Journal of Information Technology and Applications

(BANJA LUKA)

Exchange of Information and Knowledge in Research

VOLUME 3 NUMBER 1 BANJA LUKA, JUN 2013 (1-60) ISSN 2232-9625 (Print) UDC 004

APEIRON

THE AIM AND SCOPE
The aim and scope of the Journal of Information Technology and Applications (JITA) is:
• to provide international dissemination of contributions in field of Information Technology,
• to promote exchange of information and knowledge in research work and
• to explore the new developments and inventions related to the use of Information Technology towards the structuring of an Information Society.
JITA provides a medium for exchanging research results and achievements accomplished by the scientific community from academia and industry.

By the decision of the Ministry of Education and Culture of the Republic of Srpska, no.: 07.030-053-160-4/10 from 3/3/2010, the journal „Journal of Information Technology and Applications“ Banja Luka is registered in the Registry of public organs under the number 591.
Printed by Markos, Banja Luka in 300 copies two times a year.

Indexed in: LICENSE AGREEMENT, 3.22.12. **EBSCO** Publishing Inc., Current Abstracts

EBSCOHOST.COM
SCHOLAR.GOOGLE.COM
DOISRPSKA.NUB.RS
CROSSREF.ORG

Printed on acid-free paper

UDC 004

ISSN 2232-9625 (PRINT)
ISSN 2233-0194 (ONLINE)

JITA

VOLUME 3 NUMBER 1 BANJA LUKA, JUN 2013 (1-60)

CONTENTS

Dear Readers,

Welcome to the fifth issue of the JITA Journal

We are very pleased that the previous editions of this journal have aroused significant interest of the scientific and expert community, both in the country and abroad. This interest is, without doubt, the result of the quality of papers written by the members of prestigious scientific associations, university professors and eminent scientists and researchers.

In addition to well-known authors, whose names regularly appear in scientific journals, JITA also invites young and unestablished authors to submit their papers in which they will present the results of their research. As JITA is based on a strict selection of papers in the process of review, only quality papers will be accepted for publication in the journal.

The first paper is *The Impact of Quantum phenomena on complexity of communication system***,** by Aleksandar Stojanović. This paper puts emphasis on strategic issues in the transfer of information. The analysis is based on a fundamentally different structure between the classical and quantum information unit.

The second paper is *Web page characteristics of educational adaptive web sites*, by Željko Eremić and Dragica Radosav. The paper states that educational material can be placed on adaptive websites. Adaptive websites can customize their view and the structure on the basis of previously recorded user behavior.

The third paper is *Using Kerberos protocol for Single Sign-On in Identity Management Systems,* by Ivan Milenković, Olja Latinović and Dejan Simić. In this paper, various important aspects of the Single Sign-On functionality are revised. Special attention is given to the Kerberos protocol and its use in Identity Management Systems.

The fourth paper is *A Case Study on Introducing E-learning into Seafarers' Education*, by Sanja Bauk, Michael Kopp and Zoran Avramović. This paper considers beginning steps in introducing e-learning into seafarers' education, as additional mode of acquiring knowledge at the Faculty of Maritime Studies which is a part of the University of Montenegro.

The fifth paper titled *The innovation ICT strategy in agrifood sector*, by Luisa Sturiale and Alessandro Scuder, represents the analysis of ICT usage in agrifood industry in Italy.

The sixth paper is *Software simulations usage in business decision making education*, by Marko Marković and Katarina Plećić. The paper describes SAPO software system which uses broad-based algorithms which are expected to best assist students in their studies.

We thank the authors who have made a huge effort to prepare the papers in a quality manner, members of the review committee for their quality work and selfless engagement despite their many daily duties.

As editors, we recommend intensive communication between authors and readers, and we believe that, in this way, the usability of each presented paper will be increased.

We wish for authors that their papers are well received by the scientific and expert community. We will endeavor to increase the reputation and quality of the journal with each journal issue.

The Impact of Quantum Phenomena on the Complexity of Communication Systems

Aleksandar Stojanović

PhD student, Telecommunication Institute, Portugal, stojanovic.alex1@gmail.com

General survay

DOI: **10.7251/JIT1301005S** UDC: **004.056.55:004.087.5**

Abstract: This publication put the accent on strategical problems in information transmission. The analysis is based on substantially different structure between classical (bit) and quantum information unit (qubit). The scientific methodology used in this publication is relatively new (single qubit transfer based on no-cloning theorem). Important part of publication is devoted to solving problems where quantum information processing offers much more prolific solutions than classical information processing. From practical point of view, the advances of quantum based information technologies have been presented.

Keywords: quantum information, communication complexity, cryptography

Introduction

This publication is aimed to provide an outline of the current state of the quantum information technologies, as well as giving an insight into a possible direction of their further development. A quantum computer can be analyzed on the grounds of two completely different approaches:

1. by means of a model based on a family of quantum networks. [10]
2. by improving of the model of Turing machine.

Although the technical aspect was the most important in the delivery of this publication, its introductory part (i.e. the first three sections) deal with the essential changes the development of quantum algorithms have introduced into the mathematical theory of complexity. One should bear in mind that the greatest successes in the field of the quantum information processing came about by seeking quantum algorithms. At the same time, a new definition was thought of. Algorithm is computational method of the function which characterizes a given task [13].

The fourth section analyzes the quantum information from the point of view of finding an optimal code. By doing so, the results of the classical theory of information are used and new issues are pointed out, typical of quantum coding. The extent of the effects of applying quantum theory of information will heavily depend on how successfully these issues are solved.

The fifth section mirrors the dialectics in the development of technical systems – by combining two subsystems (RSA and BB84) a bi-system is created, which possesses a better average performance from its separate parts (which surprisingly enough, resembles the incidence of *'entanglement',* being the main resource of quantum cryptography).

Quantum crypto-analysis (still in its fledgling stage) is one of the main requirements for the physical realization of quantum computers.

Quantum Communication Complexi ty

The quantum communication model is based on the communication model of Yao[23]. This model

(the classical one) deals with the issue of communication by considering a situation in which two players *A, B* wish to evaluate a function *f(x, y)*. The input *x* is known only to *A*, and y is known only to *B*. In order to compute the function they have to communicate using some protocol. The resource in which the model is interested is the minimal amount of communication needed for this purpose [7]. In this context, it is necessary to mention Shanon's information theory, which also deals with the issue of transferring information and compare between the two models. Roughly speaking the main difference between this model and the well known Information theory of Shannon [19] is that information theory deals with the question of how to send messages (how to overcome problems of noise, bad links, etc.). The communication model on the other hand is concerned with the problem of what to send (i.e. design of protocols). The motive in construction of this model was the motivation to analyze computational models. This model has been proved to be successful in the area of computational complexity and many results were obtained by considering this model. Moreover, extensive research whose main subject was communication was conducted in the field of computer science. The reason for this is the importance of the abstract notions communication and information in computer science.

The quantum communication model deals with the information transfer in a quantum system. The model considers a quantum system divided into 3 parts *A, B and C,* where *A, B* are the parts which communicate via *C*. Similarly to the classical model, here is a situation in which some input *x* is coded in *A* and the other input y in *B*. The interest of this paper is the amount of information (communication) needed to be transferred by a quantum time evolution process until the value *f(x,y)* can be determined.

Motivation for this paper has been to show how quantum processes (which are more and more present from day to day) may influence complex (communication) systems (which already have enormous social importance and represent a scientific entity of our time).

Computational Complexity

Computational complexity is a mathematical branch of computer science which deals with the analysis of difficulties one comes up with in the calculation of functions. The purpose of the present section is to discuss various approaches used in solving problems in computational complexity. These differ in several aspects from those used in other areas of mathematics. For a more detailed discussion in this subject there is a good reference [16].

In order to investigate difficulties of computing certain function f it is necessary to specify some computational model which is a mathematical model (e.g. Turing machines, Boolean circuits). Having defined a particular model, 'algorithm' is the method of computing a desired function in this model. In the model, it is necessary to specify the various resources required in the computational process (the number of steps, memory requirements, etc.). These resources determine various measures of the "cost of the algorithm" which presents the central issue in computational complexity. The "cost of the algorithm" is normally calculated for the worst case situation ("worst input"). Most cases deal with Boolean functions $f: \{0, l\}^n \longrightarrow \{0,1\}$. It is assumed that f is defined for every *n*. It is of interest in the asymptotical behavior of the cost of the algorithm when $n \longrightarrow \infty$. The cost of the best possible algorithm [14] for a function ("cheapest" algorithm) defines the complexity of the function.

For every "computational model" a probabilistic variant can also be defined. This can be done in two ways which are equivalent:

1. Define a "random algorithm" as an algorithm which uses "random steps".
2. Define a "random algorithm" as constructing a probability distribution over deterministic algorithms.

The cost of the "randomized algorithm" or the reliability of the "randomized algorithm" in computing the function are measured by averaging over the random steps, or alternatively over the distribution of the algorithms. It should be marked that these results refer in most cases to the worst case input. Please note that no assumption is made regarding a specific distribution over inputs.

Complexity theory categorizes functions into classes according to their complexity. The aim is to find relations among different complexity classes. An important method in order to determine relations between two classes *A* and *B* is to find a complete function f (complete problem), which is a function of *A*, and to which it is possible to reduce every function *f* ' belonging to *A* (by reduction from *f* ' to *f* it is meant the transformation of a problem of computing *f'(x)* to a problem of computing *f(y)).*

Definition of the Model

Overview

In this section the model of quantum communication is defined.

