofit Rilski"- Blagoevgrad, Bulgaria*
***University Of Tabuk- Tabuk, Kingdom Saudi Arabia,*
****Hawler Polytechnic College "Erbil Technical Institute"-Erbil, Iraq*
*****Technical University of Sofia, Bulgaria*

1. INTRODUCTION

Modern wireless computer networks offer more high-speed data transmission in the physical layer (PHY) and using highly efficient protocols in the Media Access Control layer (MAC) to access the communication medium.

High-speed wireless networks use the mechanisms for aggregating packets in order to improve efficiency of Media Access Control layer. Most studies of mechanisms for aggregating packets using models in which traffic has a Poisson or Bernoulli distribution. These models cannot capture the strong correlative nature of actual network traffic and the sequence of wrong packets (burst error).

The aim of this paper is to investigate an adaptive mechanism for aggregation with fragments retransmission as examine its performance, taking into account time-varying radio channel characteristics and their strong relation with errors.

2. MECHANISM FOR AGGREGATION WITH FRAGMENTS RETRANSMISSION

In the aggregation mechanism with fragment retransmission -AFR, multiple packets are aggregated into one large frame to be sent. Using technology of fragmentation, whereby if the packets are larger than a threshold, they are split into fragments that are re-transmitted in case of loss, rather than retransmitting of whole aggregated frames.

In order to AFR mechanism would improve delays in aggregation in the literature [2] is proposed aggregation to do with utilization above a certain threshold. In low intensity of arrival packets in the buffer, respectively utiliza-

tion ($\rho = \lambda/\mu$) below this threshold, aggregation is not done, and each new arrival packet formed frame.

The A-AFR mechanism and more precisely the transmitter assigns unique identifier (ID) to each fragment in the aggregated frame In the receiver side fragments of a packet are concatenated according to their IDs. After the transmission of aggregated frame, constituent fragments temporarily buffered while the acknowledgement frame (ACK frame) arrives back to the transmitter. This happens with some delay. In case that a positive acknowledgment (ACK) arrives for given fragment, this fragment will be removed from the retransmission buffer (waiting buffer). If the acknowledgement arrives negative (NACK) – the fragment will be transmitted again.

The arriving of fragments of packets in the buffer of transmitter is described by:

- Intensity of the arrival packets - λ.
- Average number of packets in one aggregated frame –p.
- Average number of 128B fragments in a packet - L.

The last parameter characterizes the process of fragmentation of packets, i.e. the average number of fragments aggregated in one frame is $A = p.L$.

New arrival packet is immediately transmitted [9] only when the buffer is empty as well as there is no request for retransmission of fragment/s of earlier transmitted packet. This is because retransmission of the fragments has a higher priority than fragmentation, aggregation and transmission of newly arrived packets.

The sent data from the transmitter reaches the receiver on radio channel in which there is interference which can lead to loss of fragments. In the proposed model this error prone channel is also modeled by ON-OFF generator (process with two states) and is described by parameters:

- Error probability of the channel also called channel error probability- ε;
- Average error burst length (length of the sequence of lost fragments due to the packet error)- B.

The receiver responds with a positive or negative acknowledgment (ACK / NACK) depending on whether the fragment was received without errors or with errors. After the round-trip-time, i.e. after m slots the transmitter gets feedback (ACK/ NACK) and then starts transmission of a new aggregated frame or retransmission of lost fragment/s (for which is arrived a negative acknowledgement - NACK). Corresponding flags - $bi\ (i = 1, 2, \ldots m)$ are used to model the result of transmission in mi slot, where $bi = 1$ - means that the transmission of i-th fragment is not successfully and its retransmission is necessary, otherwise i.e. $bi = 0$ and the transmission is successfully.

In the proposed model is assumed that no errors occur in transmission of acknowledgements (ACK / NACK), i.e. all acknowledgements arrive to the transmitter.

General Purpose Simulation System (GPSS) has been chosen to create simulator for evolution of the A-AFR mechanism. The proposed modeling approach reflects the requirements and limitations of the GPSS language environment and accurately describes the parameters and the processes in the wireless network.

3. SIMULATION RESULTS

The duration of simulations is 100 000 packets, each with an average length L= 3.2 fragments (according statistics [9] for traffic in the Internet) and transfer rate λ = 150 Mbps. The values of all delays are converted to microseconds.

The behavior of delays is examined versus the varying average number of fragments in aggregated frame (A), at different intensities of incoming packets (ρ =λ / μ = 0.4 and ρ = 0.6). The average errors burst length in this case is chosen to be B = 3 fragments. Figure 1 shows the delay in the queue Tq and the delivery delay Td for the given above parameters values. As one can see the delivery delay of packets-Td does not change significantly when ρ and A change. The delay in the queue (of the transmitter) is increased with increasing ρ, as it is expected. The graph also shows that the delay in the queue increases with increasing parameter A. This can be explained by the fact that packets fragments arrived explosively (burst) and accumulate in the queue, which increases the value of Tq.

The above means that this delay, and thus total delay can be large even at low intensity, but explosively generated fragments.

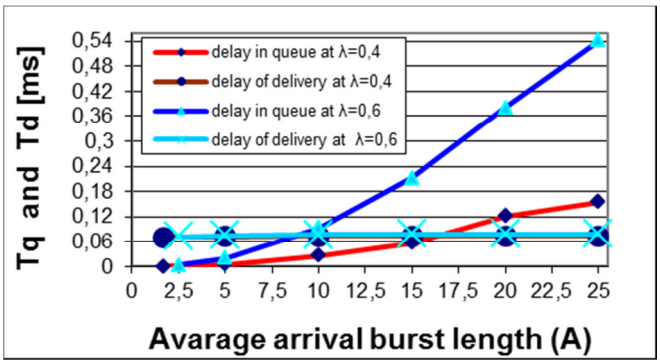


Fig. 1: Average delay in queue and delivery delay, for *m = 10*, *= 0.1*, *B = 3* as a function of *A*, with values of *ρ = 0.4* and *0.6*.

The results for the delays in the transmitter queue are compared with these calculated by well-known formula W =1/(μ-λ), and as expected the differences are not greater than 20%, which is a kind of verification of proposed model.

Fig.2 shows the delivery delay as a function of load -***ρ*** (respectively, the intensity of the packets arrival) at ***m = 10, = 0.1, A = 2.5***, and ***B = 3, 10, 60***. Can be expected that with increasing ***ρ***, the delay will be increased because the system becomes more and more loaded. This is correct for the queue delay, but it is not true for the delivery delay. In fact, when B is close in value to the number of slots for receiving feedback -***m***, i.e. channel is correlated; the delivery delay hardly depends on the intensity of packets arrival and may even decrease with increasing ***ρ***. This can be explained by the fact that when the channel is highly correlated it is possible to have a long series of slots, where the channel is in "good" condition. The above phenomenon is more pronounced for large values of error burst length B.

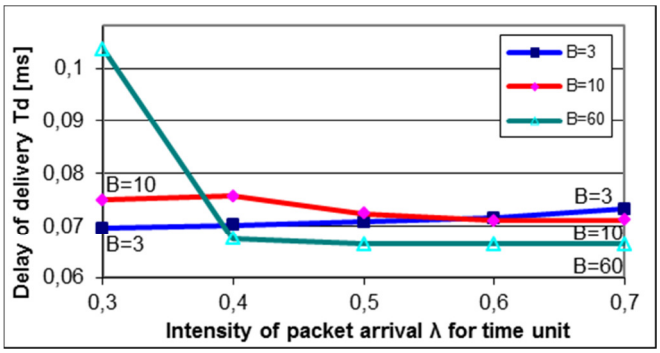


Fig. 2: Averages for delivery delay as a function of ρ, where *m = 10, = 0.1*, *A = 2.5*, at different values for *B*.

Fig.3 shows the total delay as a function of ***B***, where ***ρ = 0.6***, ***A = 7***, ***m = 10*** and ***m = 0.1***. As seen from the graphs the total delay initially decreases and then increases.

The reason for this is that from one side at small and medium error burst length, ***B***, the delay of retransmission dominated (see Td and Tq). From other side, by increasing B, the delay of retransmission reduces and hence also reduces the total delay. For large values of B, the delay in the queue has a strong character and the total delay increases (see Tq).

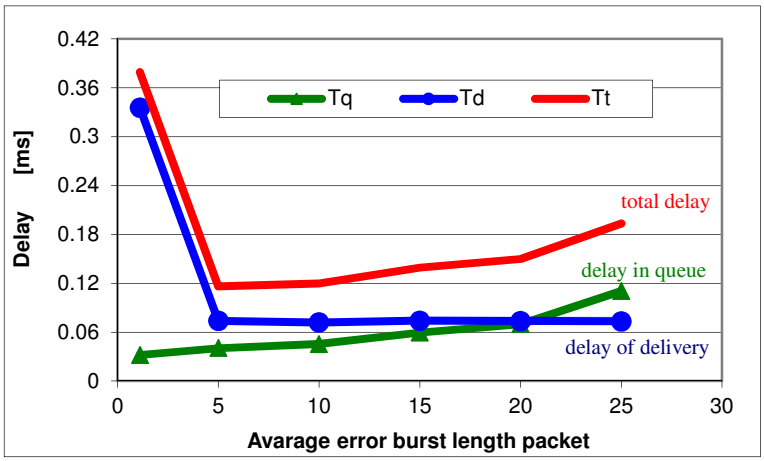


Fig.3: The total delay as a function of ***B***, at
ρ = 0.6, ***A = 7***, ***m = 10*** and ***m= 0.1***.

4. CONCLUSION

The performance of mechanism for aggregation with retransmission of fragments is examined through simulations which have been developed by GPSS model.

The presence of correlation between the time of feedback and the error burst length through transmission leads to non-trivial results, such as minimizing delays. This can be very important when designing [4] new communication applications for operating in wireless networks using the proposed adaptive mechanism for aggregation.

5. REFERENCES

[1] N. Ghazisaidi, M. Maier and C. Assi, “Fiber-Wireless (FiWi) Access Networks: A Survey”, IEEE Communications Magazine, February 2009, pp 160-167.

[2] J. Xie and X. Wang, “A Survey of Mobility Management in Hybrid Wireless Mesh Networks”, IEEE Network, November/December 2008, pp 34-44.

[3] J. Hong and K. Sohraby, “On Modeling, Analysis, and Optimization of Packet Aggregation Systems”, IEEE Transactions on Communications, vol. 58, no. 2, February 2010, pp 660-668.

[4] L. Taneva, “ Intelligent Module for Data Exchange using CAN Interface”, CEMA’09, 8-10 October 2009, Sofia, Proceedings p.102-104.

[5] R. Jain, C. So-In and A. Tamimi, “Level Modeling Of IEEE 802.16e Mobile Wimax Networks: Key Issues”, IEEE Wireless Communications, October 2008, pp 73-79
[6] V. Hristov, , B. Tudzharov, Adaptive mechanism with aggregation and fragment retransmission for highspeed wireless networks, Bulgarian Journal of Engineering Design, No 7, February 2011, pp. 15-22 (in Bulgarian).
[7] Taneva L., R. Bagalev, “Testing in electronics manufacturing”, FMNS’2011, 8-11 June 2011, Blagoevgrad, Proceedings Volume 1, p. 153-158.

Experimental Platform for measuring the parameters of magnetization of a transformer in a quasi-static transitional regime

Vasil Milovanski, Krasimir Stoyanov, Stefani Milovanska

South-West University "Neofit Rilski", Blagoevgrad, Bulgaria
HMS "Acad. S. P. Corolov", Blagoevgrad, Bulgaria
American University in Bulgaria, Blagoevgrad, Bulgaria

***Abstract**: Some opportunities for development of an experimental module for magnetic research have been examined in the current paper. The goal is to attain a more accurate reading of the measured electrical signals which are directly related to the magnetic parameters and characteristics of the ferromagnetic material.*

***Keywords:** transformer, magnetic, hysteresis cycles, harmonious components*

1. INTRODUCTION

Experiments for quasi-static re-magnetization can be conducted by the means of a computer simulation of transitional processes in measuring transformers. [1] The correct approaches for an accurate measurement of the results are looked for in this research paper. This includes some special construction features of the experimental block for measuring and processing the signals, describing the processes of transitional magnetization of the examined object.

2. ANALYSIS OF THE EXPERIMENTAL BLOCK AND OF SOME OF ITS ELEMENTS WHICH ARE USED FOR MEASURING AND PROCESSING OF THE GENERATED RESULTS

The tasks related to the study of ferromagnetic materials by the means of computer simulation of transitional magnetization in measuring transformers have been issues of several studies. [1,2]

An equivalent scheme of an experimental module is shown on *Figure 1*. The relationships given in (1) are based on some basic laws of electrical engineering. These relationships relate the electrical and the magnetic parameters of the measuring transformer.

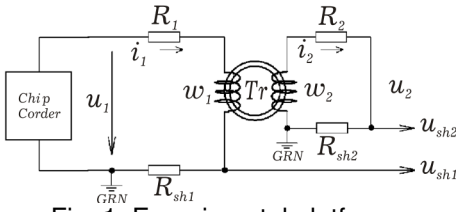


Fig. 1: Experimental platform.

$$(1)\begin{cases} u_1 = (R_1 + R_{SH1})i_1 + w_1 \dfrac{d\Phi}{dt} \\ u_2 = -(R_2 + R_{SH2})i_2 + w_2 \dfrac{d\Phi}{dt} \\ i_1 w_1 - i_2 w_2 = i_0 w_1 = l_{av.} H \end{cases}$$

By the means of these equalities, the relationships between $B(t)$ and $H(t)$ can be found, depending on the method of work of the transformer. There are current (CT) and voltage transformers (VT). The respective relationships are shown in (2) and (3).

$$(2)\begin{cases} u_2 \approx 0, \quad i_1(t) = \dfrac{u_{SH1}}{R_{SH1}}, \quad i_2(t) = \dfrac{u_{SH2}}{R_{SH2}} \\ B(t) = B_0 + \dfrac{(R_2 + R_{SH2})}{w_2 S} \int_0^t i_2(t)dt \\ H(t) = \dfrac{1}{l_{av.}}(i_1 w_1 - i_2 w_2) \end{cases} \qquad (3)\begin{cases} i_2 \approx 0, \quad i_1(t) = \dfrac{u_{SH1}}{R_{SH1}}, \quad u_2 = u_2(t) \\ B(t) = B_0 + \dfrac{1}{w_2 S} \int_0^t u_2(t)dt \\ H(t) = \dfrac{w_1}{l_{av.}} i_1(t) \end{cases}$$

Taking into consideration these relationships, it can be concluded that in both cases, the magnetic induction is computed by integrating mathematically either the current ($\int_0^t i_2(t)dt$) or the voltage ($\int_0^t u_2(t)dt$) in the secondary coil of the transformer. In practice, this means that the calculation error will be accumulated as a result of the calculation of these signals. The errors may be caused either by inappropriate measuring resistors or by "non-ideal" operational amplifiers used for amplifying the signals. They may also be caused by improper selection of analog-to-digital converters (ADC), bad topology of the board design, etc.

The current paper presents an analysis of the parts of the experimental block that one who wants to get accurate results should pay special attention to.

2.1. Choice of appropriate measuring resistors R_{sh1} and R_{sh2}

The choice of R_{sh1} and R_{sh2} is crucial. In order to repeatedly get the same results from the measurement, it is necessary to decrease significantly the influence of the temperature on the value of the resistance. This can be achieved by the means of precise resistors, designed particularly for this purpose. Their parameters are very precise. These resistors are made of alloys, the resistance of which depends on the

temperature very little. An example of such an alloy is *Manganin*, which is a trademarked name for an alloy of typically 86% copper, 12% manganese, and 2% nickel. The value of the measuring resistors should be low for two reasons: heat reduction, and insurance of a large dynamic range. However, it is necessary to consider the fact that the tiny value of R_{sh} may contribute to the measurement of a low voltage with a value close to that of the induced voices.

Precise resistors R_{sh1} and R_{sh2} have been used in the conducted research. Their average point and total resistance is $R_{sh1ab} = R_{sh2ab} = 2 * 350,\mu\Omega$, and their own parasitic inductivity is $L_{sh1} = L_{sh2} = 2 * 2,nH$. The constructive and the equivalent schemes are shown in *Figure 2*.

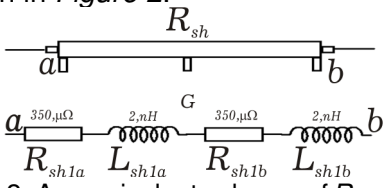


Fig. 2: An equivalent scheme of R_{sh}.

Knowing i_1 and i_2, the nominal value of the dispersed power may be found. The maximal current in the particular case discussed is 10, *A*. Therefore, the dispersed power is the following:

$$P_{sh1} = P_{sh2} = 10 * 700 * 10^{-6} = 70,mW$$

To avoid a phase shift between the inputs of the operational amplifiers, it is necessary to study the influence of the parasitic inductivity on the impedance of the resistor. When the operating frequency is maximal with a value of $f = 20,Hz$, the impedance is the following: $Z_{sh} = 350,\mu\Omega + j0.5,\mu\Omega$. Taking into consideration the generated result, it can be concluded that in the worst case, the measuring resistor has a negligible reactive component, i.e. it has an active character.