The model of quantum communication deals with the complexity of the time evolution of many particle systems. It is based on the analysis of information transfer within the system [13]. For this purpose the system is divided into three parts: A, B and C. A and B are entities which communicate with each other. They correspond to Alice and Bob in Yao's model. Communication is transferred via C. This system is regarded as a model for computing Boolean functions $f: \{0,1\}^n X \{0,1\}^n \longrightarrow \{0,1\}$. The initial state of the system codes the input of the function: $x \in \{0, 1\}^n$ is coded in A and $y \in \{0, 1\}^n$ is coded in B. The final state codes the value of $f(x, y)$. The coding is done by the state of one of the particles (spinors). In terms of quantum mechanics, a random variable which can take the values from the set $\{0,1\}$ is obtained by measuring the state of the particle. The value of the random variable will be $f(x,y)$ with high probability. The process of computation (called the protocol) consists of a series of unitary transformations. Each unitary transformation can change either the state of the pair of components A, C or that of B, C. It is implied that there is no direct interaction between A and B. The amount of communication which is transferred is equal to the number of unitary transformations times the number of particles in C. This quantity is called the cost of the protocol. It is said that a protocol P computes the function f, if for every pair of values x, y the protocol changes the state of the system starting with a certain initial states coding x, y and ending in a final state coding $f(x, y)$. The quantum communication complexity of a function f is then defined as the minimal cost required in order protocol to compute f.

Quantum algorithm

As it has been already said, the model of Turing machine [8] does not seem to be the most appropriate to show how quantum processes work in computer science.

Therefore, the „quantum circuit" model is applied. The classical Boolean circuit is represented by Bull's elementary operations AND, OR and NOT which can simultaneously affect only one or two bits. They transform an incoming vector (represented by bits) into outcoming one (represented also by bits).

The „quantum circuit" is of a similar structure but, instead of Boolean operations it introduces elementary quantum operations - so called GATEs. A GATE is an operation over one or two qubits and it indirectly acts as an identity operator on other qubits of the quantum state.

Hadamar's transformation which copies the basic state $|b\rangle$ into $\frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^b |1\rangle\right)$. is an example of a single qubit GATE. In the form of matrix it is given as:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

An example of a two qubit GATE is a so called CNOT GATE which performs the following operation:

$$|c, b\rangle \rightarrow |c, b \oplus c\rangle$$

In the form of matrix it is given as:

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

It is known that the set of quantum logical operations (GATEs) containing CNOT and all single qubit quantum operations is universal. This means that any unitary operation can be written as a logical product of the set's elements.

The product of all elementary GATEs in a quantum circuit is a great unitary transformation which transfers an initial state into the state of the final superposition. The circuit outcome is the result of the measurements of certain parts of the system final state. It is said that the quantum circuit exactly calculates certain function f: $\{0, 1\}^n \rightarrow Z$ if it always determines the exact value of $f(x)$ for the given input x. The circuit calculates f with the final mistake if for each x gets exact $f(x)$ with a probability not less than $\frac{2}{3}$. It should be noted that quantum logic circuits could sustain only one measurement; more measurements would require additional memory, which illustrates TRADE OFF between the efficiency (complexity) of processor operation and the required amount of memory resources of the quantum computer. The complexity of the quantum logic circuits is usually measured by the number of elementary operations provided by the circuits.

A circuit is considered efficient if its complexity is, in the worst case, of the polynomial order for the set input lengths n. The brightest example of the efficiency of quantum circuits is Shore's algorithm [20] for factoring large integers.

Factorization (finding simple factors of a big number) illustrates so-called intractable problem of the following characteristics:

- The found solution is easily proven.
- Problem difficulty lies in discovering simple factors.

The point is, if p and q are large prime numbers, the product $n = pq$ is easily determined (number of elementary operations of bits is approximately of $\log_2 p \log_2 q$ size). However, it is difficult to find p and q for the given n.

The envisaged factorization time is of the super-polynominal order in relation to $\log(n)$. That means that, with the increase of n, the efficiency of the algorithm functioning is described by the function that has a faster growth rate than $\log(n)$. The best-known algorithm requires the following computer time:

$$time \approx exp[c(\ln n)^{1/3} (\ln \ln n)^{2/3}]$$

where c≈1.9. It is currently known that 65-digit factors of a 130- digit large number can be found within one month using a network of a hundred computers. Having this in mind, as well as the last formula, it can be estimated that the factorization of a 400-digit number would be completely out of reach of currently available computer networks.

The factorization problem is interesting from the aspect of the theory of complexity. For example, when referring to an intractable problem, it means the problem cannot be solved in computer time that is limited by the polynomial function of the input variable. In the case of this paper, that variable is $\log(n)$. This also is of practical importance since the scheme of public cryptography (e.g. RSA) is based on the assumed difficult factorisation of large whole numbers.

The importance of Shore's result lies in the fact that he pointed out the power of quantum computers that are capable of the factorisation in polynomial time. So, if a quantum computer capable of the factorisation of a 130-digit number during one month (which is unthinkable at the moment) was available, the use of Shor algorithm would enable factorisation of a 400-digit number in less than three years. On the basis of the fact mentioned, there is a clear insight into the direction and the extent of progress of complexity theory.

"Private quantum protocol" model

In a quantum communication model [14] Alice and Bob are holding quantum bits. The initial situation is when Alice has x, and Bob has y. The initial condition is simple $|x, y\rangle$. Let Alice start the game.

She can make a random unitary transformation over her qubits and send one or more of them to Bob. Sending quantum bits has no impact on the superposition, thus enabling Bob to apply this unitary

transformation on the received quantum bits. Each participant can measure their own qubits. At the end of the protocol the participans will have to say their values. The quantum protocol complexity is a number of quantum bits exchanged by the parties. It is said that the quantum protocol calculates $f:XxY\rightarrow\{0,1\}$ with the biggest error ε, if the likelihood that the protocol will determine the function $f(x,y)$ for each input (x,y) is at least 1-ε. The complexity of the best protocol (the lowest price) that computes f with the biggest error e is indicated as $Q_e(f)$.

"Public quantum protocol" model

An appropriate quantum protocol can be defined based on the analogy with the probability model, as in the case of the "private quantum protocol"(where analogy was also used) [14]. While, in the classical case, strings of classical bits are shared, in the quantum case, the parties share correlated quantum bits. For example, Alice and Bob share indefinitely many ERP pairs of quantum bits where Alice has the first qubit and Bob has the second qubit of one quantum pair. If Alice measures her part of the ERP pair, then both Alice and Bob look at the random string of bits. Therefore, this model represents generalisation of the"public protocol probabilistic model". The complexity of the communication of the public quantum protocol model is indicated as $Q_{\varepsilon}^{pub}(f)$.

Contrary to the classical case, the correlation between the public and private quantum protocol models has not been completely clarified.

Quantum Analogue of Huffman Coding

Quantum information is a natural generalization of classical information. The goal of this section is to find a quantum source coding scheme analogous to Huffman coding in the classical source coding theory [5] . Let us recapitulate the result of classical theory. Consider the simple example of a memoryless source that emits a sequence of inde-pendent, identically distributed signals each of which is chosen from a list $w_1, w_2,\ldots w_n$ with probabilities $p_1,p_2,\ldots,p_n$. The task of source coding is to store such signals with a minimal amount of resources. In classical information theory, resources are measured in bits. A standard coding scheme to use is the optimally efficient Huffman coding algorithm, which is a well-known lossless coding scheme for data compression. Apart from being highly efficient, it has the advantage of being instantaneous, *i.e.*, unlike block coding schemes the encoding and decoding of each signal can be done immediately. Note also that codewords of variable lengths are used to achieve efficiency. As it can be seen below, these two features—instantaneousness and variable length of Huffman coding are difficult to generalize to the quantum case. Now let us consider quantum information. In the quantum case, there is a quantum source which emits a time sequence of independent identically distributed pure-state quantum signals each of which is chosen from $|u_1\rangle,|u_2\rangle,\ldots|u_m\rangle$ with probabilities $q_1,q_2\ldots, q_m$, respectively. Notice that vectors are normalized *(i.e.*, unit vectors) but not necessarily orthogonal to each other. Classical coding theory can be regarded as a special case when the signals $|u_i\rangle$ are orthogonal. The goal of quantum source coding is to minimize the number of dimensions of the Hilbert space needed for almost lossless encoding of quantum signals, while maintaining a high fidelity between input and output. For a pure input state $|u_i\rangle$, the fidelity of the output density matrix ρ_i is defined as the probability for it to pass a yes/no test of being the state $|u_i\rangle$. Mathematically, it is given by $\langle u_i|\rho_i|u_i\rangle$ [12]. In particular, the paper is concerned with the average fidelity $F=\sum_i q_i\langle u_i|\rho_i|u_i\rangle$. It is convenient to measure the dimensionality of a Hilbert space in terms of the number of qubits (i.e. quantum bits) composing it; that is, the base-2 logarithm of the dimension. Though there has been some preliminary work on quantum Huffman coding [17], the most well-known quantum source coding scheme is a block coding scheme [12,17] . In block coding, if the signals are drawn from an ensemble with density matrix $\rho=\sum q_j|u_j\rangle\langle u_j|$, Schumacher coding, which is almost lossless, com-

presses N signals into $NS(\rho)$ qubits, where $S(\rho) = -tr\ \rho log \rho$ is the von Neumann entropy. To encode N signals sequentially, it requires $O(N^3)$ computational steps [5]. The encoding and decoding processes are far from instantaneous. Moreover, the lengths of all the codewords are the same.

Difficulties in a quantum generalization

A notable feature of quantum information is that measurement of it generally leads to disturbance. While measurement is a passive procedure in classical information theory, it is an integral part of the formalism of quantum mechanics and is an active process. Therefore, a big challenge in quantum coding is: How to encode and decode without disturbing the signals too much by the measurements involved? To illustrate the difficulties involved, a naive generalization of Huffman coding to the quantum case will be considered first. Consider the density matrix for each signal $\rho = \sum q_j \left|u_j\right\rangle\left\langle u_j\right|$ and diagonalize it into

$$\rho = \sum_i p_i \left|\phi_i\right\rangle\left\langle\phi_i\right| \qquad (1)$$

where $\left|\phi_i\right\rangle$ is an eigenstate and the eigenvalues p_i's are arranged in decreasing order.

Huffman coding of a corresponding classical source with the same probability distribution p_i's allows one to construct a one-to-one correspondence between Huffman codewords h_i and the eigen-states $\left|\phi_i\right\rangle$. Any input quantum state $\left|u_j\right\rangle$ may now be written as a sum over the complete set $\left|\phi_i\right\rangle$. Remarkably, this means that, for such a naive generalization of Huffman coding, the length of each signal is a quantum mechanical variable with its value in a superposition of the length eigenstates. It is not clear what this really means nor how to deal with such an object. If one performs a measurement on the length variable, the state-ment that measurements lead to disturbance means that irreversible changes to the N signals will be introduced which disastrously reduce the fidelity.

Therefore, to encode the signals faithfully, the sender and the receiver are forbidden to measure the length of each signal. The emphasis is on this difficulty—that the sender is ignorant of the length of the signals to be sent— is, in fact, very general. It appears in any distributed scheme of quantum computation. It is also highly analogous *to the synchronization problem in the execution of subroutines in a quantum computer: A q*uantum computer program runs various computational paths simultaneously. Different computational paths may take different numbers of computational steps. A quantum computer is, therefore, generally unsure whether a subroutine has been completed or not. There is no satisfactory resolution to those subtle issues in the general case. Of course, the sender can always avoid this problem by adding redundancies *(i.e.,* adding enough zeroes to the codewords to make them into a fixed length). However, such a prescription is highly inefficient and is self defeating for our purpose of efficient quantum coding. For this reason, such a prescription is rejected in this discussion. In the hope of saving resources, the natural next step to try is to stack the signals in line in a single tape during the transmission. To greatly simplify our discussion we shall suppose that the read/write head of the machine is quantum mechanical with its location given by an internal state of the machine (this head location could be thought of as being specified on a separate tape). But then the second problem arises. Assuming a fixed speed of transmission, the receiver can never be sure when a particular signal, say the sixth signal, arrives. This is because the total length of the signals up to that point (from the first to sixth signals) is a quantum mechanical variable (*i.e.*, it is in a superposition of many possible values). Therefore, Bob generally has a hard time in deciding when would be the correct instant to decode the sixth signal in an instantaneous quantum code.

Let us suppose that the above problem can be solved. For example, Bob may wait "long enough" before performing any measurements. We argue that there remains a third difficulty which is fatal for instantaneous quantum codes—that the head location of the encoder is entangled with the total length of the signals. If the decoder consumes the quantum signal (*i.e.,* performs measurements on the signals) before the encoding is completed, the record of the total length

of the signals in the encoder head will destroy quantum coherence. This decoherence effect is physically the same as a "which path" measurement that destroys the interference pattern in a double-slit experiment. One can also understand this effect simply by considering an example of N copies of a state $a|0\rangle + b|1\rangle$. It is easy to show that if the encoder couples an encoder head to the system and keeps a record of the total number of zeroes, the state of each signal will become impure. Consequently, the fidelity between the input and the output is rather poor.

Storage of quantum signals

Nevertheless, here will be shown that Huffman-coding inspired quantum schemes do exist for both storage and communication of quantum information. In this section, the problem of storage is considered. Notice that the above difficulties are due to the requirement of instantaneousness. This leads in a natural way to the question of storage of quantum information, where there is no need for instantaneous decoding in the first place. In this case, the decoding does not start until the whole encoding process is done. This immediately gets rid of the second (namely, when to decode) and third (namely, the record in the encoder head) problem mentioned in the last section. However, the first problem reappears in a new incarnation: The total length of say N signals is unknown and the encoder is not sure about the number of qubits that he should use. A solution to this problem is to use essentially the law of large numbers. If N is large, then asymptotically the length variable of the N signals has a probability amplitude concentrated in the subspace of values between $N\left(\bar{L}-\delta\right)$ and $N\left(\bar{L}+\delta\right)$ for any $\delta > 0$ [2,12,17]. Here $\bar{L}$ is the weighted average length of a Huffman codeword. One can, therefore, truncate the signal tape into one with a fixed length say $N\left(\bar{L}+\delta\right)$. ['0's can be padded to the end of the tape to make up the number, if necessary.] Of course, the whole tape is not of variable length anymore. Nonetheless, now it will be demonstrated that this tape can be a useful component of a new coding scheme—which we shall call quantum Huffman coding—that shares some of the advantages of Huffman coding over block coding. In particular, assuming that quantum gates can be applied in parallel, the encoding and decoding of quantum Huffman coding can be done efficiently. While a sequential implementation of quantum source block coding [2,12,17] for N signals requires $O(N^3)$ computational steps [5], a parallel implementation of quantum Huffman coding has only $O((\log N)^a)$ depth for some positive integer a. Now, our coding scheme for the storage of quantum signals will be desbribed. As before, we consider a quantum source emitting a sequence of independent identically distributed quantum signals with a density matrix for each signal shown in Eq. (1) where p_i's are the eigen-values. Considering Huffman coding for a classical source with probabilities p_i's allows one to construct a one-to-one correspondence between Huffman codewords h_i and the eigenstates $|\phi_i\rangle$. For parallel implementation, it is found useful to represent $|\phi_i\rangle$ by two pieces,[1] the first being the Huffman codeword, padded by the appropriate number of zeroes to make it into constant length,[2] $|0\cdots 0h_i\rangle$, the second being the length of the Huffman codeword, $|l_i\rangle$, where l_i = length(h_i). We also pad zeroes to the second piece so that it becomes of fixed length $\lceil \log l_{\max} \rceil$ where $l_{\max}$ is the length of the longest Huffman codeword. Therefore, $|\phi_i\rangle$ is mapped into $|0\cdots 0h_i\rangle|l_i\rangle$. Notice that the length of the second tape is $\lceil \log l_{\max} \rceil$ which is generally small compared to n. The usage of the second tape is a small price to pay for efficient parallel implementation. In this Section, the model of a quantum gate aggay for quantum computation is used. The complexity class **QNC** is the class of quantum computations that can be performed in polylogarithmic parallel depth. The well known fact that encoding or decoding of a quantum Huffman code for storage is in the com-

1 The second piece contains no new information. However, it is useful for a massively parallel implementation of the shifting operations, which is an important component in our construction.

2 The encoding process to be discussed below will allow us to reduce the total length needed for N signals.

plexity class **QNC**[18] will be used for the the results of the next subsection.

Communication

Now, the usage of the quantum Huffman coding for communication rather than for the storage of quantum signals is attempted. By communication, it is assumed that Alice receives the signals one by one from a source and is compelled to encode them one-by-one. As it will be shown below, the number of qubits required is slightly bigger, namely $N\left(\bar{L}+\delta+\left\lceil \log l_{\max}\right\rceil\right)+\left\lceil \log\left(Nl_{\max}\right)\right\rceil$. The code that will be constructed is not instantaneous, but Alice and Bob can pay a small penalty in stopping the transmission any time. In fact, there is the following:

Theorem 1: Sequential encoding and decoding of a quantum Huffman code for communication requires only $O(N^2(\log N)^a)$ computational steps.

The proof follows in the next three subsections.

Encoding

The encoding algorithm is done through alternating applications of the swap and shift operations.

$$|h_1\rangle|l_1\rangle|h_2\rangle|l_2\rangle\cdots|h_N\rangle|l_N\rangle|0\rangle_{tape}\otimes|0\rangle_{total\,length}$$

$$\xrightarrow{swap}|0\rangle|l_1\rangle|h_2\rangle|l_2\rangle\cdots|h_N\rangle|l_N\rangle|0\cdots0h_1\rangle_{tape}\otimes|0\rangle_{total\,length}$$

$$\xrightarrow{shift}|0\rangle|l_1\rangle|h_2\rangle|l_2\rangle\cdots|h_N\rangle|l_N\rangle|h_10\cdots0\rangle_{tape}\otimes|0\rangle_{total\,length}$$

$$\xrightarrow{add}|0\rangle|l_1\rangle|h_2\rangle|l_2\rangle\cdots|h_N\rangle|l_N\rangle|h_10\cdots0\rangle_{tape}\otimes|l_1\rangle_{total\,length}$$

$$\xrightarrow{swap}|0\rangle|l_1\rangle|0\rangle|l_2\rangle\cdots|h_N\rangle|l_N\rangle|h_10\cdots0h_2\rangle_{tape}\otimes|l_1\rangle_{total\,length}$$

$$\xrightarrow{shift}|0\rangle|l_1\rangle|0\rangle|l_2\rangle\cdots|h_N\rangle|l_N\rangle|h_1h_20\cdots0\rangle_{tape}\otimes|l_1\rangle_{total\,length}$$

$$\xrightarrow{add}|0\rangle|l_1\rangle|0\rangle|l_2\rangle\cdots|h_N\rangle|l_N\rangle|h_1h_20\cdots0\rangle_{tape}\otimes|l_1+l_2\rangle_{total\,length}$$

$$\cdots$$

$$\xrightarrow{shift}|0\rangle|l_1\rangle|0\rangle|l_2\rangle\cdots|0\rangle|l_N\rangle|h_1h_2\cdots h_N0\cdots0\rangle_{tape}\otimes|l_1+\cdots+l_{N-1}\rangle_{total\,length}$$

$$\xrightarrow{add}|0\rangle|l_1\rangle|0\rangle|l_2\rangle\cdots|0\rangle|l_N\rangle|h_1h_2\cdots h_N0\cdots0\rangle_{tape}\otimes|l_1+\cdots+l_N\rangle_{total\,length}$$

An ancillary space storing the total length of the codewords generated so far is included. This space requires $\log(Nl_{max})$ qubits.

Even though the encoding of signals themselves is done one-by-one, the shifting operation can be sped up by parallel computation. Indeed, as before, the required controlled-shifting operation can be performed in $O(\log N)$ depth. As before, if a sequential implementation is used instead, the complete encoding of one signal *stil* requires only $O(N(\log N)^a)$ gates. Now the encoding of the N signals in quantum communication is done sequentially, implying $O(N)$ applications of the shifting operation. Therefore, with a parallel implementation of the shifting operation, the whole process has depth $O(N(\log N)^a)$. With a sequential implementation, it takes $O(N^2(\log N)^a)$ steps.

Transmission

Notice that the message is written on the message tape from left to right. Moreover, starting from left to right, the state of each qubit once written remains unchanged throughout the encoding process. This decoupling effect suggests that rather than waiting for the completion of the whole encoding process, the sender, Alice, can start the transmission immediately after the encoding. For instance, after encoding the first r signals, Alice is absolutely sure that at least the first rl_{min} (where l_{min} is the minimal length of each codeword) qubits on the tape have already been written.