2.2. Choice of operational amplifiers

The selection of appropriate operational amplifiers starts from the consideration of what signals will be amplified, where the corresponding inputs will be included, and how the coordination between inputs and outputs will be executed. In addition, it is necessary to choose such amplifiers that are not very noisy, have small asymmetries and a high coefficient of reduction of the synphase signals *CMRR*, etc.

Figure 1 represents the different way in which the measuring resistors are connected in the scheme. In contrast to R_{sh2}, R_{sh1} is connected in series and in a galvanic way with the primary coil of the transformer and the generator of magnetization. *Figure 3* represents an experimental platform, and the way the resistors and the operational amplifiers are connected.

High-quality operational amplifiers produced by *Analog Devices* – AD8138 are used. [4].They have low levels of private noise, wide frequency band and differential input and output devices.

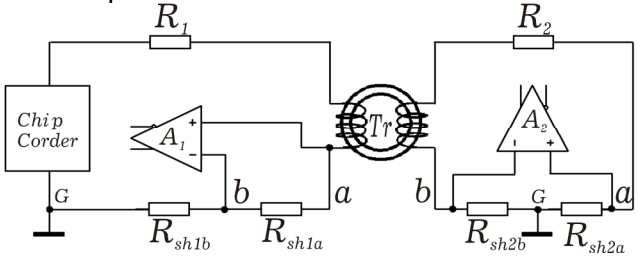


Fig. 3: Experimental block with included operational amplifiers.

The inputs of the amplifier A_1 are included in points ***a*** and ***b***, which is one half of R_{sh1}. Point ***G*** is at the other end of the resistor. It is connected to the common conductor. Thus one of the two halves R_{sh1a} is used for measuring the current i_1, while the other half is used for lifting up the source of the signal from the ground. The goal of the latter is to reduce the noise voltage towards the input of the amplifier. [3]

The size of the maximal input signal depends on the value of the current $I_1 = 10,A$, which creates a voltage drop on R_{sh1a} determined by the following equality: $U_{1ab} = R_{sh1a} * I_1 = 3.5,mV$. The scope of this voltage is $u_{1pp} = 2\sqrt{2} * U_{1ab1} \approx 9.9,mV$. The choice of a high-quality operational amplifier with a differential input device allows the typical synphase voltage for the scheme to be reduced, and the asymmetric input to become symmetric at the output.

The middle point ***G*** of R_{sh2} has to be connected to the ground on the output side of the transformer. Thus the synphase signals at point ***G*** from the two inputs of the amplifier turn out to be in a counter-phase and cancel each other out. The only condition is the following: $R_{sh2a} = R_{sh2b}$.The differential signal is the only thing that is amplified in this way.

2.3. Coordination of the operational amplifier output with ADC's input

The differential output of AD8138 allows itself to be connected to the differential input of the analog-to-digital converter (ADC) of the type AD7400. This is an ADC with $\Sigma\Delta$modulator, operating at a relatively high sample rate - $900,kHz$. The usage of an analog amplifier between R_{sh} and ADC allows an execution of a bufferization and an easy change of the synphase level.

The principle of analog signal sampling is the reason why noise occurs. It is necessary to find a way to reduce this noise. First, this should be done

by reducing the over-sampling. It is characterized by an expansion of the sampling frequency range, which is many times higher than the frequency range of the signal. As a result of the operation of the $\Sigma\Delta$modulator, the spectrum of the noise sample partly flattens by the process of integration in the scheme itself. However, a large part of the noise belongs to the high-frequency region and can be eliminated by the means of a low-frequency filter of high order.

Another component of the noise sample is obtained by the means of superimposing of the spectrum of the signal – *aliasing*. *Figure 4* shows that the harmonic components of the input signal, which exceed half of the sampling frequency ($450_{+\Delta}, kHz$), have a mirror image in the operational low-frequency spectrum. When the chosen sampling frequency is high, the harmonic components may be filtrated by the means of a simple *RC* filter.

The usage of filters at the inputs of the two ADC converters leads to a phase shift of the signals, which may change the real general image of the study.

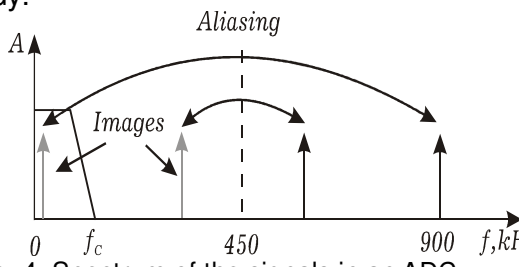


Fig. 4: Spectrum of the signals in an ADC.

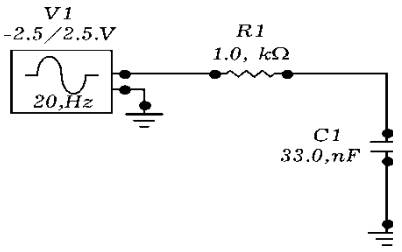


Fig. 5a: A scheme of a *RC LPF*.

A low-frequency filter (*Figure* 5*a*) with elements $R = 1.0, k\Omega$ and $C = 33, nF$ is used. It has been examined by a computer simulation program in the frequency range from $f_1 = 10, Hz$ to $f_2 = 1.0, MHz$. The amplitude – frequency (*Figure* 5*b*) and the phase – frequency (*Figure* 5*c*) characteristics of a *LPF* are graphically shown.

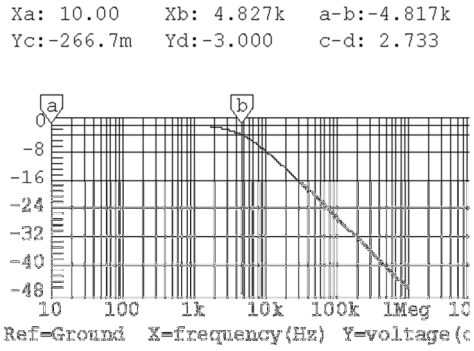


Fig. 5b: *RC LPF - АЧХ*.

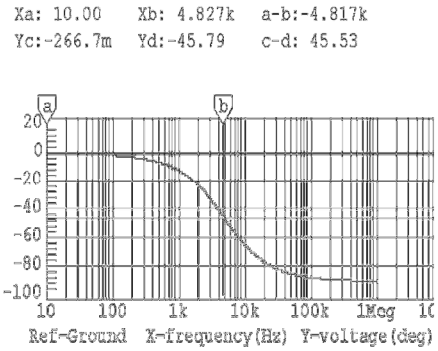


Fig. 5c: *RC LPF - ФЧХ*.

$$(4)\begin{cases} A = 20\,lg\left(\sqrt{\dfrac{1}{1+2\pi fRC}}\right) \\ \varphi = -arctg(2\pi fRC) \end{cases}$$

In the worst case, $f = 20,Hz$,
the attenuation is $A = \text{-}74.7,\mu dB \approx 0,dB$,
and
the phase shift is $\varphi = -0.24,deg$.

By the means of the graphs and the equalities in (4), the attenuation and the phase shift can be determined. Both the attenuation and the phase shift emerge when the filter is placed at the output of the operational amplifier.

When accurate resistors $\delta_R = 0.1,\%$ and capacitors $\delta_C = 20,\%$ are used, the maximal value of the phase shift does not increase by more than $\Delta\varphi \le 19,\%$.

3. CONCLUSION

3.1. When transient processes in the magnetic core of the measuring transformer are simulated, low levels of magnetization are used. This allows several parasitical, reactive components to be ignored and the experimental model to be simplified.

3.2. Precise measuring resistors are used. They have low resistance and are made of an alloy, which does not depend on temperature too much.

3.3. The presence of galvanic connections between the measuring resistor and the preceding device requires precise (and expensive) operational amplifiers. These amplifiers emit less noise. They also have wide bands, small asymmetries, high coefficient of repressing synphase signals *CMRR*, and differential input and output.

3.4. It is necessary to put an *antialiasing* filter in order to reduce the noise emitted during the sampling. This filter is a simple *RC LPF* thanks to the high sampling rate.

4. REFERENCES

[1] Milovanski V. St., Interface Converter for Computer Simulation of Transient Processes in Current Transformers. Jubilee Scientific Session'97 – Technical University, Varna, Bulgaria, 16 – 18 October 1997

[2] Milovanski V. St., E. V. Radev – Reducing the Induction of ScatteringInside the Measuring Current Transformers During the Simulational Process of Transitional Magnetization by the use of Chip Corder ISD1400. Fourth International Scientific Conference South-

West University, Faculty of Mathematics & Natural Sciences Blagoevgrad, Bulgaria, 8 - 11 June, 2011
[3] Ott H. W., Noise reduction techniques in electronic systems. John Wiley & Sons, Inc., 1976.
[4] http://www.analog.com
[5] http://www.winbond.com

Improving network management with Software Defined Networking

Pavel Dzhunev

South- West University- Blagoevgrad, Bulgaria

***Abstract**: Software-defined networking (SDN) is developed as an alternative to closed networks in centers for data processing by providing a means to separate the control layer data layer switches, and routers. SDN introduces new possibilities for network management and configuration methods. In this article, we identify problems with the current state-of-the-art network configuration and management mechanisms and introduce mechanisms to improve various aspects of network management.*

***Keywords:** SDN, OpenFlow, Net Flow, Control layer, SDN Controller*

1. INTRODUCTION

The article considers a model of a new control system that is more efficient and improving reliability, speed and flexibility than this - network built entirely in hardware. The system is called SDN or translation software defined network. SDN efficiently automate the network configuration and allows easy and flexible operation, without the need for configuration and writing of specific scripts, as in conventional devices for routing. In this type of network architecture, the physical topology is separated from the network control software which allows government level. There are different models of governance - the report examined the model with NetFlow protocol and OpenFlow.

2. ARCHITECTURE OF SOFTWARE-DEFINED NETWORKING

The elements of the Software Defined Networking (SDN) architecture are shown in Figure 1. The Data Plane comprises switches connected together to form a network [1]. However, instead of relying on proprietary software running on each switch to control its forwarding behavior, switches in SDN architecture are controlled by a Network OS (NOS) that interacts with the switches to provide an abstract model of the network topology to Applications running on the Network Operation System. Applications can adapt the network behavior to suite specialized requirements, for example, providing network virtualization services that allow multiple logical networks

to share a single physical network - similar to the way in which a hypervisor allows multiple virtual machines to share a single physical machine.[2]

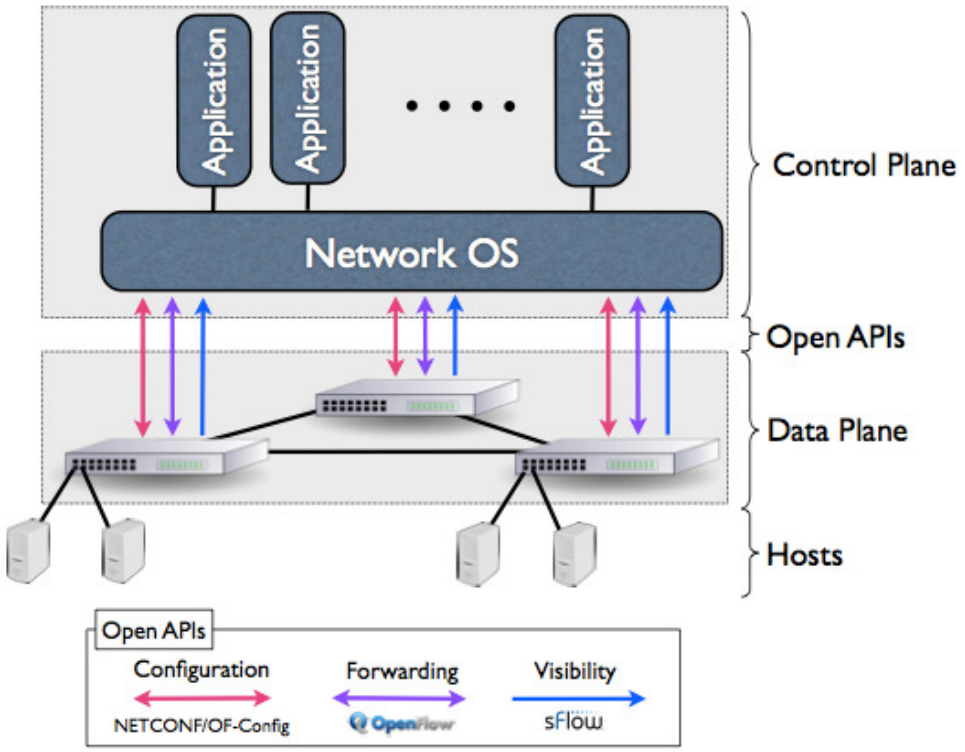


Fig. 1: Software Defined Networking architecture.

Open APIs for programatic access to the switches is an essential pre-requisite to building a software defined network:

- **Forwarding**. The OpenFlow protocol was originally developed so that academic researchers could experiment with external control of switch packet forwarding.

- **Configuration.** It was quickly realized that OpenFlow alone isn't sufficient - a configuration protocol is needed to assign switches to controllers, configure port settings and provision queues.

- **Visibility.** Current efforts in the SDN community are focused on provisioning of network services.

- **NetFlow** is a network protocol developed by Cisco Systems for collecting IP traffic information. NetFlow has become an industry standard for traffic monitoring[citation needed] and is supported on various platforms, see NetFlow support below.

sFlow is a technology for monitoring network, wireless and host devices. With sFlow monitoring, the decode, hash, flow cache and flush functionality are no longer implemented on the switch.

The controller is the core of an SDN network. An SDN controller is an application in software-defined networking (SDN) that manages flow control to enable intelligent networking. SDN controllers are based on protocols, such as OpenFlow, that allow servers to tell switches where to send packets.

It lies between network devices at one end and applications at the other end. Any communications between applications and devices have to go through the controller.

The controller also uses protocols such as OpenFlow to configure network devices and choose the optimal network path for application traffic.

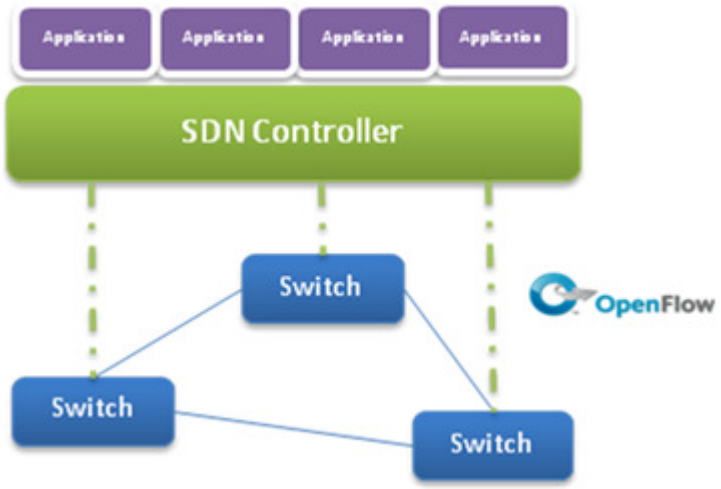


Fig. 2: SDN Controller.

3. PERFORMANCE ANALYSIS OF SDN SCHEME

The number of OpenFlow clients (which generate requests) is N. Note that SDN controller can be multiprocessor system with M processors and each processor can start L threads [3-5], i.e. K=M.L. If N>K, the model segments which correspond to processing of OpenFlow requests would be realized with only K facilities, e. g. duplicating model segments- 1,2,…k the necessary times.

The modeling process aims at getting the response delay for OpenFlow requests. The delay includes two components- search time and transmission delay (latency due transport over communication channel). The search time, or processing time due to bind (open the connection) and search in directory actually increases slightly at heaviest load [4]. The time slot in this model is time that one thread processes one byte of the OpenFlow request.

N - model segments which correspond to server processing of OpenFlow requests (in manner one thread one request) and one model segment which corresponds to the transmission (over communication channel) of OpenFlow as well as non - OpenFlow messages.

The entry size for these simulations is random and realistic values in each data item, and the default directory size is 10 000 entries. We make the assumption that these entry sizes are geometrically distributed with mean value 1/(1-α)=490 bytes. The probability that the OpenFlow clients start a new request is denoted by β, therefore the probability that a client starts a new request is β/N. We assume β =0.008 and N=10.

The bandwidth of the communication channel is considered fixed, but only a fraction σ of it is available for the transmission of OpenFlow messages. The ratio between the transfer rate from SDN controler and the communication channel bandwidth is denoted by p. We assume p={1, 2, 3, 4, 5} and 10 Mbps channel.

The formula of system load is:

$$\rho = \frac{\beta . p}{\sigma(1-\alpha)} \quad (1)$$

The load at the communication channel for non- OpenFlow message is generated by source (fig.6) with mean rate-γ, i.e:

$$\gamma = \left(\frac{1-\sigma}{\sigma}\right)\cdot\left(\frac{\beta}{1-\alpha}\right) \quad (2)$$

Fig. 3 represents shows the OpenFlow response delay, or latency versus load generated by OpenFlow messages, as well as trendline for delay versus OpenFlow and non- OpenFlow load. Note, that the dimension of Y-axe is ms. As one can see the OpenFlow response delay increases with the system load, which is logical.