She is free to send those qubits to Bob immediately. There is no penalty for such a transmission because it is easy to see that the remaining encoding process requires no help from Bob at all. (Note that in the asymptotic limit of large r, after encoding r signals, Alice can even send $r\left(\overline{L}-\in\right)$ qubits for any $\in > 0$ to Bob without worrying about fidelity).

In addition, Alice can send the first r length variables l_1, ..., l_r, but she must retain the total-length variable for continued encoding. Since the total-length variable is entangled with each branch of the encoded state, decoding cannot be completed by Bob without use of this information. In other words, Alice must disentangle her system from the encoded message before decoding may be completed.

Decoding

With the length information of each signal and the received qubits, Bob can start the decoding process before the whole transmission is complete provided that he does not perform any measurement at this moment.

Problem of Quantum Key Distribution (QKD)

In the contemporary cryptography the essential problem is not how to hide the message, as it was in the past. The focus is how to protect (hide) the key. Key is secret information that is used to encrypt the message. After encryption, its result (ciphertext) is sent through the transmission media (communication channel). The encryption key should be (as much as possible) random, known only to communicating parties (Alice and Bob) and should be reused with frequency rate which is large enough for the required level of secrecy (that rate could be changed in real time, depending on communication scenario). That will give secret communication system (cryptosystem).

The one time pad (based on Vernam cipher) offers unconditional security [9]. The main drawback of this method is that all the parties exchanging secret information should be aware of a secret sequence of random numbers, i.e. a key, which is of the same length as the text to be encrypted and which is to be used only once. These keys are normally exchanged by physical means (for instance by way of a CD – Rom). By doing so, the security problem is created and difficulties may arise. Should this happen, a security problem is relocated from the message to the key and is known as the key distribution problem [3].

Since often there are no practical ways of distribution of large symmetric keys, majority of today's cryptographic protocols rely onto the public (asymmetric) distribution of keys . They could be seriously compromised (as it has been shown in the chapter 3) once the quantum computer is invented [20].

The system for quantum key distribution (QKD) may well sort out this problem. QKD technology enables an adequate regeneration of cryptographic keys and provides the proper way to secure key distribution between remote locations. In the figure 2 there is a diagram of the functioning of QKD system from one point to another, in which QKD system increases the seurity of useful information exchange. In this scenario, MagiQ-QPN [15] represents an additional hardware part used to generate and distribute the keys in a way the encryption of communication channel is performed. That additional hardware is given by optical fiber and truly random number generator.

The security performance (due to this fiber) achieved is significant and is approved with RoI (return on investment), since the additonal cost of fitting that fiber in current infrastructure is negligible comparing to potential losses and security problems that would arrise without the fiber.

On the other hand, truly random number generator (TRNG) is based on quantum logic, which is not compatible to the classical logic (on which is based pseudo-random number generator (PRG)). As an important consequence, the correlation between generated output bits from that TRNG will be ideal (zero), which is not possible with PRG generated bits. This is important for obtaining higher level of security.

The protection against breakage of the keys

Majority of the cryptosystems rarely reuse their cryptographic keys, very often less than once a year, which is the case with systems which require the physical exchange of keys (such as those using cryptographic boxes). The situation is even worse with symmetric cryptosystems that use private key (due to the impossible task of updating the keys and maintaining a number of these). It happens rarely that refreshment of cryptographic keys results in a higher rate of key expansion (the length of encrypted data/ the length of the key). That ratio should be as less as possible as far as the security is concerned. Even if the key is compromised (when the frequency of the key reusage is high) the quantity of information that the eavesdropper will get will be small.

On the other side, encryption protocols using public keys (asymmetric cryptography) require great computer power in order to achieve a considerable speed of the key generation. These protocols are going to be compromised with the advance in either mathematical algorithms or with the increase of computer power that can be exploited by an adversary.

When the key is endangered, the information which is transferred by way of communication link is vulnerable as long as the cryptographic key on that link is not regenerated. In systems in which the rate of reusage of the keys is very low (or zero), the decrypted key enables the eavesdropper (Eve) a complete access to the useful information.

The solution provided by MagiQ – QPN enables the continous refreshment of keys and by doing so the security of communication channel is improved in many ways. It should be strongly emphasised that the mentioned ratio between useful data and the corresponding key is not as large as in the case of symmetric cryptosystem. In this manner, the decrypted key in the system of MagiQ-QPN can be used to decode a small segment of information being exchanged, and thus the cryptographic key in the system is refreshed at least once per second, which is noticiable frequency of key reusage, due to the fact that this is the first commercial application ever of QKD. Not only does MagiQ-QPN provide protection against cryptographic external attacks, but it also improves the physical security of the system in terms of its internal cryptographic threats (i.e. man in the middle attack, which is current problem to QKD). This is achieved thanks to the fertile combination between classical (RSA or Vernam) and quantum cryptosystem QKD. In this symbiosis RSA can serve for the secret key exchange, QKD for solving the key distribution problem and Vernam for the encryption of useful message. As an alternative solution (which is more up-to-date) we can use quantum authentication of classical messages [1] to obtain fully QKD and after that to apply Vernam cipher. In that way, both problems of key-sharing and key establishment should be overcomed.

Secure key exchange

The security of quantum cryptography rests in the absolute potential of key exchange – quantum key distribution. By sending the key coded on the level of only one photon, quantum mechanics guarantees that if the eavesdropper intercepts the photon, he must perform the measurement on it (this is the only way for him to get the knowledge about unknown quantum state). This irreversibly changes the information coded on that particular photon and communicating parties are able to detect the eavesdropper. Therefore, the eavesdropper can neither copy that photon, nor he can read the encrypted information on it, without changing it (by no-cloning theorem (direct consequence of Heisenberg uncertainty principle and its qualitative meaning) and its experimental verification) [22] .

The encryption of data becomes indisputably secure by transsmition of quantum keys through optical fiber and truly random number generators.

For the first time, MagiQ-QPN [15] solves the problems of distribution and protection of keys, which has been implausible for centuries. The key formation in real time, which is offered by MagiQ-QPN, as well as the quantum distribution of these keys makes the cryptographic system the safest one up to now, offering the most economical key management. The useful information (encrypted message-ciphertext) can be transmitted through an optical fiber after the secret key has been established (us-

ing the same fiber). The key length and the frequency of the key reusage in this system could be adjusted to the optical channel band-width, so that communication system could support the higher useful data rate (we are sparing communication resources of the fiber and the whole communication system). Due to that fact, we obtain communication system with better average performance (better spectrum efficiency), comparing to the communication system which is not using mentioned Magic-QPN setup. Also, according to given definition of communication complexity (chapter2), our system is more efficient (we can, by using Magic QKD system easily obtain the same bit error rate (BER) as in the classical case with spending smaller number of communicating bits or bandwidth at the same time).

By using MagiQ-QPN, the two sides (Alice and Bob) communicate via photons (on physical level) which are generated, sent and detected independently. That method of information processing guarantees that an eavesdropper will be either left without information (if he wants to copy unkown quantum state) or will be uncovered by the eventually obtained partial information, (if he performs the measurement and disturbs the state which is unknown to him) . This will be described in more detail in the forthcoming chapters.

Once a secure distribution of keys has been established, one can use (indisputedly secure) code Vernam [9] which provides absolute security. This has a huge advantage as it eliminates the risk built in the systems based on the security of current commercial cryptographic solutions (which are based on the computational complexity and which have been proven to lose their security due to unpredicted development in hardware and algorithms).

Superposition

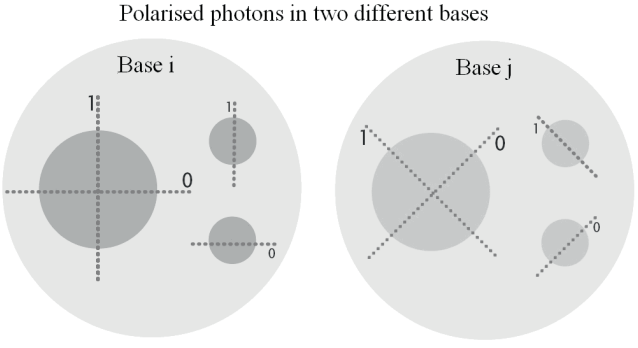
Classical information is encrypted in a binary (digital) form, i.e. in the form of zero and one, in electrical and optical systems. Quantum bit is unique as it encrypts two possible classical information states into a single coherent state of superposition. The formation of photon encoded qubits, or a coherent superposition of classical states is made possible by application of a number of techniques out of which all are mathematically equivalent. For instance, qubits can be formed by photon polarization, in time domain or in spacial domain. For QKD applications, the most enduring and most easily applicable photonic qubit transmission is in a time domain. An example of one QKD system which uses photon polarization for the encryption of qubits will be provided, since it can be applied very easily, and it provides a good insight into high level of security .

The encryption of photons

An optical channel requires a sender and a receiver (normally called Alice and Bob), and a fiber in which individually encrypted photons are transmitted. In this system, Alice can transmit photons in one of the two polarizational basis, which is shown in figure 1. Polarizational basis i encodes the photons to O degrees (which represents a binary zero, though this selection is debatable and Alice and Bob have to agree on it) and 90 degrees (which is a binary one). Polarizational basis j encodes the photons onto 45 degrees (which is a binary zero), and on 135 degrees (which is a binary one). The encoding is the matter of convention, previously established by Alice and Bob.

Alice uses a generator of random numbers (TRNG 1, figure 2) for making a random string of bits, with equal number of 0 and 1. Another generator of random numbers (TRNG2), is used to select the polarization basis (*i* or *j*) with the equal probability. After that individual photons encrypted in the appropriate way are sent through the fiber.

Figure 1. Polarization basis for encoding of photons in QKD systems



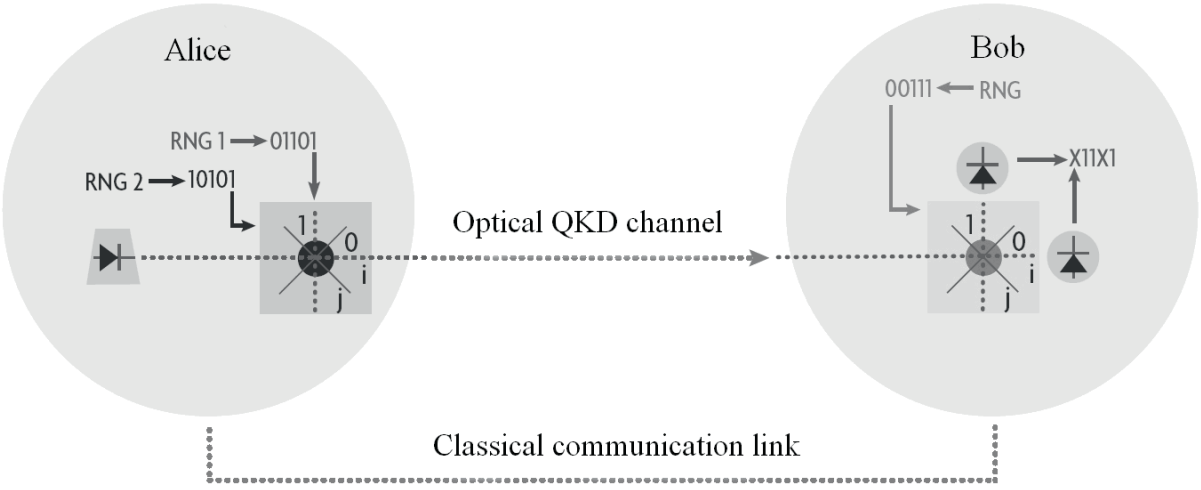
For instance, if the sequence of random numbers obtained by the generator RNG 1 = 01101, and the

sequence of random numbers obtained by the generator RNG 2 = 10101, then Alice sends five photons of the polarization as follows: 45, 90, 135,0 and 135 degrees by that order.

Photon detection

At the other end of the system, Bob receives the photons and measures their polarization. The receiver can be configured in a way that it differentiates polarization basis i and j as well as the appropriate photons polarized to 0 and 90 degrees (i base) and 45 and 135 degrees (j base).

Figure 2. Diagram of QKD system



As it is shown in figure 2, Bob uses a generator of random numbers and selects a base of reception (i or j). The laws of quantum mechanics dictate that Bob cannot properly measure the photons which are not adjusted according to the measurement base. For instance, if Alice sends the photons to the base i, and Bob has configured his receiver to measure the photons in the base j, then the receiver has equal chance to measure both 0 and 1 and the measurement result will be random. Bob then secretly saves the information about the received key and about the measurement base he used.

When the key transmission is finished, Bob reads which basis he has used to measure photons and uses classical (public) communication channel to announce it. Alice then communicates to Bob through the public channel to agree upon which corresponding basis are the same. Finally, Alice and Bob reject the bits measured in the opposite basis. That is statistically the half of the total number of transmitted (received) photons (bits), whereas the remaining bits which correpond to correct basis forms are the so called sifted key. After that, remaining steps are completely classical.

Error estimation

If sides are using a QKD protocol over a noisy channel, this situation turns into an advantage for an eavesdropper. Because at any time slot, if both sides use same type of filter for sending (reading) process and they do not have the same qubit value this can be due to not only existence of an eavesdropper but also to physical noise of transmission medium. This situation prepares a suitable environment for attacks on QKD systems over physical channel's noise.

To avoid such attacks, both sides determine an error threshold value "Rmax"(bit rate) when they are sure that there is no eavesdropping on transmission medium. Then after each QKD session, they compare (sacrifice) some bits of their raw keys in order to calculate a transmission error percentage "R". In that way, for R > Rmax case they can be sure about the existence of an eavesdropper and the protocol is restarted. It also must be stated that for QKD systems Rmax threshold value must be ideally chosen in a way that it is not smaller than the percentage of photons of which polarisations are spoiled due to transmission channel's or hardware's noise and not big enough to allow eavesdropping attempts [21]. An improper choice can lead to revelation of secret data or false alerts. This

ideal threshold value will keep on decreasing as physical noise of today's transmission lines and hardwares decreases and eventually it will be so hard to eavesdrop on QKD systems by hiding behind physical noise.

Key reconciliation

Even for R ≤ Rmax case, there can be erroneous bits in uncompared parts of keys. In this situation sides apply an error minimization step called "Key Reconciliation". This step includes these sub-steps:

1. Sending and receiving sides reorders their bit sequences by a common permutation function on which they agreed over public channel. In this way they distribute erroneous bits uniformly.
2. Bit sequences are divided into blocks of k bits. To reduce the possibility of more than one erroneous bit's existence in each block, k must be chosen ideally.
3. For each block, sending and receiving sides calculates a parity value and announces it. Last bit of each block of which parity value is annonunced, is deleted.
4. Both sides divide each matching block with different parity values into subblocks
5. and compare parity values of these sub-blocks in order to find erroneous bits [6]. This method is like "Binary Search". Last bit of each sub-block of which parity value is annonunced is also deleted.
6. There can be more than one erroneous bit in any block, for this reason first 4 sub-steps are reapplied by increasing k.
7. In order to detect remaining erroneous bits, both sides calculate the parity value of half of their bit sequences by announcing bit indices. If those values are *still* different then sides start "Binary Search" method in fourth substep again.

Privacy amplification

Privacy Amplification is the fourth step which is applied to minimize the number of bits that an eavesdropper knows in the final key [21]. Sending and receiving sides applies a shrinking method to their bit sequences in a way that eavesdropper can not apply properly to his/her bit sequence.

Let's assume that we have a bit sequence of *n* bits after application of first 3 steps. And also let's assume that eavesdropper knows m (m is a value derived from Rmax) bits of this final bit sequence. Then a number of *n-m-s* (s is a constantly chosen security parameter) sub-blocks is extracted from final bit sequence without revealing its contents and union of these subblocks's parity values form the final key. By this way number of bits that an eavesdropper may know is reduced to 2 – s / ln 2 and length of final key since start of QKD session is reduced to *n-m-s* bits.

Detection of eavesdroppers

One technique for performing attacks for Eve on the key between Alice and Bob is the use of transmitter and receiver similar to those which Alice and Bob use. Thus the interception is masked. When the eavesdropper Eve tries to intercept the message, it plants an error in the system, because it cannot know which base Alice will use for encrypting the photons [4]. In this scenario (figure 3), Eve detects the transmitted photons in the same way as Bob- by random choice of a measuring base. It uses also truly random number generator (TRNG). Even under very strong assumptions for Eve, (she has the same devices as Alice and Bob, has big computational power and the access to all critical points of the channel (excluding the emmision system from Alice and the detection system from Bob, which are the basic assumptions of quantum cryptography), Magic-QPN provides unconditional (information-theoretical) security, which is the strongest known type of secure communication [19].

Since Eve is forced to randomly select a basis, she will put an error into the transmitted photons. Alice and Bob verify the integrity of a quantum channel by detecting randomly chosen subset of the key and they check the rate of errors using a public communication channel. The presence of an eavesdropper is easily detected by uncovering the increase in the error rate by at least 25%. More information quantity Eve gains, it creates proportionally more disturbance. Therefore, the probability that Eve will be detected by Alice and Bob will be higher. This is true for any kind of attack (including entanglement-based attack).

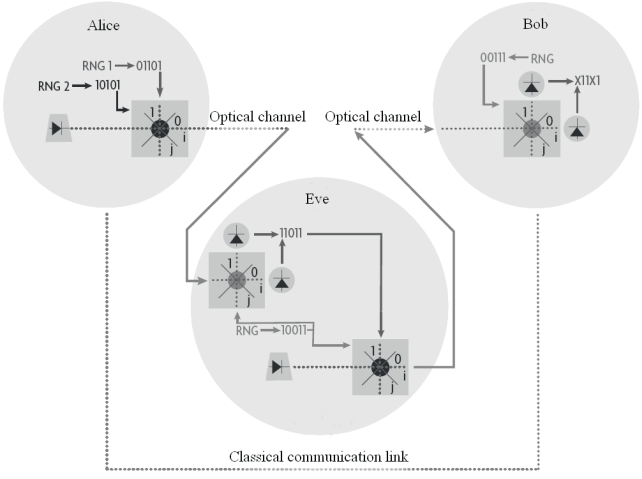
Beside eavesdropper, the main factor which contributes to bit losses in communication channel and to QBER at detection side is noise (in our case-optical). It is well established fact in quantum information theory

that (if the level of noise in the channel is reasonable) the noisy channel could be approximated with the noiseless (at the price of slightly higher BER). Noise has ambigous role in quantum cryptography. On one side, it is very frequent problem for Alice and Bob to discriminate between noise and the eavesdropper. This fact the eavesdropper can use to remain undetected. On the other side, noise prevents eavesdropper to read perfectly from noisy channel [1]. Beside that, noise can help key establishment phase (5.6.2. and 5.6.3.) in a way that it increases secret key space (the secret key rate).

Finally, it can be stated that mentioned Magic-QPN system satisfies all conditions for successful contemporary cryptosystems:

1. It is immune to any known mathematical algorithm
2. It has relatively high rate of key-reusage (integrity)
3. It is able to detect adversary with high probability, due to no-cloning theorem (availability)
4. The length of the secret key should be long enough comparing to the length of the message (confidentiality)
5. It will catch up with trends in technology (lack of perfect single-photon sources Magic-QPN compensates with the frequency of key reusage and its ability to perform error correction and privacy amplification in real time).

Figure 3. Diagram of Magic-QPN QKD system with the eavesdropper



Conclusion

The objectives of this paper are the following:

- Interpretation of the quantum theory of information,
- Description of a quantum coding scheme,
- Complete analysis of BB84 quantum protocol,
- Implementation of the complex communication system in real scenario.

Complexity is one of the main themes in information study and that makes the role of complexity theory important for research of information entities.

Quantum cryptography, which demonstrates the use of complexity, currently represents the greatest achievement of the quantum information technology. On the other hand, it is thought that the quantum information theory stands for the generalization of classical information theory, with significant improvements it has made in the areas of the current application of the information theory, and with applications in areas which are completely new for the classical theory of information.