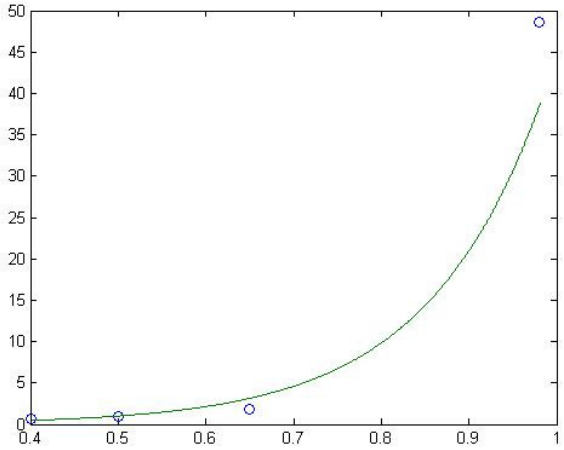


Fig. 3: Simulation Results.

4. CONCLUSION

In order to decrease OpenFlow response delay, or improve performance, the dual processor server could be deployed. The dual processor server shows similar performance at low loads, and the advantage increases to give roughly 35 - 40% smaller latency at higher loads for the total response time. The reduction in latency is observed mainly due to the reduction in the so-called connect time.

The technologies we describe enable network operators to implement a wide range of network policies in a high-level policy language and easily determine sources of performance problems.

5. REFERENCES

[1] Hyojoon Kim and Feamster, N., February 2013 *improving network management with software defined networking*. Communications Magazine, IEEE, Volume: 51, Issue: 2, Page(s): 114 - 119

[2] Myung-Ki Shin 15-17 Oct. 2012 *Software-defined networking (SDN): A reference architecture and open APIss*, ICT Convergence (ICTC), Page(s): 360 – 361

[3] Hristov, V. Oct. 2009, *Using Lightweight Directory Access Protocol for Service Level Specifications Administration*, Proc. of the International Conference CEMA'2009, Sofia, Bulgaria, pp.19 -23.

[4] Hristov, V. Sept. 2010 Session Initiation Protocol Interworking with Traditional Telephony and Signaling Delay Introduced by Internet, Proceedings of the International Conference on Information Technologies InfoTech-2010, September 16-17, 2010, Varna, Bulgaria, pp. 167- 172

[5] Hristov, V. Oct. 2010 Simulation of Selective Repeat Automatic Retransmission Request Scheme, 5th International Conference on Communications, Electromagnetics and Medical Applications (CEMA'2010) Athens , Greece, October 7th-9th, 2010, pp.49-53

[6] Snejana Pleshkova. FPGA & DSP Infrared image processing module for people and objects detection. 15th WSEAS INTERNATIONAL CONFERENCE in SYSTEMS, Corfu Island, Greece, 2011, pp.253-258

[7] Snejana Pleshkova. Spiking Neural Networks for Real-Time Infrared Images Processing in Thermo Vision Systems. 16th WSEAS International Conference on SYSTEMS (part of the 16th CSCC / CSCC 2012), Kos Island, Greece, pp.182-187

[8] Alexander Bekiarski, Snejana Pleshkova, Svetlin Antonov, "Real Time Processing and Database of Medical Thermal Images", 4rd INTERNATIONAL CONFERENCE on Communications, Electromagnetics and Medical Application (CEMA'11), Sofia, 2011, pp.101-106

Microprocessor System for Non-Invasive Measurement of Blood Glucose

Ljudmila Taneva[*], Antoaneta Daskalova[**]

[*] *South-West University "Neofit Rilski", Bulgaria,*

[**] *Technical University-Sofia, Sofia, Bulgaria*

***Abstract**: In this paper is presented a microprocessor system for monitoring blood glucose levels using new noninvasive method. The MHC method consists in measuring physiological indexes related to metabolic heat generation and local oxygen supply, which corresponds to the level of blood glucose in the bloodstream. Shown is a sample schematic of the device obtained after studies of different methods and selection of appropriate electronic components required for the development of the proposed device. There have been a number of measurements with various individual instruments that show the relationship between the measured parameters and trends in the change in blood sugar, which makes the proposed date noninvasive system.*

***Keywords:** blood glucose, noninvasive, metabolic heat conformation, measurements, microprocessor system.*

1. INTRODUCTION

The paper presents the structure of the microprocessor system for the non-invasive measurement of blood glucose, using the metabolic heat conformation (MHC) method. MHC method consists in measuring physiological indexes related to metabolic heat generation and local oxygen supply, which corresponds to the level of blood glucose in the bloodstream. The proposed device measures the peripheral temperature, galvanic skin-resistance, heart rate, saturation and perfusion of the skin and determines the level of blood sugar in the human body. Tests were conducted and the obtained results demonstrates the reliability of the results.

2. TYPES OF DIABETES AND PHYSIOLOGICAL PARAMETERS

Diabetes is a disease which affects the lives of at least 366 million people worldwide. The diabetics should monitor glucose levels in the blood and check it daily. This is done by invasive glucose testers that are uncomfortable and hurt of the respondents. With development and distribution of

equipment for monitoring blood sugar levels in a noninvasive way, it would make it easier and more comfortable for everyone affected by this disease.

New technologies allow the construction of smaller devices. Development of a tool for monitoring blood sugar levels in the form of a watch or bracelet would make the daily monitoring of diabetics very easy and painless. Data can be transmitted by wireless technology to the mobile phone or PC where the respondent can monitor levels changes and dose the insulin dosed correctly.

2.1. Type1 diabetes

Type 1 diabetes is an autoimmune disease of unknown origin. The body produces antibodies against the beta cells of the pancreas and as a result, islands of Langerhans are destructed. It is responsible for the production of the peptide hormone insulin and glucagon. When the amount of the hormone insulin decreases, the blood sugar levels remains very high and the cells "suffer", because at the same time they are 'hungry', have no energy, and is impaired the carbohydrate homeostasis. If the body does not receive 'external' insulin, it will develop diabetic acidosis – state with very high level of ketones. People with ketoacidosis are intoxicated and the symptoms are “acetone” breath, tachycardia and increased diuresis.

2.2. Type2 diabetes

Type 2 diabetes is characterized by "closing" of the cell membrane of the skeletal muscle, the liver and the adipose tissue, because the membrane receptors become resistant to glucose. Cells "starve" because there is no glycolysis and this slows the Krebs cycle in the mitochondria, where is synthesized adenosine triphosphate stored in the cells. This is the reason diabetics may be fatigue, weak, sometimes with accelerated heartbeat.

2.3. Gestational diabetes

During the pregnancy 7% of women develop this type of diabetes and 40% of them are liable to develop type 2 diabetes. Children of mothers whit gestational diabetes are usually with higher birth weight. It is very important to be detected early – maximum to 4 months in the pregnancy, because the high blood sugar could impair the fetus.

2.4. Physiological parameters in the three types of diabetes

- Weight loss - no glycogen accumulation in the skeletal muscles;

- Constant fatigue, because the Krebs cycle, where the adenosine triphosphate is synthesized (only in the presence of oxygen / aerobic /), does not close;
- Tachycardia - sympathetic nervous system sends signals accelerating the heartbeat and this way affect the entire metabolism;
- Sweating for thermoregulation
- Glycosylated hemoglobin-HbA1C – this is hemoglobin that is related to the erythrocytes and gives an accurate picture of the blood sugar for the last 3 months;
- Triglycerides: "good" cholesterol - HDL; "bad" cholesterol - LDL

All these data can be obtained only through blood tests.

Noninvasive methods are friendly and based on biophysical parameters such as pulse, blood density and the heat exchange as a way the body to maintain the homeostasis.

3. EXISTING METHODS FOR BLOOD GLUCOSE MEASUREMENT

The diabetics need to monitor the glucose levels in their blood in order to know how the treatment goes and how much insulin the body needs. For measurement of the blood glucose are used meters and depending of the method of measurement there are two main types: invasive and non-invasive blood glucose meters. Invasive method consists in the measurement of the blood glucose in the blood by glucose meter. Non-invasive methods don't need a drop of blood and are based on measurements without piercing the skin or causing pain. They are:

- Near Infrared Spectroscopy
- Ultrasound technology
- Dielectric Spectroscopy
- Metabolic heat conformation (MHC)

MHC method is based on the amount of heat dissipated (peripheral temperature), the blood flow (perfusion) and the degree of oxygenation of the blood [1].

4. IMPROVED MHC METHOD

Here is proposed MHC method that extends the measured parameters and provides correlation between them, which approximately determines the level of glucose in the blood. The method consists of measuring the physiological parameters of the human body, and uses an improved method to calculate the parameter "perfusion". Used are noninvasive thermal and optical sensors to measure the peripheral temperature, the velocity of the blood

flow, the concentration of hemoglobin and oxyhemoglobin concentration.

Mathematical transformations are used to determine the level of glucose in the blood. Mathematical procedures are multivariant statistical analysis, including values of sensor signals, polynomials from different values of the individual patient regression and cluster analyzes of patient groups. The glucose is calculated individually for each patient, applying a cluster and using discriminate analysis.

The oxidation of glucose is associated with the generation of energy that can be released into the environment as heat, so the amount of heat dissipation is related to the levels of glucose and oxygen [2]. Since the amount of oxygen supplied is a function of the level of oxygen in the blood and the rate of blood flow in capillaries, the amount will be dissipated heat (1):

$$H = f(G, BF, O), \quad (1)$$

where: H – Dissipated heat, G – glucose level, BF – blood stream velocity, O - degree of oxygen saturation in the blood.

It is proposed to use the measurement of heat dissipation by evaporation on the principle of action of skin-galvanic reaction (SGR), also known as BSR (basal skin response), measuring the activity of sweat glands and electrolyte balance of the body fluids. In a state of stress, the sweat glands increase the secretion of salt solution, resulting in a change in electrical resistance of the skin.

For measuring the perfusion, the level of oxygen saturation and the pulse is used pulseoxymeter. The measurement method is based on passing a light with two different wavelengths, such as 650 nm - red and 800 nm – infrared, through patient finger, ear, etc., and measuring the absorption.

5. HARDWARE REALIZATION AND RESULTS

The developed system is built on 16-bit RISC microcontroller (MCU) MSP430F149. Generalized block diagram of the device to monitor glucose levels in the blood is given in fig. 1.

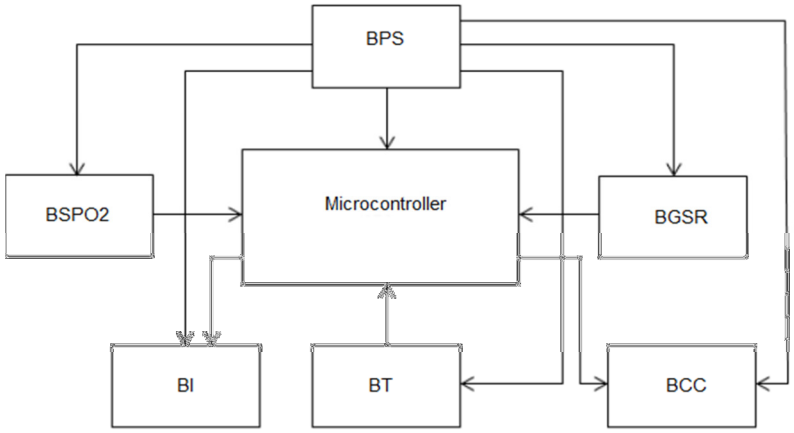


Fig. 1: Glucose meter block diagram.

The unit is controlled by a microcontroller, to which the data measured data is provided by the next blocks: Block-Galvanic Skin Response (BGSR), Block Temperature (BT), Block Saturation, Perfusion and Oxygen (BSPO2). Block Indication (BI) displays the measurements results on a display. Block for Communication with the Computer (BCC) provides connection of the device with a personal computer for data transfer.

Tab.1: Comparative data on physiological parameters.

Date	Age	Diabet or not	Saturation	Perfusion	Pulse	Peripheral Tempera-ture	Blood sugar
22.05	22	no	96	0.9	79	30	5.4
22.05	49	no	97	1,9	69	30	5.1
22.05	51	no	95	5,7	77	30	4.8
1.06	24	no	98	28	57	30,3	4,9
2.06	25	no	98	17	81	31,3	5,1
15.06	42	no	99	7,5	65	30,3	5
22.05	24 - f	Type 1	98	1,1	88	30	8
23.05	24 - f	Type 1	96	0,5	88	31	10
23.05	24 - f	Type1	98	0.2	84	32	5.8
24.05	24 - f	Type 1	98	0.9	90	31,3	14,9
25.05	24 - f	Type 1	95	0,2	80	30	7,4
30.05	24 - f	Type 1	99	1,2	76	31,3	6
30.05	24 - f	Type 1	99	2,3	89	31,3	7.3
1.06	24 - f	Type 1	98	1,4	60	29,2	10,9
1.06	24 - f	Type 1	98	0,8	72	29,4	11,8
1.06	24 - f	Type 1	98	2,8	103	33,5	2,8

2.06	24 - f	Type 1	98	0,7	55	29,2	7,1
4.06	24 - f	Type 1	99	2,9	93	30,2	4,3
5.06	24 - f	Type 1	98	1,9	88	32,1	8,6
22.06	60-m	Type 1	97	1,3	65	33,3	20,5
23.06	60-m	Type 1	96	1,8	70	33,1	~21
24.06	60-m	Type 1	97	1,5	72	33,4	22
25.06	60-m	Type 1	96	1,9	78	33,5	~21
26.06	60-m	Type 1	96	1,4	64	33,4	21
27.06	60-m	Type 1	95	1,7	70	33,3	~21
28.06	60-m	Type 1	93	1,4	72	34	20
23.05	76	Type 2	98	3.1	75	30	7
14.06	66 m	Type 2	73	8,6	85	34	~9
17.06	66 m	Type 2	99	6,5	79	33	~9
13.06	62 -f	Type 2	96	4,1	67	31	-
14.06	62 -f	Type 2	97	5,9	79	32	-
15.06	62 -f	Type 2	94	2,6	74	28	-

The goal, achieved with the development of the device, is to assess the trend of increase or decrease of the blood sugar. The measurements are made with pulsoksimeter; thermometer for peripheral temperature, based on the same sensor and meter MLX90614DAA and glucose meter Optium Xceed. Using the proposed MHC method we measured blood glucose concentrations in 20 patients, 2 with diabetes type1 (1 female and 1 male), 2 with diabetes type2 (1 female and 1 male) and 15 without diabetes (7 male and 8 female), comparing results obtained with the MHC device with measurements obtained with Optium Xceed [3], [4]. The ages of the patients ranged from 22 to 76 years. Invasive and noninvasive measurements were temporally obtained as close to each other as possible. The mean glucose concentrations were 12,1 mmol/L for the patients with diabetes type1, 7,7 mmol/L for the patients with diabetes type 2 and 5.1 mmol/L for the patients without diabetet. The data is shown in tab.1.

6. CONCLUSION

In this paper is presented a microprocessor system for monitoring glucose levels in the blood MHC improved noninvasive method. There have been a number of measurements with various individual instruments that show the relationship between the measured parameters and trends in the change in blood sugar, which makes the proposed date non-invasive system.

Based on the suggested method is developed portable pulsoksimetar for measurement of the degree of saturation of blood oxygen, pulse rate and perfusion rate of blood flow in peripheral tissues. Tests were conducted and

data were obtained demonstrated the reliability of measurement of the instrument.

7. REFERENCES

[1] Fei Tang, Xiaohao Wang, Dongsheng Wang, Junfeng Li, (2008) Non-Invasive Glucose Measurement by Use of Metabolic Heat Conformation Method. Sensors, 8(5), 3335-3344.

[2] Ok Kyung Cho, Yoon Ok Kim, Hiroshi Mitsumaki, (2004) Noninvasive Measurement of Glucose by Metabolic Heat Conformation Method, Clinical Chemistry 50, No.10,1894-1898

[3] Hristov, V., Petrov, I. (2008) Investigation of 802.11N WLAN Throughput, 3rd International Conference on Communications. Athens, Greece: Electromagnetics and Medical Applications (CEMA'08), 64-69.

[4] Hristov, V., (2009) Signaling Delay in Wireless Networks with Session Initiation Protocol over User Datagram Protocol, Blagoevgrad, Bulgaria: Proc. of the Conference FMNS'09 (1), 78-85.

Speed testing of Sliding spectrum analysis

Emil Frenski, Member, IEEE
Dimitar Manolev
South-West University "Neofit Rilski", Blagoevgrad, Bulgaria

***Abstract**: The standard method for spectrum analysis in DSP is the Discrete Fourier transform (DFT), typically implemented using a Fast Fourier transform (FFT) algorithm. The reconstruction of the time-domain signal is then performed by the IFFT (Inverse Fast Fourier transform) algorithm. The FFT calculates the spectral components in a window, on a block-by-block basis. If that window is move by one sample, it is obvious that most of the information will remain the same. This article shows how to measure execution time of scripts realizing SDFT algorithm written for MatLab.*

***Keywords:** Sliding Discrete Fourier transform (SDFT), Fast Fourier transform (FFT), MatLab.*

1. INTRODUCTION

The discrete Fourier transform (DFT) plays very important role in the implementation of discrete-time signal-processing. The DFT is identical to samples of the Fourier transform. Computation of the *N*-point DFT corresponds to the computation of the Fourier transform at *N* equally spaced frequencies $\omega_k = 2\pi k / N$ (bins[1]), i.e. at *N* points on the unit circle in the z-plane. The DFT of finite – length sequence is (1)

$$S^k = \sum_{n=0}^{N-1} x[n] W_N^{kn}, \tag{1}$$

where S^k represent the k-th frequency point (bin), $x[n]$ is sampled input data of size *N* and $W_N = e^{-j2\pi/N}$.