This publication presents critical review of physical processes on which information technology of the future could be based. It explains the importance of complexity theory in telecommunication. Futhermore, this paper points out the advantages that quantum properties have over classical ones for information processing tasks [21]. The paper considered the way how to implement these advantages in existing telecommunication infrastructure, showing in illustrative manner the first commercial implementation of quantum key distribution [15].

This paper also ellaborates on several themes of analysis of information. The information structure of quantum information unit (qubit) is well introduced along with the introduction of quantum mechanics and with the statement of generalisation of problems from classical towards quantum information theory. Communication complexity is defined in inductive manner (through examples), with conclusion that quantum algorithms offer (for specific, narrow class of problems) exponential advantage comparing to classical algorithms. From the point of view of finding an optimal code, quantum Huffman code emerged as a natural choice, with significantly better complexity-theoretical bounds than corresponding classical. Finally, last chapter shows that combination between classical and quantum cryptosystem

provides higher level of security, keeping the same BER and obtaining higher bit rate for useful data at the price of adding only one optical fiber. Therefore, the publication has its contribution as a recommendation how the communication systems can improve both security and average performance (speed), at the price of negligible efficiency cost [21].

The information transmission methodology used in this paper is based on single-qubit transfer and no-cloning theorem [21].On the other side, actuall information technologies require enatnglement-based quantum cryptography. Therefore, there is a need for better laboratory conditions in our region, which would enable coherence between theoretical and experimental results and development of the prospective area of quantum cryptography.

Authorship statement

Author(s) confirms that the above named article is an original work, did not previously published or is currently under consideration for any other publication.

Conflicts of interest

We declare that we have no conflicts of interest.

References

[1] Assis, F., Stojanovic, A., Mateus, P. & et al. (2012). *"Improving classical authentication over quantum channel"* ISI journal Entropy.

[2] Barnum, H., Fuchs, C.A., Jozsa, R. & et al. (1996). *Phys. Rev.* A 54, 4707.

[3] Bennett, C.H. & Brassard, G. (1984). "*Quantum Cryptography: Public key distribution and coin tossing",* in Proceedings of the IEEE International Conference on Computers, Systems, and SignalProcessing ,Bangalore, p. 175.

[4] Bennet, C. & Brassard, G. (1989). *The dawn of a new era for quantum cryptography: the experimental prototype is working.*

[5] Cleve, R. & Divincenzo, D.P. (1996). *Phys. Rev.* A54, 2636.

[6] Cover, T.M. & Thomas, J.A. (1991). *Elements of Information Theory* (Wiley, New York).

[7] De Wolf, R. (2001). *Quantum Computing and Communication,* Complexity PhD thesis.

[8] Deutch, D. (1985). *Quantum theory, the church-turing principle and the universal quantum computer*.

[9] Kobayashi, H., Le Gall, F., Nishimura, H. & et al. (2010). *Perfect quantum network communication protocol based on classical network coding*, IEEE conference.

[10] Jozsa, R.J. (1994). Mod. Opt. 41, 2315.

[11] Jozsa, R. & Schumacher, B. (1994). J. Mod. Opt. 41, 2343.

[12] Kremer, I. (1995). *Quantum Communication,* Master Thesis.

[13] Kushilevitz, E. & Nisan, N. (1995). *Communication Complexity.*

[14] Magic Technologies. (2004). *Quantum Information Solutions for real world.*

[15] Papadimitriou, C., Dasgupta, S. & Vazirani, U. (2006). *Algorithms* McGraw-Hill, September.

[16] Schumacher, B. (1995). Phys. Rev. A51, 2738.

[17] Schumacher, B. (1994). Presentation at Santa Fe Institute.

[18] Shannon, C. (1948). Mathematical Theory of Communication. *Bell System Technical Journal.* 27 (3): 379–423.

[19] Shor, P.W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring" *Proc. 35th Annual Symposium on the Foundations of Computer Science*, p. 124 Edited by S. Goldwasser (IEEE Computer Society Press, Los Alamitos, CA.

[20] Stojanovic, A. (2009). The impact of quantum phenomena on complexity of communication systems MSc thesis, faculty of electrical engineering, Belgrade.

[21] Wootters, W.K. & Zurek, W.H. (1982). *Nature* 299 802.

[22] Yao, A.C.C. (1979). Some complexity questions related to distributive computing. In Proceedings of 11th ACM STOC, pages 209–213.

Internet source

[23] http://en.wikipedia.org/wiki/One-time_pad.

Submitted: November 19, 2012.
Accepted: May 16, 2013.

Web page characteristics of educational adaptive web sites

Željko Eremić[1], Dragica Radosav[2]

[1] *Technical College of Applied Sciences, Zrenjanin, Serbia, zeljko.eremic@gmail.com*

[2] *Technical Faculty "Mihajlo Pupin" Zrenjanin, University of Novi Sad, radosav@tfzr.uns.ac.rs*

Critical review

DOI: **10.7251/JIT1301020E** UDC: **004.738.12:[681.324:659.12**

Abstract: Educational information about single topic may be found on many different website pages. Those web pages may have different roles, such as the display of information related to teaching, teaching content or routing to other web pages. Educational material can be placed on adaptive websites. Adaptive websites can customize their view and the structure on the basis of previously recorded user behavior. Documents on which visitors often end their navigation are called target documents, and users often visit waypost documents before visiting the target documents. Characteristics of different types of documents are being investigated in this paperwork. Also guidelines related to the design of such educational web sites are being provided.

Key words: Adaptive website, Waypost, Web design.

Introduction

Information on the syllabus are most commonly found on websites of educational institutions. One topic (that, for example, refers to specific school subject) can often be placed on many web pages. While some of the web pages contain a large amount of text and images, and are able to attract the user's attention for a long time, there are web pages whose function is to direct users to other web pages. There are also web pages from which users are allowed to start their navigation more often than from any other web pages. It's It is essential to notice that there are user visits to different types of documents (web pages) in the user navigations.

Educational, and not only educational, websites can be implemented as adaptive web sites. Adaptive web sites adapt their display and structure in order to stand out from the competition with its efficiency and ability to meet the needs and expectations of customers. One way to significantly improve the navigation of these web sites is to use a shortcut or link. It makes sense to establish a connection among the documents that were not previously linked, and often occur together in the users' paths. In this way, a minimal impact is done on the layout of the pages and it therefore allows a considerable saving of time and effort of users who have a need for accessing useful information. Links are established to documents (files or pages) which are labeled with waypost status or the target document status. "Providing a link (i.e.,shortcut) between these potential wayposts could assist users by reducing the number of clicks they have to make while browsing, pointing them in the right direction towards a specific target document." [1]

Users have a motive for finding specific content, and their satisfaction is very important in this process. "Users' activities in a web site are motivated by the need to reach specific content. The result may be either successful – the user accessed specific document or not successful – the user failed to access specific document, gave up on further search and ended the session. Target documents are those documents

that user has been successfully reached depending on the requirements. Series of documents which have been visited make user's path." [7]

It should be noted that a document can have a waypost status in relation to one or more target documents, while it has no waypost status for other target documents. "If there are some documents which are often accessed in various paths (more often than in some other documents) before target document has been accessed, then those documents can be considered as some kind of road sign and they are candidates for a status of a waypost document." [7]

This paper is built on the results of previous researches. Different strategies to improve the navigation in the adaptive web sites are discussed in papers such as [10], [1], [2] and [4]. In the high percentage of cases, useful information about the users' previous behaviors are is taken from the log files, as described in [9]. On the other hand, there are alternative sources of information such as Page Tagging or cooperation of users described in [6]. In situations where it is necessary to gather more information about the behaviors of users it is possible to use the History Enriched Digital Objects described in [8] and [2].

The aim of this paper is to find a link between the use of specific HTML elements on web pages and the type of those web pages. Also it's it is essential to notice a correlation between the type of document and its size in bytes, and the average retention in this type of document. If the designer of the educational website has a clear idea as to what type of page his pages belong to then he can take into account the results of this study and use the appropriate HTML elements accordingly. In this way, web information related to education can be presented in a way that is suited to their purpose.

Method

The research presented in this article is based on information about past behaviors of the educational website visitors recorded in log files. The procedure of preprocessing of data from the log files consists of several steps and is quite standardized. One example of this procedure is given in Figure 1.

The goal of data preprocessing is to obtain a list of user sessions. A list of target documents is obtained from the list of user sessions. Two approaches are described in [1]. Next, extracting of user paths from user sessions is performed. User paths are extracted from the user sessions as extracting arrays of user visits which are ended on a document that was previously declared as target document. Similar user paths are grouped in the clustering process and waypost documents, that are often accessed before accessing the target documents, and are documents which are being searched for in such groups. An example of clustering procedure is illustrated in [5]. Based on the list of user's paths, target and waypost documents, it is possible to form lists of shortcuts that link documents (web pages and files).

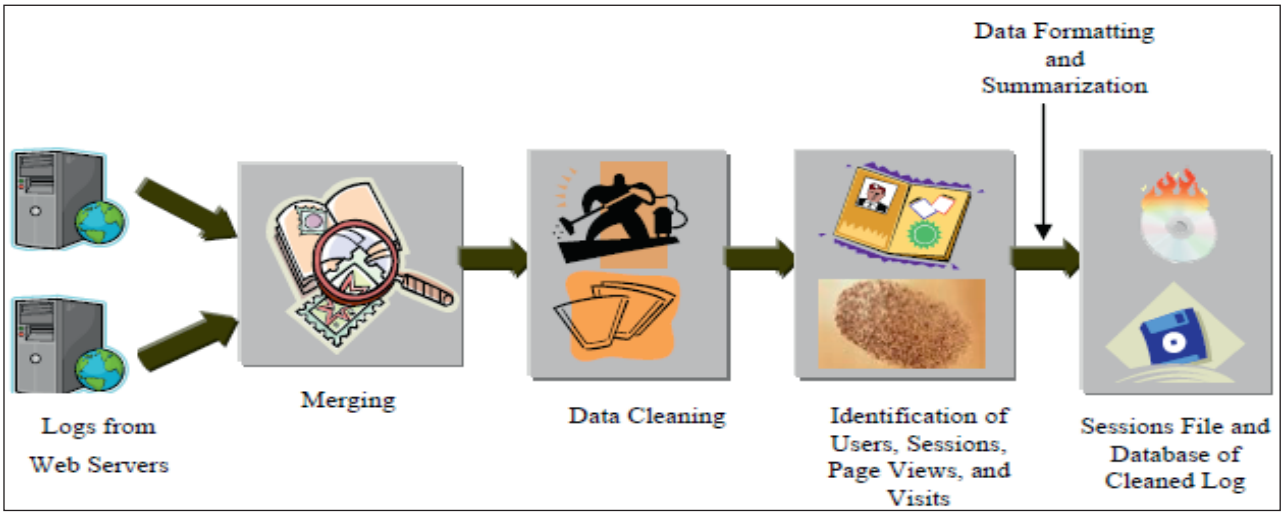
Target and waypost documents are calculated on the basis of their position in the user sessions, and on the basis of calculated duration of user visits. The question that is left open is related to what these documents contain? The computer does not have the ability to perform reasoning conclusions at the level of a human being, but on the other hand it has the ability to analyze large amounts of available information. In this article the focus will be on the specific use of certain HTML elements, which exist in various types of documents.