Since in (1), both $x[n]$ and S^k may be complex, *N* complex multiplication and (*N*-1) complex addition are required. Computational complexity of

[1] Frequency bins k corresponds to the band of frequencies centred at $\omega_k = 2\pi k / N$ with a bandwidth of approximately $2\pi / N$

each successive *N*-point output is approximate $O(N^2)$ where *O*(·) denotes order of. It is evident that the number of arithmetic operations required computing DFT becomes very large for large values of *N*.

Set of algorithms known as the fast Fourier transform (FFT) is used for reducing the computational complexity to $O(N \log_2 N)$.

The FFT is "fast" when all the *N* values of S^k are needed and the number of samples N is a power of two. But if we are only interested in the k-th value of the DFT, we have to compute the entire DFT - sequence and discard the unwanted values.

On the other hand, in the case of DFT, it has been noted that the algorithm can be implemented with $O(N)$ complexity, for any (non power of two) value of *N*. This can be achieved by using a set of parallel recursive digital filters [1] - this is called sliding DFT (SDFT). In the current literature, the term running DFT has also been used for this purpose.

2. SLIDING DISCRETE FOURIER TRANSFORM

The sliding DFT (SDFT) use the circular shift property. We use this shift principle to express sliding DFT process as [2][3][4]

$$S_{[n]}^k = \left[S_{[n-1]}^k - x[n-M] + x[n] \right] W_M^k, \tag{2}$$

where $S_{[n]}^k$ is the new spectral component at the time index [n] and $S_{[n-1]}^k$ is the previous spectral component at the time index [n-1]. The superscript *k* is associated with the *k*-th DFT bin. There is no requirement for the window size to be a power of two and we use *M* for sample data points, instead of the usual convention *N*. The difference between the current sample $x[n]$ and the last sample $x[n-M]$ can be computed once for each $S_{[n]}^k$.

The sliding algorithm (2) performs an M=16 point DFT on time samples is depicted in Fig. 1.

First the SDFT computes the DFT at the time index [n-1], second at the time index [n]. For this we forget the oldest sample $x[n-M-1]$ and accept new sample $x[n]$.

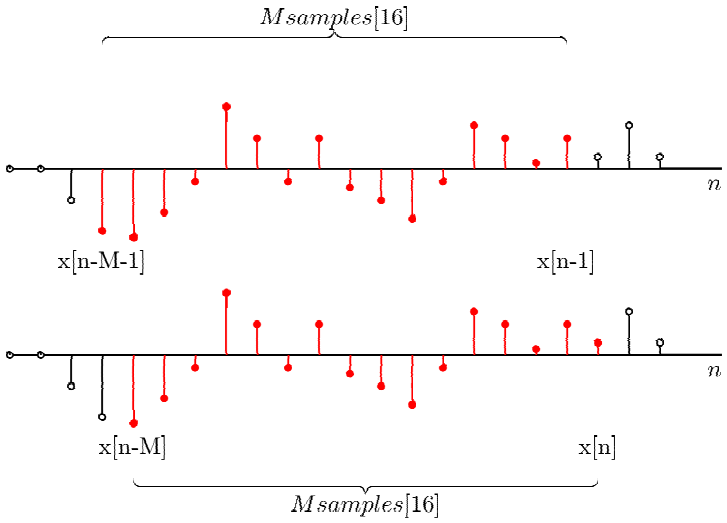


Fig. 1: Data samples at the time index [n] and [n-1].

The z transform which corresponds to a (2) is

$$S_{[n]}^{k} = \left[S_{[n]}^{k} z^{-1} - x[n] z^{-M} + x[n] \right] W_M^k . \tag{3}$$

And transfer function is

$$H(z) = \frac{\left(1 - z^{-M}\right) W_M^k}{1 - z^{-1} W_M^k} . \tag{4}$$

The transfer function (4) has *M* zeros located at the *M* root of 1 and single pole located at $z_1 = e^{(j2\pi/M)k}$. We see that the single pole cancelled the k-th zero (i.e.) transfer function having (M-1) zeros and no poles. As example, Fig 2. shows the zero – pole plot and frequency response for the *M*=16 and *k*=2

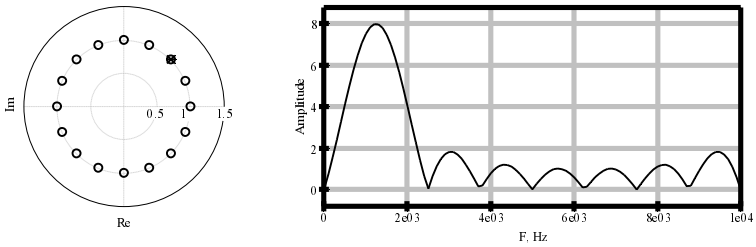


Fig. 2: Zero-pole plot and frequency response for the *M*=16 and *k*=2.

Equation (4) leads for filter structure shown in Fig. 3. The single - bin SDFT algorithm is implemented as an IIR filter with a comb filter followed by a complex resonator [2].

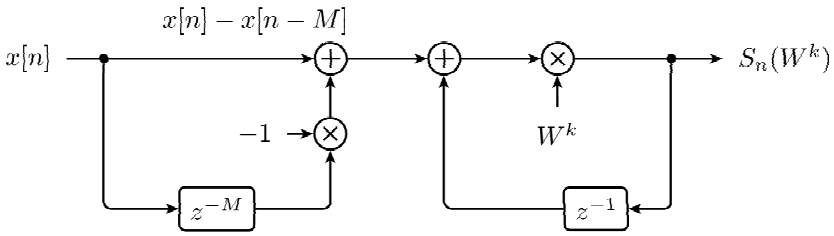


Fig. 3: The single - bin SDFT filter.

The frequency response of comb filter, complex resonator and single-bin SDFT filter is depicted in Fig. 4.

If we want to compute all M DFT spectral components, M resonators will be needed, all driven by a single comb filter. The comb filter delay of M samples forces the filter's transient response to be M–1 samples in length, so the output will not reach steady state until the Sk(n) sample.

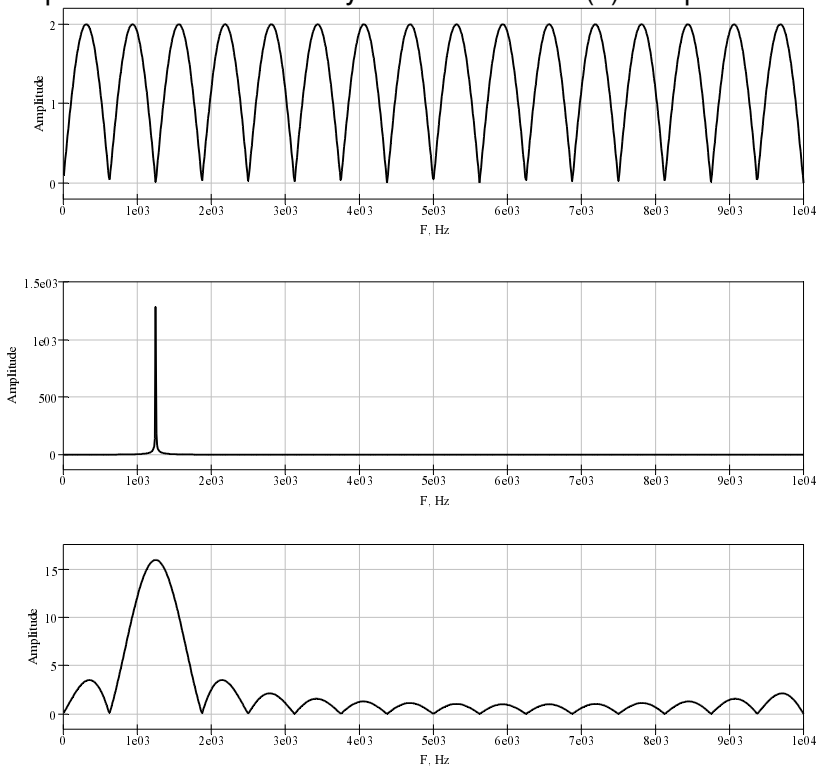


Fig. 4: The single - bin SDFT filter frequency response.

3. EXECUTION TIME IN MATLAB

The scripts performing a SDFT algorithm are written in MatLab. When calculating the execution time, we does not includes scripts realizing input-output operations, as well as those for drawing diagrams. Execution time is measured only on scripts realizing SDFT and SIDFT.

There are two ways to measure the execution time of the scripts in MatLab. First, by using the *tic* and *toc* functions, which use clock time. Second, through the functions *clock* and *etime*. The function *clock* uses the system time, changing periodically. Because of this, there can be no precise criteria for comparing the execution times. To calculate the execution time, we have used two different ways:

```
 % Using tic and toc functions
iStart = tic;
% Here is scripts of SDFT and SIDFT calculation
iElapsedTime = toc(iStart);
```

and

```
% Using clock and eTime  functions
iStart = clock;
% Here is scripts of SDFT and SIDFT calculation
iElapsedTime = etime(clock, iStart)
```

The results is shown in Fig. 5.

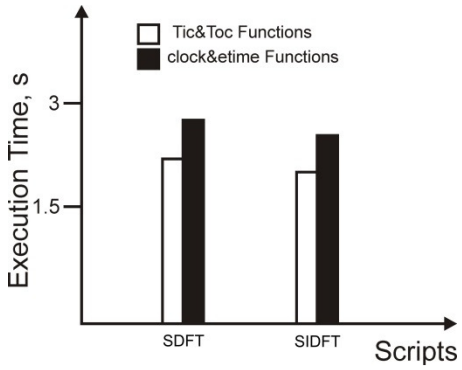


Fig. 5: Execution Times of the SDFT algorithm in MatLab.

4. CONCLUSIONS

Many factors influence the execution time of a task in the field of signal processing. In this paper we used Matlab version 7.12 on Windows 7 x64,

PC with processor Intel Celeron B800 / 4Gb RAM. Methods that are used to measure execution time is with ensure accuracy up to 0.1 seconds [5]. In this case used two different ways to measure the execution time on the same platform. Nevertheless, the execution times are different. Future work includes measuring the execution time of the SDFT algorithm on different platforms using advanced techniques.

5. REFERENCES

[1] Rabiner, L., Gold, B. (1975) Theory and Application of Digital Signal Processing. Upper Saddle River, NJ: Prentice Hall, pp. 382-383.
[2] Jacobsen, E., Lyons, R. (2003) The sliding DFT. IEEE Signal Processing Magazine, vol. 20, no. 2, pp. 74–80.
[3] Jacobsen, E., Lyons, R. (2004) An update to the sliding DFT. IEEE Signal Processing Magazine, vol. 21, no. 1, pp. 110–111.
[4] Farhang - Boroujeny, B., Lim Y. C. (1992) A comment on the computational complexity of sliding FFT. IEEE Transactions on Circuits and Systems, vol. 39, no. 12, pp 875 876.
[5] Martin K., McKeeman B. (2011) Accelerating the pace of Engineering and science. MathWorks,Inc.

Survey paper on wireless network applications implemented on FPGA

Sotirios Pouros[*], Angel Popov[**]

**Alexander Technological Institute of Thessaloniki, Greece*

***Technical University, Sofia, Bulgaria*

***Abstract**: This paper summarizes and organizes recent research results in a novel way that integrates and adds understanding to work in the particular field of wireless network protocol implementations on FPGA. Various implementations extracted unique results which are essential for the development and optimization of the proposed system. Adaptive mechanisms and protocol variations lead to a combination of summarized knowledge to be implemented in the near future. Researchers, worldwide, never stopped proposing alternatives for improvements on wireless network protocols and by the use of innovative technology have come up to the results to follow. Finally, the research team introduces an implementation scheme using FPGA.*

***Keywords:** Wireless Network Protocols, Field Programmable Gate Arrays, FPGA, WLAN*

1. INTRODUCTION

The constant evolvements of the wireless LAN technology as well as the growth of the FGPA deployment industry lead to the inevitable marriage of the two technologies. Their most significant advantages and innovations can be incorporated in solutions, exploitations and developments to benefit all. Current research projects have also adapted the use of the FPGAs in their research projects [1-9].

The industry requires engineers capable of developing relevant solutions to applications. The FPGAs and networking combined understanding can provide an essential tool for all electronic and network engineers.

The main target is to incorporate the FPGA usage in every aspect of the WLAN [18] like 802.11i [10]. The specific paper introduces FPGA implementations worldwide and an innovative approach to future development of a system on reconfigurable platforms that could be a paradigm for novel technologies using adaptive mechanisms [19].

2. METHODOLOGY – RELATED WORK

Especially through the past ten years, researchers have implemented systems depending on the industry needs and they have proposed future implementations for problem solving of vulnerabilities and system limitations.

2.1. Related Work

Paradigms on FPGA - based implementations concerning WLANs are mentioned as follows:

- PEARL: A Programmable Virtual Router Platform. A proposed architecture with new approach on PEARL platform implementations [4].
- Exploring FPGA Network on Chip Implementations Across Various Application and Network Loads [1].
- MAC Implementation for IEEE 802.11 Wireless LAN [2].
- Novel Design and Implementation of IEEE 802.11 Medium Access Control [3].
- VHDL Modeling of Wi-Fi MAC Layer for Transmitter [6].
- Synchronized CSMA Contention: Model, Implementation and Evaluation [7].
- Realization of MAC Layer Functions of ZigBee Protocol Stack in FPGA [5].
- Implementation of adaptive mechanism with aggregation and fragment retransmission for 802.11 wireless networks [8].

2.2. Need for novel implementations

The focus on WLANs, the swift proliferation of wireless data communication systems, and the ever-increasing demand for faster data rates requires that engineers be able to quickly design, implement and test new wireless algorithms for data communications [11]. The researchers have proposed designs to meet the high speed requirements [20] for the Enhanced IEEE 802.11 MAC (Medium Access Control) with hardwired logic and embedded firmware on FPGAs [2]. Moreover it has been proven that that network on chips with complex routing and switching functionality are still useful under high network loading conditions [19]. Additionally, it is also shown for our network on chip implementations, a simple solution that uses 4-5x less logic resources can provide better network performance under certain conditions [1]. Finally, the IEEE 802.11i architecture has been used on FPGA as a new security paradigm for wireless networks [10].

3. IMPLEMENTATION

The following designs will be analyzed, simulated [17] and implemented in order to create a state of the art innovative implementation of a system.

3.1. Implementing the 802.11n PHY and MAC

The paper is providing a rapid prototyping system which can be used as a starting point for developing new wireless data algorithms. The hardware to be used is:

- Xilinx Virtex-5 ML505 XUPV5-LX110T development board and
- Xilinx Spartan-II evaluation board
- Oscilloscope
- Notebook with i5 CPU and 8GB RAM
- The software to be used is:
- Xilinx ISE13
- Matlab 2011b
- Simulink 6.5
- Xilinx System Generator for DSP 13.2

The schema of the design for the OFDM transmitter and receiver is shown in Fig.1 and Fig. 2. [13]

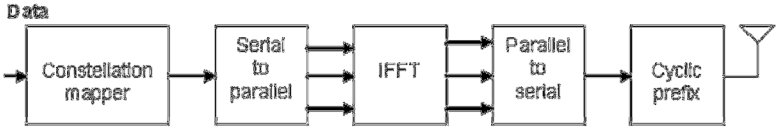


Figure 1: OFDM transmitter

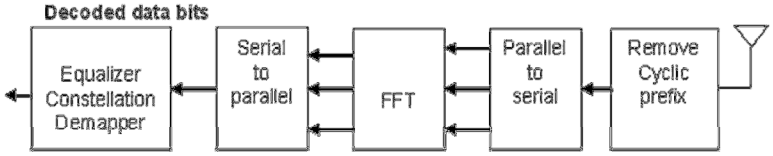


Figure 2: OFDM receiver

3.2. Evolving the WPA2 - AES IP core

A new IP core will be created to provide the security required. Both encryption and decryption will be implemented according to the IEEE 802.11i specifications. The Fig. 3 is showing the block diagrams.

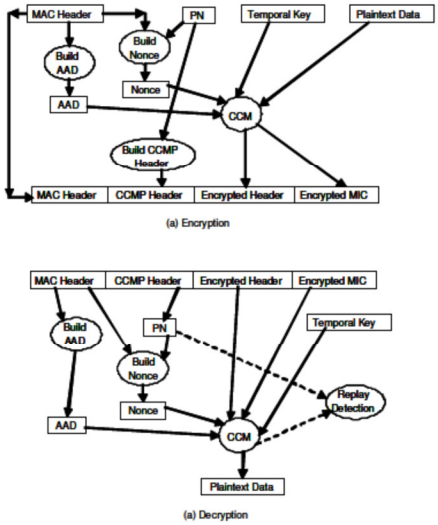


Fig. 3: IEEE802.11i encryption decryption [10].