The analysis of the source code of website pages is performed by computer. This analysis counts those HTML elements that are relevant to this research. Documents are divided into those that are target documents and other (non-target documents). A type of accessed document is being determined for each user visit which belongs to any user paths. The survey is conducted on two levels:

- Documents – where all the web pages are being classified into two group of document types: target and non-target documents
- User visits – where all the user visits are being grouped on the basis of document type. Groups of user visits are as follows:
  - Normal (N)
  - Start (S)
  - End (E)
  - Waypost (W)
  - Target (T)

It should be noted that a single document (web page) may have a different type in different user paths. This rule is not applied only when a documents is a target document, because target documents have a "Target" type in each user path.

Figure 1: "Overview of data preprocessing in KDWUD" [10]



There are several characteristics that can be recorded on the document (web page) or during a visit to the document. The characteristics of the documents that are taken into account in this experiment are certain HTML tags which are contained in the document (web page), and its size is expressed in bytes. A characteristic that is observed at the level of the user visits to certain documents is duration of user visits.

The research should provide answers regarding the type of document and intensity of use of certain HTML elements. As a result, expected answer to the question which groups of documents use which HTML elements below average and above average is expected. It is also expected to compare the intensity of use of certain HTML elements between the different types of documents. Average size of the document in bytes and the length of the retention of certain document type are being compared as well.

Results

An experiment is conducted based on the log files and web pages of Technical College of Applied Sciences in Zrenjanin [12]. Log files are related to activities in the period from 1st June 2011 until 31st January 2012. These inputs are also used in the first experiment in [3]. A list of visited documents and a list of unique documents that exist on the website are is established.

User visits are grouped based on the types of documents listed in Table 1. For each unique document a number of following HTML elements which are described on the basis of [13] are being recorded:

- font – Defines font, color, and size for text
- p - Defines a paragraph
- td – Defines a cell in a table
- em - Defines emphasized text
- u - Defines underlined text
- ul – Defines an unordered list
- tr – Defines a row in a table
- b - Defines bold text
- table - Defines a table
- strong - Defines strong text
- ol – Defines an ordered list
- li – Defines a list item
- a - Defines an anchor
- img - Defines an image
- i – Defines italic text

Attribute "length" which represents the size in bytes of the document is also observed at the level of a single document. Duration of user visits expressed in seconds is observed at the level of user visits. The experiment was conducted on over a total of 351 web pages whose HTML code is analyzed, and over 202,220 tracked user visits to the documents where each user visit belongs to a certain user path. User visits are classified based on the types of visited documents (see Table 1).

Table 1: The Frequency Of User Visits, Grouped And Sorted By The Type Of Visited Documents

Document type	Frequency
Normal (N)	110163
Start (S)	52504
End (E)	25468
Waypost (W)	7570
Target (T)	7085

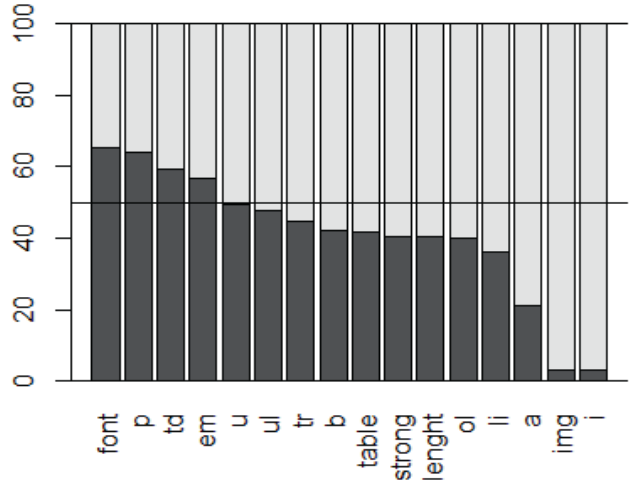
Documents (web pages) can be divided into those which are target documents and those which are non-target documents. There are 53 target web pages, while the remaining 298 web pages are non-target documents. The average value of the frequency of HTML elements is calculated from the analysis of the source code of these documents. The average length in bytes of these document types is calculated as well (see Table 2).

Table 2: Average Frequency Of Occurrence Of Observed Elements In Target And Non-Target Documents. The Average Length Of These Types Of Documents Are Given In Bytes

Document type	Target	Non Target
font	2,66	1,4
p	29,28	16,55
td	22,57	15,54
em	0,38	0,29
u	0,6	0,62
ul	0,55	0,6
tr	3,15	3,9
b	2,13	2,93
table	0,2	0,29
strong	6,04	8,85
lenght	3149,21	4628,37
ol	0,23	0,34
li	2,74	4,8
a	1,45	5,43
img	0,038	1,12
i	0,04	1,16

In Figure 2 there has been given a ratio of the average frequency of HTML attributes, and the size in bytes between the target and other documents. Target documents have frequent usage of HTML elements font, p, td, and em, while on average they use less the remaining elements, u, ul, tr, b, table, strong, length, oi, li. a img, i. The size in bytes of the target document is only 68% of the length of non-target documents

Figure 2: "Percentage Ratio Of The Average Frequency Of Html Attributes, And The Size In Bytes Between The Target And Non-Target Documents. Target Documents Are Given In Dark Gray Colour



The second part of the experiment is related to the level of user visits. Target documents remain the same when the user paths are considered. Actually user path in this study is considered to be a series of visits from the same IP address with the time difference between the two visits no more than 30 minutes, and which is ended by a visit to a target document. End document is a document which terminates user session, as defined in [1]. User path starts with start document and waypost document status is determined by the methodology given in [3]. Normal documents are all those documents that are not associated with any of these groups.

In Table 3 there have been given the average values of HTML elements appearing in each type of document. The average size in bytes of document types has been also given. In Table 4 there have has been given the same data, but expressed as a percentage and relative to other types of documents.

In Figure 3 there has been given the percentage of ratio of the frequency of HTML elements and the attribute "length", which refers to the size of web pages in bytes.

Average time of the users retention in certain documents can be seen at the level of the document type. In fact, users, on average, retain longest in the target documents (140.285522 seconds), and about the same in normal documents (63.328522 seconds) and

TABLE 3: THE AVERAGE VALUES OF THE FREQUENCY OF HTML ELEMENTS, AND THE SIZE OF DOCUMENTS GIVEN IN BYTES, GROUPED BY TYPES OF DOCUMENTS

	N	E	S	T	W
font	0,222724	0,152309	0,093230	0,893685	0,013606
p	69,543594	61,424026	105,945223	36,822043	61,781373
td	123,299755	88,114050	227,067499	30,875315	82,930118
em	0,054918	0,078398	0,033426	0,479678	0,074372
u	0,822662	1,116367	0,719297	0,363719	1,403830
ul	0,817806	1,114195	0,718478	0,345809	1,401453
tr	18,396376	14,496525	32,117095	5,149712	16,554557
b	10,451222	9,732553	13,031235	3,218828	9,860105
table	0,620725	0,595736	0,972173	0,444546	0,957199
strong	38,836605	35,722672	56,359705	8,141216	37,656406
lenght	14203,039523	14184,497357	18485,144008	4172,196785	15650,966050
ol	0,881666	1,087737	0,833612	0,274626	1,226816
li	11,400751	15,640147	7,224782	2,250975	15,530515
a	26,631654	27,265057	27,973087	1,502640	21,512549
img	0,209534	0,151042	0,170672	0,115958	0,038969
i	0,224185	0,162118	0,174101	0,115958	0,040554

TABLE 4: THE AVERAGE VALUES OF THE FREQUENCY OF HTML ELEMENTS AND THE SIZE OF DOCUMENTS GIVEN IN BYTES, GROUPED BY THE TYPES OF DOCUMENTS, EXPRESSED AS PERCENTAGE COMPARED TO THE VALUES FROM OTHER GROUPS

	N[%]	E[%]	S[%]	T[%]	W[%]
font	16,19158535	11,07256	6,777633	64,9691	0,989129
p	20,72733948	18,30732	31,57678	10,97474	18,41382
td	22,32531523	15,9544	41,11406	5,59045	15,01577
em	7,619118969	10,87665	4,637399	66,54874	10,31809
u	18,58755613	25,22365	16,25209	8,218013	31,7187
ul	18,59604738	25,33562	16,33743	7,863333	31,86757
tr	21,2149362	16,71758	37,03784	5,938714	19,09093
b	22,57578707	21,02338	28,1489	6,953022	21,29891
table	17,2885648	16,59257	27,07717	12,38159	26,66011
strong	21,97677192	20,21467	31,8927	4,606933	21,30892
lenght	21,2952393	21,26744	27,71559	6,255557	23,46618
ol	20,48262998	25,27002	19,36625	6,380038	28,50106
li	21,90465111	30,04995	13,88122	4,324875	29,83931
a	25,39129265	25,9952	26,67025	1,432655	20,51061
img	30,53652494	22,01217	24,87296	16,89919	5,679163
i	31,2707486	22,61325	24,28471	16,17456	5,65673

in the start documents (59.94747 seconds), while the lowest average retention of the documents is recorded in waypost documents (38.325 099 seconds).