3.3. AES Encryption Algorithm [10]

Rijndael algorithm has been selected as the new Advanced Encryption Standard (AES) algorithm by the National Institute of Standards and Technology (NIST). AES is a symmetric block cipher having variable key and fixed data length. The key lengths can be independently chosen as 128, 192 or 256 bits, which result in 10, 12 and 14 rounds of operation respectively. The data length is fixed to 128 bits. The input as well as intermediate data can be considered as a matrix with four rows and four columns called state. Each element of the matrix is composed of eight bits, therefore enabling efficient implementation of AES on 8 bit platforms also. The AES algorithm has four basic transformations.

- SubByte Transformation
- ShiftRows Transformation
- MixColumns Transformation
- AddRoundKey Transformation

3.3.1. The new AES IP Core

The WPA2 implementation fully supports the AES algorithm for 128 bit keys in Counter Mode (CTR) method of encryption with CBC message integrity check as required by the CCM protocol of the 802.11i standard and NIST SP800-38C.The new IP Core to be design will have the appropriate IOs and it will result to an IP Core similar to the one in Fig. 4.

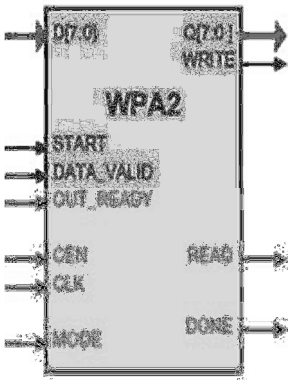


Fig. 4: WPA2 – AES IP Core [16].

The pin description of the IP Core will be as in the Tab. 1.

Tab. 1: Table of the IP Cores pin description.

Name	Type	Description
CLK	Input	Core clock signal
CEN	Input	Synchronous enable signal. When LOW the core ignores all its inputs and all its outputs must be ignored.
MODE	Input	Mode. When HIGH, transmit, when LOW receive
START	Input	HIGH starting input data processing
READ	Output	Read request for the input data byte
DATA_VALID	Input	HIGH when valid data byte present on the input
WRITE	output	Write to the output interface
OUT_READY	Input	HIGH when output interface is ready to accept data byte
D[7:0]	Input	Input Data
Q[7:0]	Output	Output Data
DONE	Output	Data processing completed

3.4. Testing

After the implementation of the system, a testing and validation of operability will take place to ensure the performance of the system. Measurements will be taken, based on specifications and standards [12].

4. CONCLUSIONS – FUTURE WORK

4.1. Proposed System

The proposed system to be implemented, based on the related work presented, will incorporate the following subsystems:

4.1.1. 802.11n PHY and MAC

An FPGA based experimental PHY and MAC for 802.11n WLAN will be designed and implemented to be capable of rapid prototyping of wireless communications algorithms. The testbed will be similar to the ones already designed [12,14,15,17]. Comparative analysis for quantifications purposes will take place.

4.1.2. Wireless Security Algorithm

The system will introduce the FPGA based new IP Core on WPA2 – AES security encryption. The security protocol around AES is the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol or CCMP. CCMP is used to encrypt or decrypt data at the MAC Protocol Data Unit.

4.2. Conclusions

An innovative system will be evolved and implemented to be compared to the existing systems. The FPGA feedback of the resources used can provide to the systems designer all the data required to optimize the system. Tools computate the use of these resources and compare utilizations. Bit Error Ratio (BER) is one of the main analysis aspects of the system.

The application should make headway to the midrange bandwidth applications as it provides flexibility of lower power consumption and cost and it offer encryption at 600Mbps. It meets current IEEE 802.11n operating data requirements and it provides cryptography, integrity and authenticity.

Future work will optimize the design for reconfigurable platforms on terms of interoperability and security algorithms based on concurrent user's number, CPU load and memory restrictions.

5. REFERENCES

[1] Schelle G.,Grunwald D., (2008), "Exploring FPGA Network on Chip Implementations Across Various Application and Network Loads", IEEE International Conference on Field Programmable Logical Applications (FPL2008), Heidelberg, Germany

[2] Youjin K., Haewon J., Hyeong L., Kyoung C., (2001), “MAC Implementation for IEEE 802.11 Wireless LAN”, 4th IEEE International Conference on ATM and High Speed Intelligent Internet Symposium, pp191-195 (ICATM 2001), Seoul, Korea
[3] Luo, Fei; Zhang, Hao L.; Zhou, Zu-Cheng (2004), “Novel Design and Implementation of IEEE 802.11 Medium Access Control”, 10th Asia-Pacific Conference on Communications, 2004 and the 5th International Symposium on Multi-Dimensional Mobile Communications Proceedings, vol 1, pp278-282, Beijing, China
[4] Gaogang X., Peng H., Zhenyu L., Yingke X., Layong L., Jianhua Z., Yonggong W., Kavé S. (2011), “PEARL: A Programmable Virtual Router Platform”, IEEE Communications Magazine, vol. 49, issue 7, pp71-77
[5] Mohana P., Radha S., (2009), “Realization of MAC Layer Functions of ZigBee Protocol Stack in FPGA”, International Conference on Control, Automation, Communication, and Energy Conservation, pp1-5, (INCACEC 2009), Perundurai, Tamilnadu
[6] Bhavikatti A., Kulkarni S., (2009), “VHDL Modeling of Wi-Fi MAC Layer for Transmitter”, IEEE International Advance Computing Conference, pp1-5, (IACC2009), Patiala, India
[7] Shi J., Aryafar E., Salonidis T., Knightly E., (2009), “Synchronized CSMA Contention: Model, Implementation and Evaluation”, IEEE Communications Society, pp2052 - 2060, (INFOCOMM2009), Rio de Janeiro, Brasil
[8] Hristov V., (2011), “Implementation of adaptive mechanism with aggregation and fragment retransmission for 802.11 wireless networks”, International Conference on Information Technologies, vol. 1, pp169, (InfoTech 2007), Bulgaria
[9] Chen W., Jin D., Zeng L., (2008), “Synchronous fine adjustable rate control circuit for Ethernet congestion management”, IEEE Electronic Letters, vol. 44, issue 4, pp325 – 326
[10] Arshad A., Nasar I., (2007), “An FPGA-based AES-CCM Crypto Core For IEEE 802.11i Architecture”, International Journal of Network Security, vol. 5, pp224 – 232
[11] Lou F., Murphy P., Frantz P., (2003), “An FPGA-based Experimental PHY for 802.11b WLAN”, The Pennsylvania State University CiteSeerX Archives, CiteSeer.
[12] Gozali R., Mostafa R., Palat C., (2001), “Virginia tech space time advanced radio (vt star)”. IEEE Radio and Wireless Conference (RAWCON) pp. 227-231
[13] Guillaud M., Burg A., (2000), “From basic concept to real time implementation: Prototyping wcdma downlink receiver algorithms-a

case study". Conference Record of the Thirty-Fourth Asilomar Conference vol. 1, pp. 84-88

[14] Murphy P., Lou F., Frantz, P., (2003). "A hardware testbed for the implementation and evaluation of MIMO algorithms", 5th Intl. Conf. on Mobile and Wireless Communications Networks

[15] Vasilko M., Machacek L., Matej M., (2001), "A rapid prototyping methodology and platform for seamless communication systems". 12th IEEE International Workshop on Rapid System Prototyping (RSP'01) pp. 70-76

[16] Security and DSP IP Cores for ASIC and FPGA Applications Available: http://www.ipcores.com/wifi_802.11i_wpa2_aes_ccm.htm (accessed March 18, 2013)

[17] Hristov V., (2007), "Simulation of wireless local area network", Proc. of the International Conference UNITECH'2007, 23-24 November, vol.I, pp. I-329 - I-332, Gabrovo, Bulgaria

[18] Hristov V., Tudjarov B., (2011), "Using Genetic Algorithm for Routing", Proceedings of CEMA'2011, 06th – 08th October , 2011, pp. 70- 73, Sofia, Bulgaria

[19] Hristov V., Kanchev M., (2008), "Investigation of Triple Play Services", 3rd International Conference on Communications, Electromagnetics and Medical Applications (CEMA'08) November 06th-08th, 2008, pp.59-63. Athens , Greece

[20] Hristov V., Petrov I., (2008), "Investigation of 802.11N WLAN Throughput", 3rd International Conference on Communications, Electromagnetics and Medical Applications (CEMA'08) November 06th-08th, 2008, pp.64-69. Athens, Greece

Improvement of forwarding process with multiple network links

Valentin Hristov*, Oleg Panagiev, Firas Ibrahim*****

**South-west University "Neofit Rilski"- Blagoevgrad, Bulgaria*
***Technical University Of Sofia, Sofia, Bulgaria*
****University Of Tabuk- Tabuk, Kingdom Saudi Arabia*

Abstract: *A scheduling algorithm must be implemented at each network facility, e.g. router or switch, to enable the sharing of the switch-limited resources among the packets traveling through it. The resources being shared include available bandwidth of linking channels and/or buffer space. The present paper aims at presenting the process of evaluating the packet forwarding mechanism, which are used for distribution of packets through number of heterogeneous linking channels and overcome limitations for delivering data over transmission protocols.*

Keywords: *packet forwarding mechanism, multiple links, heterogeneous communication channels.*

1. INTRODUCTION

Two separate computer networks can be connected through two network facilities and multiple [7],[8] communication channels between them. Load balancing allows (if the routing table has multiple paths to a destination) the router to use multiple links to a destination when forwarding packets.

Most standard routing protocols (Routing Information Protocol - RIP, Enhanced Interior Gateway Routing Protocol- EIGRP, Open Shortest Path First- OSPF, and Interior Gateway Routing Protocol- IGRP) and derived from statically configured routes allow load balancing of the communication channels. It is well known problem [2-5] with low performance with transmission of data through TCP-Transmission Protocol Transport Protocol in case of heterogeneous communication channels (different speed).

2. LOAD BALANCING

The load balancing guarantees equal load across these links, but the packets may arrive out of order at the destination [2] because differential de-

lay may exist within the network buffers. In Cisco IOS software, the forwarding process determines the outgoing interface for each packet by looking up the route table and picking the least used interface. This ensures equal utilization of the links, but is a processor intensive task and impacts the overall forwarding performance, i.e. this form of load balancing is not well suited for higher speed interfaces.

Round Robin means [1] that the network facility sends one packet for a destination over the first path, the second packet for the same destination over the second path, and so on.

In earlier work [3] an adaptive algorithm for the allocation of traffic was proposed. This algorithm is titled Rate Balance Algorithm and it is based on following principle – every packet is transmitted in that channel, which will deliver it in the correct order, i.e. earlier than the others channels. It uses formulae to determine the time of delivery of the packet (with corresponding size) over each channel, taking into account its time of the release. At the end the Rate Balance Algorithm selects this channel to deliver the packet which wills deliver it earlier relative to the others channels.

The purpose of this paper is to propose modified algorithm for the allocation of traffic which solve the problem with the low performance of these algorithms in case of heterogeneous communication channels, evaluation of its characteristics and comparing them with those of well-known other algorithms for the allocation of traffic.

3. OPTIMIZED LOAD BALANCING

Below is proposed a distributed algorithm titled Optimized Load Balancing algorithm that allows minimizing the waiting time of packets in network facilities interconnected with heterogeneous communication channels.

Keeping in mind that the algorithms for packet (frames) forwarding create extra load for CPU of the network facility, e.g. router, the computational complexity of these algorithms should be minimal.

In Fig.1 it is shown the forwarding process of packets packaged as frames $D = \{dk\}$, $k \in (1, 2... \infty)$ which entering at the entrance of the network facility. Each packet is characterized by size l_k $k \in (1, 2... \infty)$. Average value of packet's size is denoted with l. The proposed algorithm manages the N channel $C = (c1, c2... c_N)$ forming virtual channel among source and destination.

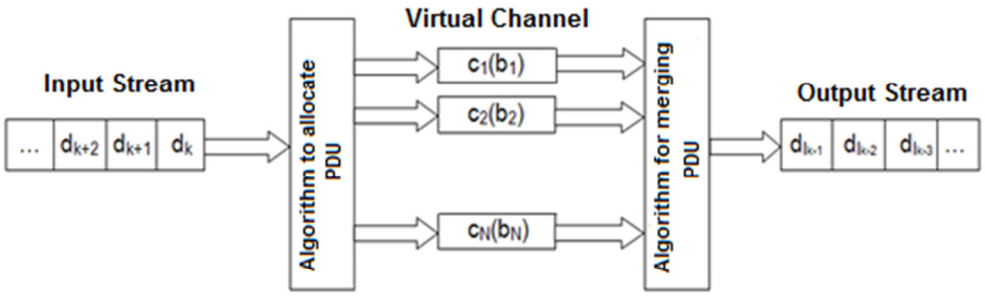


Fig. 1: Transfer of packets (Protocol Data Units- PDUs).

For each channel $c_i \in C$, $i \in \{1,2,.. N\}$ its speed is known as b_i, in bps or $\mu_i=b_i/l$, in pkts/s. Moreover $\sum\lambda_\iota=\lambda$, $i \in \{1, 2 \dots N\}$. The input packet stream is allocated to each channel with intensity λ_ι, respectively, with probability $p_i=\lambda_\iota/\lambda$, $i \in \{1,2,.. N\}$.

The proposed approach in this paper for the traffic distribution so as to minimize the waiting time of packets in network facilities for heterogeneous communication channels use mathematics methods [10], [11], and more precisely the method of Lagrange with undetermined coefficients and the well known formula for the waiting time in the M/M/1 queuing system:

$$t_i = \frac{1}{\mu_i - \lambda_i}$$

where μ_ι - the transmission speed of the packets and λ_ι - the intensity of arrival of packets in channel c_i, $i \in \{1, 2\dots N\}$ and $\mu_\iota>\lambda_\iota$.

The algorithm for traffic distribution allocates PDUs, Vd_k, $k \in (1,2 ,..., \infty)$ for each channel that is available, $c_i \in C$, with probability p_i, so as to minimize the waiting time of packets:

(1) $\sum\lambda_\iota t_i$ -> min.

According to the method of Lagrange:

(2)
$$\begin{cases} \frac{\partial \sum_{i=1}^{N} \lambda_i t_i}{\partial \lambda_1} + \lambda\xi = 0 \\ \frac{\partial \sum_{i=1}^{N} \lambda_i t_i}{\partial \lambda_2} + \lambda\xi = 0 \\ \dots \\ \frac{\partial \sum_{i=1}^{N} \lambda_i t_i}{\partial \lambda_i} + \lambda\xi = 0 \\ \dots \\ \sum_{i=1}^{N} \lambda_i = \lambda \ , i \in \{1,2,..N\} \end{cases}$$

Or

$$(3)\quad \begin{cases} \frac{\partial \sum_{i=1}^{N} \frac{\lambda_i}{\mu_i-\lambda_i}}{\partial \lambda_1} + \lambda\xi = 0 \\ \frac{\partial \sum_{i=1}^{N} \frac{\lambda_i}{\mu_i-\lambda_i}}{\partial \lambda_2} + \lambda\xi = 0 \\ \dots \\ \frac{\partial \sum_{i=1}^{N} \frac{\lambda_i}{\mu_i-\lambda_i}}{\partial \lambda_i} + \lambda\xi = 0 \\ \dots \\ \sum_{i=1}^{N} \lambda_i = \lambda \text{ , i } \epsilon \{1,2,..\text{N}\} \end{cases}$$

Whence for λ_ι:

$$(4)\quad \frac{\mu_i}{(\mu_i - \lambda_i)^2} + \lambda\xi = 0$$

Or

$$(5)\quad \mu_i + \lambda\xi(\mu_i - \lambda_i)^2 = 0$$

For a solution to equation (5), then ξ is negative because λ_i and μ_l, i ϵ {1, 2 .., N} are speeds and are positive numbers.
Equation (5) has only one root in the field of eligible values, because $\mu_\iota > \lambda_\iota$:

$$(6)\quad \lambda_i = \mu_i - \sqrt{\frac{\mu_i}{-\lambda\xi}}$$

Substituting (6) in the last equation from (2), we obtain for the literal in which participate ξ:

$$(7)\quad \sum_{j=1}^{N}\left(\mu_j - \sqrt{\frac{\mu_j}{-\lambda\xi}}\right) = \lambda$$

Or

$$(8)\quad \sqrt{\frac{1}{-\lambda\xi}} = \frac{\sum_{j=1}^{N}\mu_j - \lambda}{\sum_{j=1}^{N}\sqrt{\mu_j}}$$

Substituting in equation (6) with equation (8), we obtain the desired intensity-λ_ι **:**

$$(9) \quad \lambda_i = \mu_i - \left(\sum_{j=1}^{N} \mu_j - \lambda \right) \frac{\sqrt{\mu_i}}{\sum_{j=1}^{N} \sqrt{\mu_j}}$$

Finally, taking into account, that $\mu_i = b_i / l$, the intensity with which the algorithm distributes data to each channel c_i , λ_i, $i \in \{1,2,.. N\}$ is obtained:

$$(10) \quad \lambda_i = \frac{b_i}{l} - \left(\sum_{j=1}^{N} \frac{b_j}{l} - \lambda \right) \frac{\sqrt{b_i}}{\sum_{j=1}^{N} \sqrt{b_j}}$$

, respectively the probability p_i is obtained:

$$(11) \quad p_i = \frac{b_i}{\lambda l} + \left(1 - \frac{1}{\lambda l} \sum_{j=1}^{N} b_j \right) \frac{\sqrt{b_i}}{\sum_{j=1}^{N} \sqrt{b_j}}$$

Distribution algorithm allocates the PDUs to one of the channels by drawing a random number in the interval (0,1) and determines in which interval the number falls $\{(0, p_1), (p_1, p_1 + p_2), \ldots , (p_1 + p_2 + \ldots, 1)\}$.

We are going to get the numerical results [9] for the waiting time of packets for Optimized Load Balancing and Load Balancing mechanisms for communication channels with two different speeds (BW1 = 100Mbps and BW2 = 400Mbps). As the name suggests, in Load Balancing, packets are assigned to each of the channels, so that their load is the same, i.e. in this case the Load Balancing algorithm will allocate to the second channel four times more packets than to the first channel (p_1=const=0.2 and p_2= const=0.8).

It is expected that Optimized Load Balancing algorithm is better than Load Balancing because it allows minimizing the waiting time of packets in network facilities for heterogeneous communication channels.

4. CONCLUSION

This paper proposed a modified algorithm for routing of traffic to overcome problems with the low performance of TCP for heterogeneous communication channels. Few different algorithms for traffic distribution are analyzed and a comparison is made between them for the case of two communication channels with different speed.

Algorithm for the distribution of traffic is proposed OptimizedLoad-Balancing, which allows to minimize the waiting time of packets in network facilities for heterogeneous communication channels.

5. REFERENCES

[1] А.Филимонов, Построение мультисервисных сетей Ethernet, БХВ-Петербург, 2007;

[2] Поляков А, Адаптивныій подход К распределению информационныіх блоков по каналам передачи данныіх, журнал „Електросвязь“, №6, 2009, стр.32-35;

[3] Христов В, М.Иванов, Оценяване на алгоритми за разпределяне на трафик, Сборник с доклади ELEKTRONICA’ 2010, София, 28 Май 2010, с. 287-293. ISSN 1313-3985;

[4] Танева Л, К. Н. Славков, К. К. Славков, “Аудио/видео предавател, работещ в метровия телевизионен обхват”, Електроника’2010, 28 май 2010г., София, Доклади, стр.409-413.

[5] Adiseshu H, Parulker G, Varghese G, “Realible FIFO Load balancing over multiple FIFO channels”, Washington University, USA, 1995;

[6] Keshav S., Mathematical Foundations of Computer Networking, Addi-son-Wesley Professional, 2012.

[7] L. Taneva, R. Bagalev, “Testing in electronics manufacturing”, FMNS’2011, 8-11 June 2011, Blagoevgrad, Proceedings Volume 1, p. 153-158.

[8] L. Taneva, “ Intelligent Module for Data Exchange using CAN Inter-face”, CEMA’09, 8-10 October 2009, Sofia, Proceedings p.102-104.

[9] L.Docheva, Sn.Pleshkova, Al.Bekjarski. Application of Labview and Matlab software Products for infrared objects detection. 16th WSEAS International Conference on SYSTEMS (part of the 16th CSCC / CSCC 2012), Kos Island, Greece, pp.179-182.

[10] Sh. Sehati Dehkharghani, A. Bekiarski, S. Pleshkova. Application of Probabilistic Methods in Mobile Robots Audio Visual Motion Control Combined with Laser Range Finder Distance Measurements. 11th INTERNATIONAL CONFERENCE on Circuits, Systems, Electronics, Control & Signal Processing, CSECS 2012, Montreux, Switzerland, 2012, pp.91-99

[11] Pleshkova-Bekiarska Sn., Al. Bekiarski, Sound Propagation Model for Sound Source Localization in Area of Observation of an Audio Ro-bot, International Journal of Neural Networks and Application, 2(1), Januare-June 2009, © International Science Press, India, pp.1-4.

On DSP's Performance versus General Purpose Processors

Dimitar Manolev, Vencislav Petrov

South-West University "Neofit Rilski", Blagoevgrad, Bulgaria

***Abstract**: Digital signal processors (DSP) are processors, ensuring the required number of operations for signal processing and performing complex tasks in real-time, such as synthesis and analysis of speech, processing of medical images, wireless communications and more. Solving these problems would be sometimes difficult or even impossible to using General Purpose Processors. This paper presents a comparative analysis of the possibilities of DSP processors and General Purpose Processors for solving problems associated with digital signal processing. Future work includes computational cost analysis by using algorithms for processing of signals and images with high performance on graphics Processing units (GPUs).*

***Keywords:** Digital Signal Processor, Digital Signal Processing, Image Processing, GPP processors.*

1. INTRODUCTION

Using methods and algorithms to solve specific problems related processing of signals and images is associated with two major problems. First, the number of mathematical operations that used. The increased number of operations requires more execution time of an algorithm. The development of a algorithms with a small number of mathematical operations can be a difficult task. Second, the performance of processors fulfills these algorithms. However, this depends on many factors. GPP performance can be measured in many ways. Usually GPP performance is measured by the time for which a processor can execute a task. On the other hand, factors such as operating frequency, the addressing modes, the opportunity to work with floating point numbers, power consumption, etc.., affect the performance of GPP. In this paper we are going to present some features of DSP processors and General Purpose Processors in the implementation of signal processing algorithms.

2. FACTORS AFFECTING PRODUCTIVITY

Different types of processors are oriented towards solving different tasks. Generally, they can be separated into two groups processors: General purpose processors and specialized processors performing specific tasks [1].

- CPUs - Processors for PCs and workstations, such as the Intel Pentium.
- GPPs - Processors for embedded applications. A typical example is the ARM processor (Advanced RISC Machine).
- DSPs - Processors specialize in the signal processing and image processing. These are TMS320C6XXX series of Texas Instruments.
- Low-end DSP and GPP - have low cost and old architectures.
- High-performance DSP and GPP - use advanced techniques to increase productivity (Multi-core DSP)

Tab. 1

High - Performance		**Low - End**	
DSP	*GPP*	*DSP*	*GPP*
TMS320C64XX	Intel P4	TMS320C54XX	
TMS320C62XX	Power PC G4	TMS320C55XX	ARM9 series
ADSP-BF5xx6xx	ARM 11 (SIMD)	Motorola DSP/58000	

When solving problems in the field of digital signal processing and image processing significant effects on the performance have the following factors:

- Architecture and instruction set. In the Low-end DSPs instructions are complex and perform multiple operations. In GPP single instruction performs a single operation. It follows that if an equal number of instructions to be executed, DSP processors have an advantage in terms of execution time versus GPPs.

For DSP: One instruction multiple operations

```
mac x0,y0,a x:(r0)+,x0 y:(r5)+,y0
```

For GPP: Multiple instructions

```
mpy r2,r2,r3
add r3,r4,r4
mov (r0),r2
mov (r1),r4
inc r0
inc r2
```

High-performance DSP and GPP use different types of architectures. Traditionally, DSPs using VLIW (Very Long Instruction Word) architecture [2]. For one cycle be executed to 8 instructions. TI's DSP TMS32064xx have such architecture. In contrast the architecture of the GPPs is superscalar with up to 4 instructions per cycle.

Memory architecture. Another factor that has affects on data access. In the field of digital signal processing and image processing using large data sets, such as streams of digital data and high dimension image. The data access mode can significantly improve the processing.

Low-end DSPs have Harvard architecture with 2-4 memory accesses per cycle. Not use data cache. On-chip SDRAM and DMA (Direct memory access) are use (Fig.1).

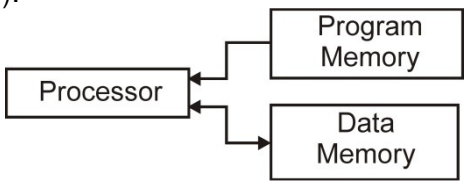


Fig. 1: Low-End DSPs.

Low-end GPPs have Von Neumann architecture with 1 memory accesses per cycle. Typically use caches (Fig. 2).

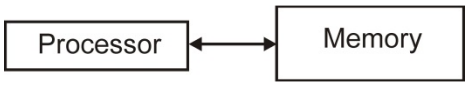


Fig. 2: Low-End GPPs.

High- performance DSPs with Harvard architecture have a 1-8 memory accesses per cycle. In some cases there use caching of data. Unlike Low-end GPPs, high- performance GPPs with Harvard architecture have 1-4 memory accesses per cycle (Fig.3). Usually use caches.

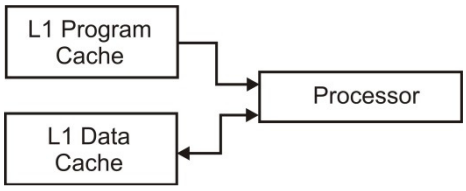


Fig. 3: High-Performance GPPs.

- Data Parallelism SIMD (Single Instruction Multiple Data). In Low-end DSP SIMD features are limited. Low-end GPP no support SIMD.

- Addressing. DSPs have embedded units for generate addresses and specialized addressing modes: Autoincrement; Modulo (Circular); Bit-reversed (for FFT). GPPs have General-purpose addressing modes.

3. CONCLUSIONS

So, what is the choice when you need to solve tasks in the field of signal processing and image processing, DSP or GPP?. DSPs have an advantage in the signal processing. But, to fully realize these benefits must be considered and other factors. Eg., use low-level languages such as assembler. Programs occupy less code space and the code run faster. In terms of the performance, the complex instructions gives advantage of DSP. There is no precise criteria for assessing the performance of DSP and GPP. When DSP and GPP equally fast there are other factors such as power consumption, chip integration, tools, etc. They can vary depending on benckmark.

4. REFERENCES

[1] Williston, K., (2005) *Microprocessors vs. DSPs:Fundamentals and Distinctions*. Berkeley Design Technology, Inc.

[2] M. Saghir, P. Chow, and C. Lee.,(1998) *A comparison of traditionaland VLIW DSP architecture for compiled DSP applications*. InCASES ’98, Washington, DC,USA

[3] Frantz G.,(2000) *Digital signal processor trends*, Micro, IEEE, vol.20,no.6, pp.52-59

Laboratory course development for teaching discipline PLD programming

Valeri Vachkov*, Ivo Angelov*, Petar Manoilov**

**South West University "Neofit Rilski", **Technical University of Sofia,*

***Abstract**: The aim of present paper is to describe an example of lab exercise used for the students training in discipline "PLD programming" for bachelor program.*

***Keywords:** PLD, FPGA, VHDL, Spartan 3E*

1. INTRODUCTION

The Basys2 development board [2] by Digilent Inc. is a circuit design and implementation platform that can be used to gain experience building real digital circuits. Ten boards were purchased and are used in the practical exercises of the students of speciality "Computer systems and technologies" in the South-West University. The Basys-2 board provides complete, ready-to-use hardware suitable for hosting circuits ranging from basic logic devices to complex controllers. A large collection of on-board I/O devices and all required FPGA support circuits are included, so countless designs can be created without the need for any other components [1].

The main characteristics of the board are [1] :

- Xilinx Spartan 3-E FPGA, 100K or 250K gates
- FPGA features 18-bit multipliers, 72Kbits of fast dual-port block RAM, and 500MHz+ operation
- USB 2 full-speed port for FPGA configuration and data transfers (using Adept 2.0 software available as a free download)
- XCF02 Platform Flash ROM that stores FPGA configurations indefinitely
- User-settable oscillator frequency (25, 50, and 100 MHz), plus socket for a second oscillator
- Three on-board voltage regulators (1.2V, 2.5V, and 3.3V) that allow use of 3.5V-5.5V external supplies
- 8 LEDs, 4-digit seven-segment display, four pushbuttons, 8 slide switches, PS/2 port, and a 8-bit VGA port
- Four 6-pin headers for user I/Os, and attaching Digilent PMOD accessory circuit boards

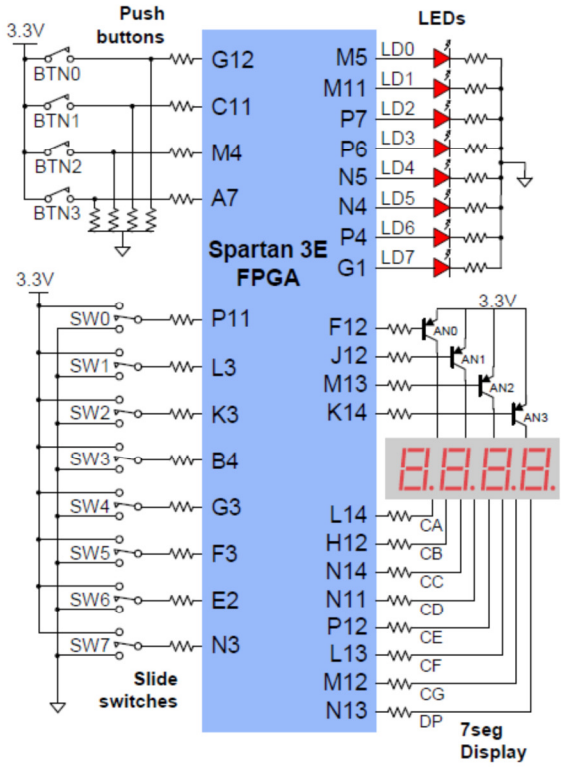


Fig. 1: Main IO circuits of Basys-2.

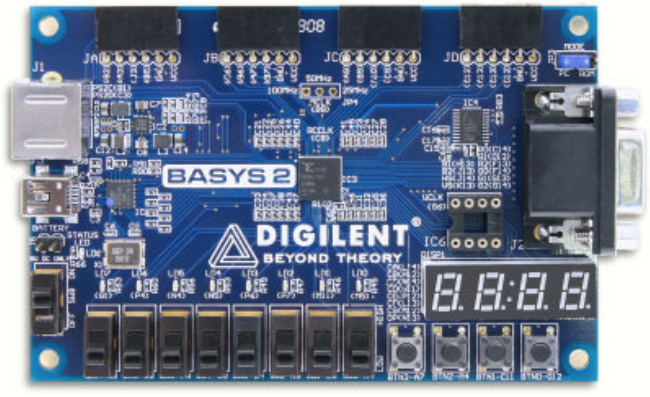


Fig.2: Basys-2 development board [1].

The described board will be used for the students training in “PLD programming” (bachelor course) and “Systems on Chip Design” (master

course). The board was used also as a tool for the design and implementa- implementation of specific digital devices on FPGA - chips [3][4].

2. EXERCISE EXAMPLE

A example exercise which uses 8- bit binary counter and 7- segment decoder is presented in this paper. The designed counter is a functional analog of the TTL 8-bit counter with output registers and 3 state outputs 74LS590 and is described in VHDL with the following code:

```
library ieee;
use ieee.std_logic_1164.all;
use ieee.std_logic_unsigned.all;

entity counter is
  port(C, CLR, CE, CS, regC : in std_logic;
       Q : out std_logic_vector(7 downto 0));
end counter;
architecture archi of counter is
  signal tmp, out_reg: std_logic_vector(7 downto 0);
  begin
    process (C, CLR)
      begin
        if (CLR='1') then
          tmp  <= "00000000";
         elsif (C' event and C='1') then
          if (CE='1') then
            tmp  <= tmp + 1;
          end if;
        end if;
    end process;

  process (regC, C)
     begin
       if (regC' event and regC='1') then if C='0'then  -- C should be replaced with
CE in real counter
           out_reg <= tmp ;  end if ;
      end if ;
  end process ;

  Q <= out_reg when CS='1' else "ZZZZZZZZ" ;

end archi;
```

Binary to 7- segment decoder was also described in VHDL:

```
library IEEE;
use IEEE.STD_LOGIC_1164.ALL;
use IEEE.STD_LOGIC_ARITH.ALL;
use IEEE.STD_LOGIC_UNSIGNED.ALL;

entity segdec is
port (
      clk : in std_logic;
        bcd : in std_logic_vector(3 downto 0);  --BCD input
        segment7 : out std_logic_vector(6 downto 0)  -- 7 bit decoded output.
    );
end segdec ;

--'a' corresponds to MSB of segment7 and g corresponds to LSB of segment7.
architecture Behavioral of segdec is
signal Tsegment7: std_logic_vector(6 downto 0);
 begin

 process (clk, bcd)
  begin
    if (clk'event and clk='1') then
      case  bcd is
         when "0000"=> Tsegment7 <="0000001";  -- '0'
         when "0001"=> Tsegment7 <="1001111";  -- '1'
         when "0010"=> Tsegment7 <="0010010";  -- '2'
         when "0011"=> Tsegment7 <="0000110";  -- '3'
         when "0100"=> Tsegment7 <="1001100";  -- '4'
         when "0101"=> Tsegment7 <="0100100";  -- '5'
         when "0110"=> Tsegment7 <="0100000";  -- '6'
         when "0111"=> Tsegment7 <="0001111";  -- '7'
         when "1000"=> Tsegment7 <="0000000";  -- '8'
         when "1001"=> Tsegment7 <="0000100";  -- '9'
         when "1010"=> Tsegment7 <="0001000";  --'A'
         when "1011"=> Tsegment7 <="1100000";  --'b'
         when "1100"=> Tsegment7 <="0110001";  --'C'
         when "1101"=> Tsegment7 <="1000010";  --'d'
         when "1110"=> Tsegment7 <="0110000";  --'E'
         when "1111"=> Tsegment7 <="0111000";  --'F'
         when others=> Tsegment7 <="1111111";
      end case;
  end if;

end process;
  segment7 <= Tsegment7  when clk='1' else "ZZZZZZZ" ;
end Behavioral;
```

The exercise is carried out in the following steps:

- A new project is created in ISE12.1 for XC3S100E device in CP132 package with Top-Level Source Type “Schematic”;
- A new source type “Schematic” is added to the empty project;
- The counter and the decoder are added to the project as VHDL modules ; The code is pasted over the template ;
- Schematic Symbols are created from these VHDL modules;
- The following circuit diagram (Fig. 3) is drawn in the schematic editor of ISE 12.1 in the Top-Level Source Type “Schematic” SCH1 sheet;

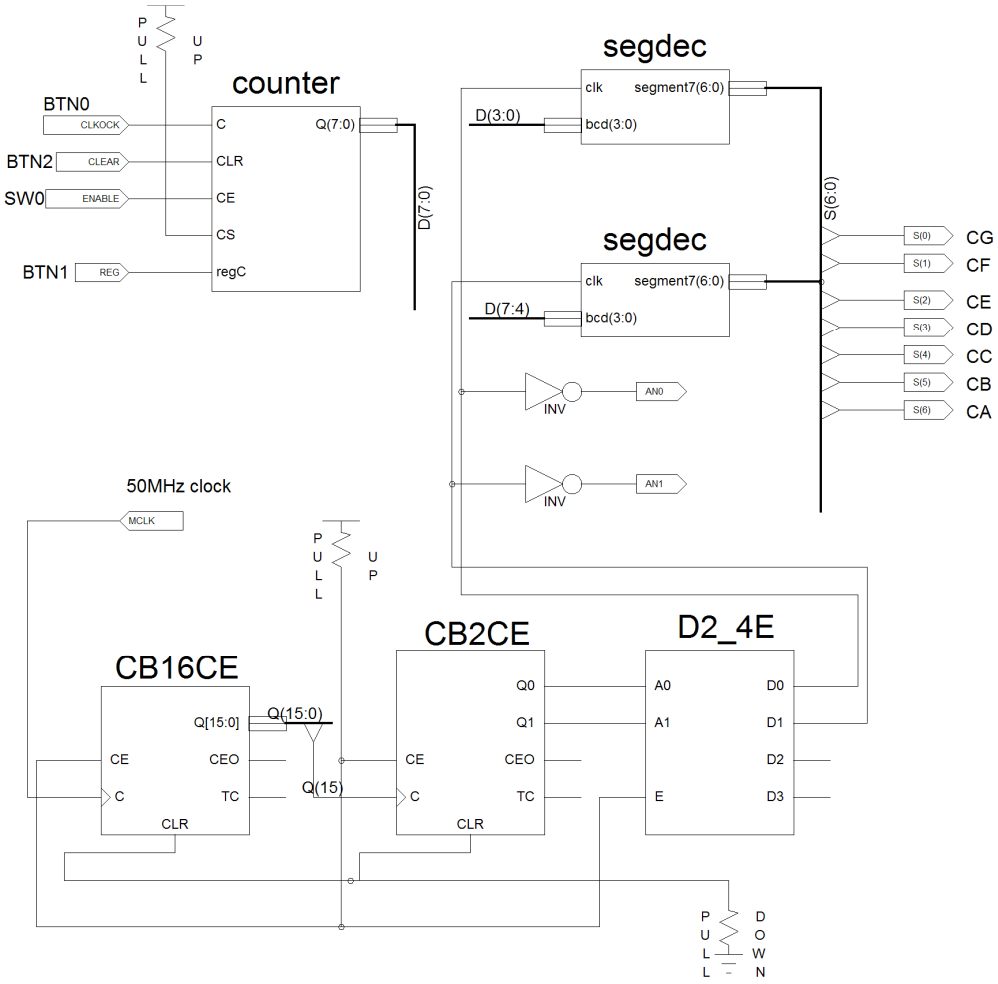


Fig. 3: Schematic diagram of the example exercise.

- I/O pin planning is carried out for the project, using PlanAhead program;

The ports are assigned to pins of the FPGA chip, with respect to the BASYS-2 I/O circuits diagram , Fig. 2 ;

- Programming file is generated ;
- The generated BIT file is used to configure the on-board XC3S100E FPGA, using ADEPT software.

After these steps the students could check the characteristics of the designed counter and decoder, using the buttons BTN0 – BTN1, the switch SW0 and the 7 segment LED indicators. The designed components and circuit could be compared with TTL based chips (for example 74LS590, 74LS47).

3. CONCLUSIONS

The board is extremely flexible and cost effective solution for students training in PLD and FPGA programming. The exercises are a little bit time consuming, and preliminary preparation for the students as home work is needed.

4. REFERENCES

[1] Digilent Inc. , Basys™2 Spartan-3E FPGA Board http://www.digilentinc.com/Products/Detail.cfm?Prod=BASYS2

[2] Digilent Inc. , Basys 2 reference manual http://www.digilentinc.com/Data/Products/BASYS2/Basys2_rm.pdf

[3] Hristov, V., Simulation of Selective Repeat Automatic Retransmission Request Scheme, 5th International Conference on Communications, Electromagnetics and Medical Applications (CEMA'10) Athens , Greece, October 7th-9th, 2010, pp.49-53.

[4] Pouros S., A. Popov, V. Hristov, Laboratory course development for teaching DSP and digital filters implementations on FPGA, Proc. of the Conference FMNS'2011, Blagoevgrad,Bulgaria, 8 - 11 June, 2011, vol. 1, pp. 209- 216.

Bachelor Degree Education in the Department of Computer Systems and Technologies of South-West University

Iliya Tinyokov, Stanko Shtrakov, Emil Radev, Valeri Ivanov

South-West University "Neofit Rilski", Blagoevgrad, Bulgaria

***Abstract**: Present paper describes the sequence of bachelor degree education in the department of "Computer Systems and Technologies" of South-West University "Neofit Rilski". It reveals the main taught disciplines and explains shortly their syllabuses. It is given an assessment of the work and development of the department in the university.*

***Keywords:** Education; Bachelor Degree; Department of "Computer Systems and Technologies"; Curriculum.*

1. INTRODUCTION

During the last decade of the past century fundamental changes in the political life of the country occurred in Bulgaria that influenced the economic processes. So far developing electronics industry began to decline, but computer systems began spreading out massively in all the areas of human life.

These changes do not remain unnoticed by the management of the South-West University "Neofit Rilski" and the specialty "Computer Systems and Technologies" occurs among the specialties of the university. The apogee of this trend might be considered the year 2003, when the specialty differentiates in the separate department "Computer Systems and Technologies". The aim of the department is training and formation of engineers, capable of not only maintaining computer systems, but also successfully developing new computer components and devices.

2. BACHELOR DEGREE EDUCATION IN THE DEPARTMENT

Education in bachelor degree program of the department of "Computer Systems and Technologies" might be divided into four: introduction to specialty, fundamental (common) training, special training and additional specialization (fig. 1).

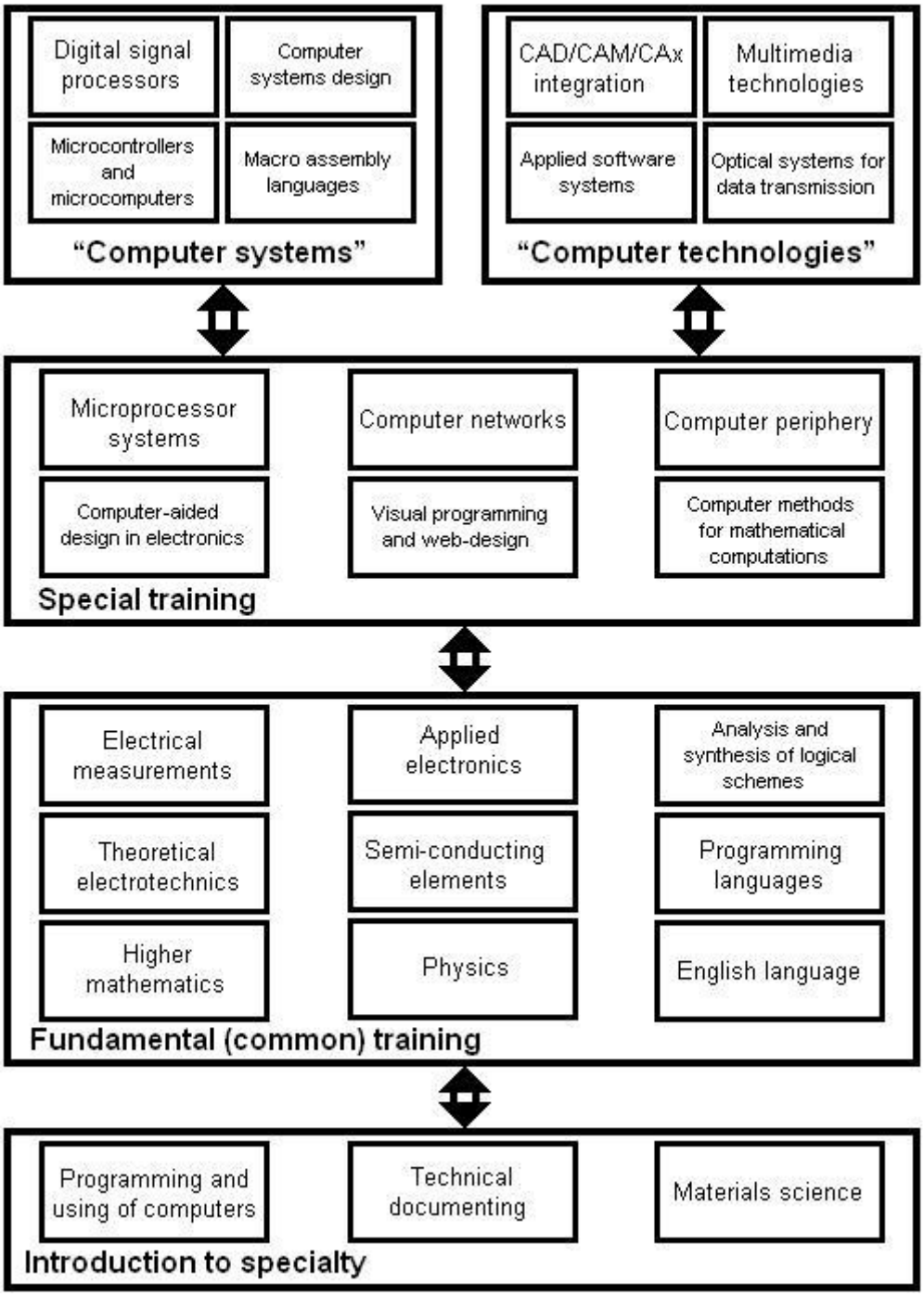


Fig. 1: Education in bachelor program "Computer Systems and Technologies".

During the introduction to the specialty the emphasis is on the assimilation of the main elements of Technical documenting, Materials science, also of the main concepts of Programming and using of computers.

Fundamental training is based on the detail familiarization with the principles of the Higher mathematics and Physics. This cycle is closed by the fundamental knowledge and skills, required in work with computer systems and in subsequent training. It includes studying of the disciplines: Higher mathematics, Physics, Theoretical electrotechnics, Semi-conductive elements, Analysis and synthesis of logical schemes, Applied electronics, Electrical measurements, Programming languages.

Specializing of the computer engineer further evolves with learning of the disciplines: Microprocessor systems, Computer networks, Computer periphery, Computer-aided design in electronics, Visual programming and web-design, Computer methods for mathematical computations.

In the final year of the course students are divided into two groups for additional specialization [1]. They can choose either the specialization “Computer systems” or the specialization “Computer technologies”. This contributes to their development in their desired direction. “Computer systems” offers the following disciplines: Digital signal processors, Computer systems design, Macro assembly languages, Microcontrollers and microcomputers. On the other hand, “Computer technologies” offers: CAD/CAM/CAx integration, Applied software systems, Multimedia technologies, Optical systems for data transmission.

Listed disciplines’ descriptions are as follows [9]:

Higher mathematics develops the mathematical skills, acquired at the high school and it reveals the main principles in evaluating the elements of the electrotechnics.

Physics studies in detail physical principles and physical quantities as a whole.

Theoretical electrotechnics reveals the main electrical circuits for connecting different electrical elements and the corresponding mathematical equations and applicable laws.

Semi-conducting elements reveals the content and structure of electronic circuits’ components, the way of connecting them in electrical circuits, physical evaluation of their main parameters.

Analysis and synthesis of logical schemes – this course is designed for familiarizing the students with the general theory and basic techniques for analysis and synthesis of logic schemes. It discusses general methods for presentation, transformation and minimization of logical functions. Students learn how to create logical schemes (consisting of logical elements, e.g. AND, OR, NOT), analyze and modify them.

Applied electronics – this discipline introduces students to the circuitry of modern electronic devices and their various applications in real life.

Students acquire skills in analyzing the circuits of different devices, used in such areas as measurement, control and management of production processes and also in compilation of simple electronic circuits.

Electrical measurements – this discipline provides basic knowledge in measuring the parameters of electrical circuits, use of measuring devices, correct data analysis and presentation.

Programming languages – this course familiarizes students with general principles of object-oriented programming. It presents fundamental constructs of conventional and object-oriented programming that are consolidated with learning of C++ language.

Microprocessor systems – reveals major design methods in developing microprocessor systems, techniques for attaching peripherals (analog-to-digital converters, digital-to-analog converters, keyboards, displays) and for establishing connections between microprocessor systems.

Computer networks – presents the problems concerning design, building and application of computer networks. The main principles of building and functioning of Local Area Networks are described. Many communication protocols are discussed.

Computer periphery deals with the structure, organization, types of devices and the basic principles and methods of their work.

Computer-aided design in electronics – it examines modern tools for computerization of engineer's labour in electronics designing. This course trains students to work with specific application systems for simulation and analysis of electronic circuits.

Visual programming and web-design – introduces the students with modern programming languages (visual and object programming) and with powerful tools for web application development. This course observes the main principles of object-oriented programming and their implementation in different programming languages – Pascal, C++, C#, Java and others. Basic principles in web-site development are described (writing HTML codes, programming in Java and Java Script, using databases).

Computer methods for mathematical computations – this discipline familiarizes students with fundamental principles and techniques for computerizing the mathematical problems resolving. It represents basic numerical methods for mathematical computations in mathematical analysis, algebra and differential equations, which are applicable for solving various engineering problems, physics problems, etc.

Digital signal processors – familiarizes students with the main advantages and techniques in digital signal processing. Students learn how to implement signal processors in realization of the methods, technologies and technical means in computer systems and networks, in audio and video systems [5-7].

Computer systems design – this course is aimed at familiarizing the students with general techniques and tools for development and adjustment of computer systems. Basic principles of computer components' design are discussed, such as: system buses and memory modules, input/output modules, computer interfaces, printed circuit boards (PCBs).

Macro assembly languages – the discipline presents I32/64 processor architecture, pipelining and optimizations. Students are trained in developing assembly applications, data models, directives, many features of MMX/XMM processor instructions and development environments for high-level programming languages are discussed, and many examples of I/O applications are given.

Microcontrollers and microcomputers – reveals general features in architecture, design and implementation of microcontrollers. It familiarizes students with the structure, main subsystems and program model of microcontrollers, their application in designing different embedded systems and single board computers.

CAD/CAM/CAx integration – it represents the capabilities of using computers in designing and manufacturing. Students learn how to use software systems for Computer-Aided Design and Computer-Aided Manufacturing. This kind of knowledge assists in growth of specialists that are able to design and put into production complex technical products in strict time limits.

Applied software systems – the course is aimed at familiarizing the students with the basic features of some of today's application software for processing and editing texts and tables, for database management, for creation and editing of images and animations. During the exercises, students explore in depth some specific software systems, like MS Office, Corel Draw and Adobe Photoshop.

Optical systems for data transmission – the discipline presents modern concepts in development of optical networks for data transmission. The fundamental principles of propagation of light in optical fibers are explained. Students understand the difference between different types of optical fibers, their optical characteristics and capabilities. The basic types of equipment, used in the construction of optical networks, and their basic modules are discussed. In addition, the basic techniques for modulation and multiplexing are discussed.

Multimedia technologies – this discipline helps students develop their skills in using recent applied software products for creation and edition of texts, tables, images and animation. During the exercises, students explore in depth some specific software systems, like Corel Draw, Adobe Photoshop, Macromedia FLASH MX and 3 DS MAX. Particular attention is paid to both the technology of creation of 3D images and animation, and the peculiarities of recording and reproducing sounds.

It is important to note that language education is essential part of computer engineers' training [8]. Computer science terminology is mainly in English, thereby English is being taught as the basic foreign language. This provides fluent use of the language as a whole, and mastering the comprehensive terminology in computer systems area.

The research work [2],[3],[4],[10],[11] in the department is in the following areas: Computer networks, Materials science, Electrotechnics and Electronics. The acquired results from the research work are used in students' training, which provides them with the latest achievements in computer science.

The laboratories of the department of Computer Systems and Technologies are well equipped. This fact guaranties quality conduction of laboratory exercises and supports students in their accumulation of practical skills.

Lecturers of the department maintain relationships with colleagues specialists from many Bulgarian and foreign universities, which ensures the exchange of information and practical application of the latest innovations in students' education in the specialty "Computer Systems and Technologies" of South-West University "Neofit Rilski".

All of these facts provide the bachelor program "Computer Systems and Technologies" to focus on establishing high-professional training and develop professionals with solid fundamental knowledge of computer engineering. The received skills and knowledge in the field of computer systems and technologies help students to know how to use the modern information and communication technologies to solve practical problems in a variety of fields, as well as careers as Computer Engineering, Software Engineering, System Design, Technical Support, etc.

Department of Computer Systems and Technologies provides education not only in a bachelor degree program, but also in a master degree program and in a Ph.D. program.

3. CONCLUSIONS

In conclusion it should be noted that the work of the department is constantly enriched and improved. Its curriculum is in line with the latest advances in the computer systems area. Modern teaching techniques cover the entire preparation process. This confirms the deserved admiration on the occasion of the department's 10th anniversary.

4. REFERENCES

[1] Curriculum of bachelor program “Computer Systems and Technologies”, South-West University, Bulgaria, avail. at http://cst.swu.bg.

[2] Hristov, V., A DCCP Congestion Control Mechanism, Proceedings of the International Conference on Information Technologies (InfoTech-2008), September 19-20, 2008, Bulgaria vol. 2, pp. 91-96.

[3] Hristov, V., Session initiation protocol interworking with traditional telephony and signaling delay introduced by Internet, Proceedings of the International Conference on Information Technologies (InfoTech-2010), September 16-17, 2010, Varna, Bulgaria, pp. 167-172.

[4] Hristov, V., and V. Vatchkov, Web based system for microscope observation with structural analyzer EPIQUANT, Engineering Science Magazine, 2006, No 2, pp. 17-24.

[5] Pleshkova, S., A. Bekiarski, Thermo vision system with embedded digital signal processor for real time objects detection, 10rd International Conference on Computational Intelligence, Man-Mashine Systems and Cybernetics, CIMMACS 2011, Jakarta, Indonesia, 2011, pp.137-142.

[6] Al.Bekiarski, Sn. Pleshkova. “Audio Information Processing for speech Localization in Multimedia Surveillance Station with Mobile robot”, Multimedia Communications, Services and Security, MCSS 2010, 6-7 May 2010, Krakow, Poland, pp. 15-19

[7] Al.Bekiarski, Sn. Pleshkova. „MPEG-4 Video and Audio Information Processing in Audio Visual Mobile Robot Systems”, 9th WSEAS International Conference on SIGNAL PROCESSING (SIP'10), Catania, Italy, pp.58-61

[8] Regulations of educational activities, South-West University, Blagoevgrad, Bulgaria, avail. at www.swu.bg.

[9] Syllabuses of bachelor program “Computer Systems and Technologies”, South-West University, Bulgaria, avail. at http://cst.swu.bg.

[10] Стоилов А., В. Христов, В. Юруков, Интегрирана CMS/DMS платформа за обслужване на дейностите във ВУЗ, сп. “Електротехника и електроника”,бр. 9-10/2007, с. 26-32.

[11] Христов, В., Л. Танева и А. Вулжев. Изследване на възможностите за намаляване на неравномерността на мрежовия трафик, Сборник с доклади Електроника'2012, София, 14.06.2012 - 15.06.2012г, с.232-237.

Mission critical radio systems. Status and trends in Bulgaria

Alexey Stefanov

College of Telecommunications and Post, Sofia, Bulgaria

Abstract: *This is an effort to establish an accepted definition for mission critical radio systems and the strategy of implementation of new technologies in PMR (professional Mobile radio) in republic of Bulgaria. It is described the situation at the moment and road map to be followed for building a modern system, based on the existing legacy is given.*

Keywords: *Mission Critical, TETRA, DMR, PMR, dispatcher systems*

Society in its current phase of development has an ever increasing need in a variety of different areas of technology including the means in which we communicate. We have to continue to innovate and develop new technologies and improve legacy systems if we are to meet the high demands of the modern pace of life and ensure its normal functioning as a single organism, including the safety and security of its individual members.

In this regard, it is essential to achieve a high level of efficiency in radio communications, to be able to provide communications in all situations of disasters, accidents or incidents and in particular social danger - so-called "mission critical communication systems".

This document will focus primarily on the high frequency part of radio technology, namely in its most dynamic and complex form as a solution to the said situations.

The concept of mission critical communication systems has been used in the field of public safety for decades, but unfortunately there has not been a uniquely comprehensive and universal definition based on world standards of what lies behind this concept. Generally this is an unusual situation, the development of this communication system if not clear and properly documented could lead to a crisis or to cause damage and casualties, there is a definite need to promptly and properly control the development of the said system [3].

For the said system to be effective it needs co-operation, rational means of all the relevant public safety stakeholders, this needs to be done to ensured cooperation and harmony throughout the network. Standardization of internal operational telecommunication features and services is essential to achieve the ultimate goal - ensuring smooth functioning of society.

The procedure of the operation of an overall organized system during a crisis situation is presented in Fig. 1.

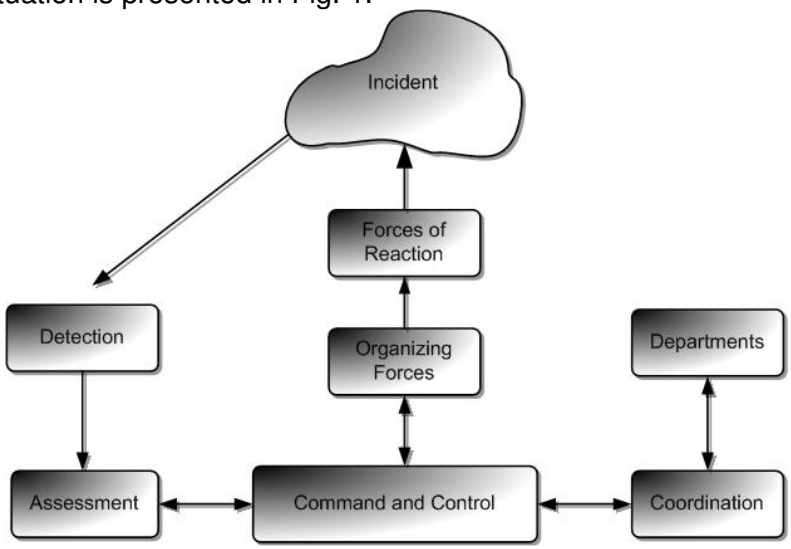


Fig. 1

To be practical and reliable the operation needs to achieve a high degree of realization of its goals, each such system must contain in itself the following key elements:

- Direct or Talk Around - This mode requires the ability to connect devices point to point, when outside the coverage area of their own radio network if for example the user is attending to an incident or threat or where the direct explicit requirement to work is outside the network;
- Push-to-Talk (PTT) - this is the mode for professional radio, which provides an opportunity for instant transmission of voice data or information at the touch of a button;
- Full Duplex - This mode is similar to the way public communication in cellular systems like GSM or public telephone exchanges Public Switched Telephone Network (PSTN). It is a characteristic that provides interoperability for the exchange of information as opposed to simplex or duplex modes which are specific for radio:
- Group call - this is a working method that provides transmission of information from one to many subscribers to the system or particular group, this is in a particular case of vital importance for the rapid assessment of the situation and timely implementation of the decision based on the need as assessed:
- Identification - a feature that allows participants to establish the operation at any time and communicate but the dispatchers control

access and give authorization or can prohibit the operation of individual subscribers into different groups or events;

- Emergency call or alarm - allows the manager or the manager of the operation to know that a client is in life-threatening situation that requires immediate intervention and provision of the highest priority;
- High quality service - a vital component of mission critical communication systems. The host country must understand that information obtained without repetition, and successfully identifies the calling party and is oriented in the nuances of the sound of the voice, which may contain additional information.

The main users of these services and similar systems are specific groups of subscribers whose activities require maximum efficiency and extremely precise coordination:

- security and defence;
- services such as responding to disasters,
- emergencies,
- emergency medical care including fire safety;
- NEC;
- forestry;
- public utility services;
- transport services.

Under the Radio Regulations (Radio Regulations) of the ITU (International Telecommunication Union) for the operation of such systems, these are allocated into several frequency bands in the range 30 MHz - 1 GHz, namely 40, 160, 390, 420, 450 and 860 MHz [1], [5].

In the Republic of Bulgaria because of the poor coordination between agencies, lack of a national strategy including funding problems we have built different professional radio action in specific situations, which can generally be classified as follows:

1. Conventional analogue systems with radial structure with solid attached radio channels with small density of subscribers manually switch operating position, divided into the following subtypes:

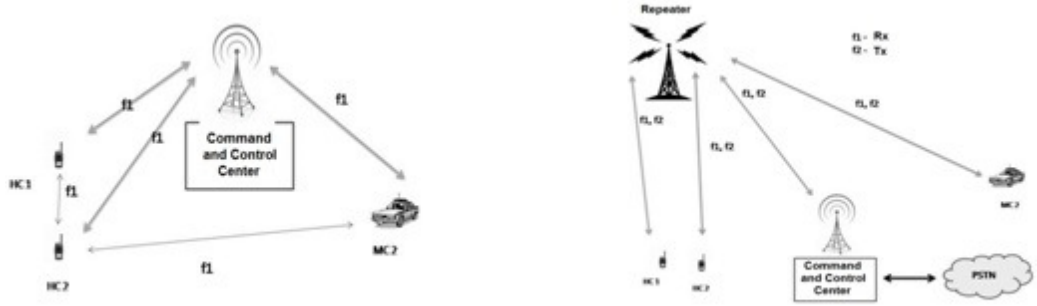
- local systems with short range without the use of a base station;
- dispatch based on simplex radios;
- dispatch based on repeater;
- complex multi zone dispatching systems.

2. Systems with distributed channels or trunked radio systems with high density of subscribers, automated management system and radial zone l structure:

- analogue (operating speech communication, status messages)
- digital integrated systems (operating speech communication, duplex wireless telephony, data transmission).

Building PMR VHF radio in Bulgaria began in the 60s of last century, mainly in the frequency ranges of 40 and 160 MHz [1]. The systems are more centralized in a regional basis, operating a simplex or a duplex frequency in simplex or duplex mode [4] - Fig. 2 a. and b.

Formation of one of the substations as dispatcher and installing its antenna height relative to other major sites (Fig. 2 a) allows for an area of up to 10 km to be realised and to connect to portable handsets and 20 to 50 km for mobile radio reception.



a) b)

Fig. 2

Thus creating the possibility of providing mobile to relatively large areas between subscribers and a control centre with stationary radio station operated by the dispatcher, which collects and distributes bi-relevant information. In addition, individual subscribers can communicate with each other within 2-7 km depending on the type of the used handset. Operating frequency is only one which is simplex therefore limited, i.e. alternating acceptance transmission by waiting for a free channel.

Particularly widespread, this system is mostly found in rural areas characterized by not very high density of construction, wherever respect the prevailing direction in point to multipoint and many of the subscribers have connections which are brief in content and duration. The number of subscribers served is up to 100.

Using repeater that receives signals from a subscriber station to a specific frequency and simultaneously retransmits it on to another frequency and so forth or other subscriber stations (Fig. 2 b), this allows to organize the connection of subscribers to each other, therefore the whole territory of the area is served. In this schematic of work the dispatcher station may be located anywhere in a separately managed station and a radio dispatcher to use a simple substation. This solution is the most flexible and therefore most widespread. Used by almost all users - power departments, fire departments, emergency medical care, large industrial sites, etc.

Recommended number of serviced subscribers up to 200.

Operating frequencies in this case are two, working in half-duplex mode - alternating reception / transmission like the simplex, at two different frequencies in order for the repeater to receive and transmit simultaneously.

A disadvantage of both the systems is that they are only particularly effective within the coverage area of the primary transmitter or repeater. If the event is classified as an emergency somewhere outside this area, the forces that have to react pass in the mode of direct communication, so in most cases there is no coordination between the centre and the units of the various agencies involved in the raid.

Since 1990, due to market liberalization and easing of the licensing regime in Bulgaria has allowed many foreign manufacturers of VHF equipment to enter the market, resulting in the emergence of many and various professional used radio systems that gradually cause problems in terms of EMC.

The practical solution is a long - build trunked systems (Fig. 3), which in addition to increasing the efficiency of spectrum it also allows the construction of radio networks with national coverage with the possibility of shared management of virtual subnets and coordination at various levels [4], [6].

Typical areas of application of trunked systems are the state, departmental and corporate organizations and institutions that involve communication security with multiple mobile users in densely populated areas. These are mainly the police and law enforcement bodies, fire safety, emergency medical services response to disasters and emergencies.

Lack of coordination between various agencies is the cause of different capacity and coverage of multiple analogue trunked networks, which essentially follow the old model of regional development and to fully solve the problems posed by changes resulting from internal and external factors.

In 1994 some concerned departments (departments of security, defence, health and civil protection) started working together in order to create a unified national system to meet modern criteria and be flexible enough for future growth and development, so that the system has a lifespan of at least 10 to 15 years. They set the estimated total number of subscribers, how to co-location, shared ownership, management separately and together and the specific responsibilities of each department.

Unfortunately, later a changed political situation did not allow the project to be financed. Each of the participants proceeded to build its own system, with the result that there are currently at least four different national systems on a technological level, with no connection between them.

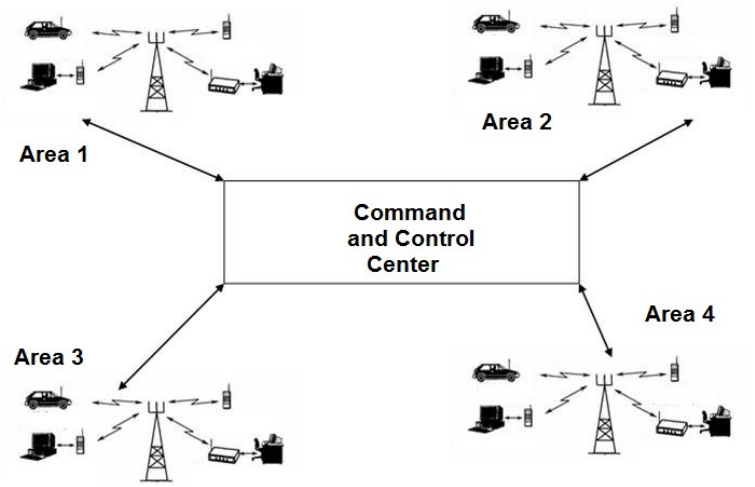


Fig. 3

As noted in the early modern requirements to mission critical communication systems, this is rejected as such an approach is not feasible, workable or sustainable. Therefore, building a modern system, based on the existing legacy need to be done:

- A phased replacement of analogue equipment with digital, given that current equipment is passed the stage of gradual migration and most are in the final replacement of the old type radios with newer, higher-tech versions;
- Focusing on high capacity centralized digital trunked TETRA networks such as in large cities, places with high traffic and boost passenger and their realization as in naturally more sequels then rarely populated areas of DMR systems and dPMR [2], [6]. Open standards such as TETRA, DMR and dPMR aim at creating a competitive environment, attracting a large amount of manufacturers of infrastructure, subscriber stations, measuring equipment for the production of compatible devices, which helps to reduce the amount of radio. On the other hand consumers choose open standards for radio fall depending on a single manufacturer and can choose equipment suppliers;
- Developing links between PMR and public and institutional PBXs, implementation of interfaces to cellular systems and switching to broadband PMR, will ensure the maintenance of high-speed data streams.

REFERENCES:

[1] Регулаторна политика за управление на радиочестотния спектър за граждански нужди [http://www.crc.bg /files/_bg/REGULATORNA_POLITIKA_29.04.08.pdf];
[2] Секторна политика в далекосъобщенията на Република България, [http://www.crc.bg/files/ _bg/rp4.htm];
[3] Cable&Wireless Worldwide, Mission Critical Communication, Annual Review 2009 /2010;
[4] Ketterling, Hans-Peter A., Introduction to digital professional mobile radio, Norwood, ARTECH HOUSE INC, 2004;
[5] Radio Regulations, ITU, Edition of 2008;
[6] Tait Communications, Tait White Paper Digital Trunked Radio US V1, [http://www.link-edin.com /redirect?url=http%3A%2F%2Fgo%2Etaitradio%2Ecom%2Frs%2Fdataratitait-ra-dio%2Fimages2FTait_White_Paper_Digital_Trunked_Radio_US_V1%2Epdf&urlhash =F4Eh&_t=tracking_disc]

Table of Contents

Volume 1 – Mathematics and Informatics

Table of Contents

Volume 2 – Computer Systems and Engineering

Table of Contents

Volume 3 – Physics and Technologies

Table of Contents

Volume 4 – Chemistry

Table of Contents

Volume 5 – Geography, Ecology and Environment Protection