Conclusions

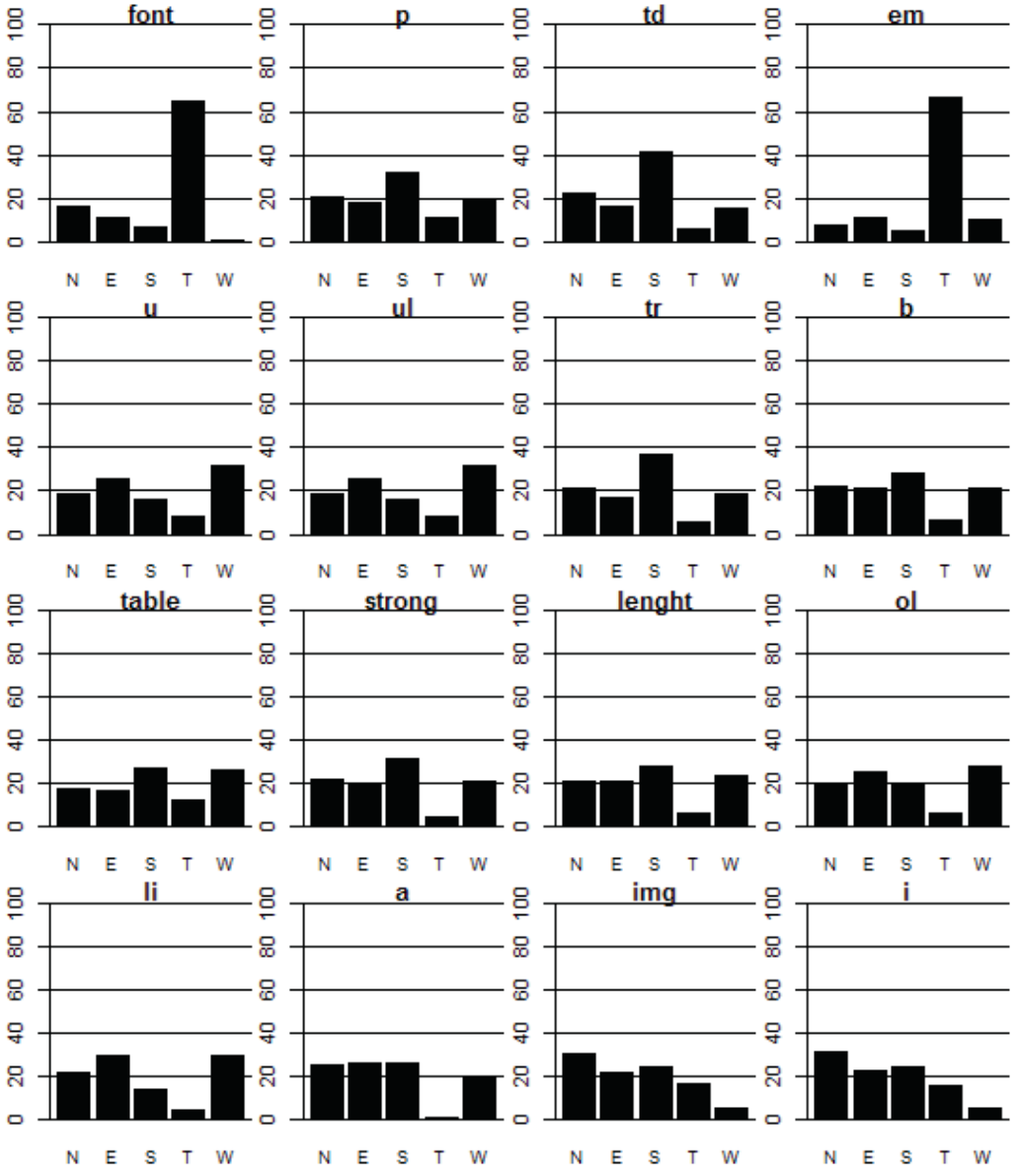
Study was conducted over an educational web site [12]. From the results of the research it is pos-

sible to make a number of conclusions. Target documents have frequent usage of the following HTML elements: font, p, td and em. The size in bytes of the target document is only 68% of the length of other documents.

The results can be observed at the level of user visits. Start documents extensively use HTML elements related to the table: tr and tb, and very rarely elements font and em. End documents also less commonly use HTML elements font and em. Waypost documents very rarely use HTML element font, i, im and relatively frequently HTML elements ul, ol, li. Target documents often use HTML attributes font and em while less than average HTML elements td, tr, u, b, string, ol, li, a. The remaining (Normal) documents less frequently use HTML element em. The size in bytes of the target documents is noticeably smaller than in other document types.

Users, on average, stay the longest in target documents around 140 seconds, and then more than double less in normal documents - around 63 seconds and in the start documents almost 60 seconds, while the least noticeable user retaining is in waypost documents around 38 seconds. Web designer of educational website could accept the suggestion that in the potential waypost pages does not there is no use of

FIGURE 3: "PERCENTAGE RATIO OF GROUP ELEMENTS WHEN HTML ATTRIBUTES ARE OBSERVED, AND ATTRIBUTE "LENGTH" (INDICATING THE WEB PAGE SIZE IN BYTES)



a specific font, italic letters and pictures which probably would not be loaded, because the user retaining time in these documents is the shortest on average.

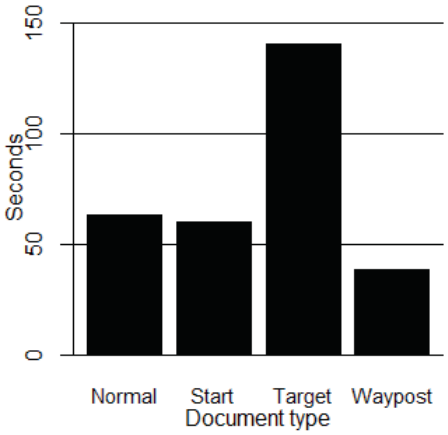


FIGURE 4: AVERAGE DURATION OF USER VISITS DEPENDING ON THE TYPE OF DOCUMENT

These conclusions are consistent with the assumptions in [1] and [3], where waypost documents are considered as signpost documents to the target documents. Considering that the waypost documents have noticeably more lists, those lists probably contain information about the possible target documents. At the same time it is logical that users do not retain too much in waypost documents because they have a tendency to find the desired information in the target pages. Also it is logical that users retain longer in the target documents as they need more time to read the information they are looking for and which they need and those that information are is often highlighted by using a different font. This paper is based on a set of input data used in [3], which refers to the educational organization website. Data are is transferred to appropriate form suitable for further processing. The results can be applied to the organization of educational content on web sites, but it can also be applied to other areas. This work is associated with web design because it suggests which HTML elements are to be used in which types of web pages. Research findings provide interesting recommendations for designers of educational web sites, when it comes to the use of HTML elements on web pages.

Authorship statement

Author(s) confirms that the above named article is an original work, did not previously published or is currently under consideration for any other publication.

Conflicts of interest

We declare that we have no conflicts of interest.

REFERENCES

[1] Bathumalai, G. (2008). Self adapting websites: mining user access logs. The Robert Gordon.

[2] Eremić, Ž. (2012). History-enriched digital objects as a factor of improvement of adaptive educational web site navigation. Journal of Information Technology and Applications, Banja Luka: 39-43.

[3] Eremić, Ž. (2012). Unapređenje navigacije adaptivnih veb sajtova korišćenjem log fajlova. Ph.D.Thesis, Technical faculty "Mihajlo Pupin", Zrenjanin.

[4] Eremić, Ž. & Radosav, D. (2011). Adaptive Web Sites in the Function of Information Access Improvement in Education. Information technology and development of education – ITRO 2011, Zrenjanin: 343-347.

[5] Eremić, Ž. & Radosav, D. (2012). Distances between clusters in the agglomerative hierarchical clustering of strings. Metalurgia International. No. 8, Vol.17: 67-74.

[6] Eremić, Ž. & Radosav, D. (2012). Collaborative user support as a contribution to navigation improvement of adaptive websites for distance learning. Information technology and development of education – ITRO 2012, Zrenjanin: 265-269. Eremić, Ž., Radosav, D. & Markoski, B. (2010). Mining User Access Logs to Optimize Navigational Structure of Adaptive Web Sites. Proceedings of the CINTI 2010 : 11th IEEE International Symposium on Computational Intelligence and Informatics, Budapest: 271-275.

[7] Hill, W. & Hollan, J. (1993). History-Enriched Digital Objects. Proceedings of Computers, Freedom: and Privacy (CFP'93).

[8] Pamnani, R. & Chawan, P. (2010). Web Usage Mining: A Research Area In Web Mining. Paper presented at the International Conference on Recent Trends in Computer Engineering ISCET 2010, Punjab, India: 73-77.

[9] Perkowitz, M. & Etzioni, O. (1997). Adaptive Sites: Automatically Learning from User Access Patterns. In Proc, 6th Int, World Wide Web Conf, Santa Clara, California.

[10] Raju, G. & Satyanarayana, P. (2008). Knowledge Discovery from Web Usage Data: Complete Preprocessing Methodology. IJCSNS International Journal of Computer Science and Network Security, Vol. 8: 179-186.

[11] Technical College of Applied Sciences in Zrenjanin. (2013). www.vts-zr.edu.rs

[12] W3Schools. (2013). http://www.w3schools.com/tags/default.asp.

Submitted: March 20, 2013.
Accepted: June 16, 2013.

Using Kerberos protocol for Single Sign-On in Identity Management Systems

Ivan Milenković, Olja Latinović, Dejan Simić

Faculty of Organizational Sciences, University of Belgrade, Belgrade, Republic of Serbia
ivan.milenkovic@fon.bg.ac.rs, olja.l@apeiron-uni.eu; dejan.simic@fon.bg.ac.rs

Critical review

DOI: **10.7251/JIT1301027M** UDC: **004.738.5:005.41**

Abstract: Today, identity management systems are widely used in different types of organizations, from academic and government institutions to large enterprises. An important feature of identity management systems is the Single Sign-On functionality. Single Sign-On allows users to authenticate once, and freely use all services and resources available to them afterwards. In this paper, we present the usage of Kerberos in identity management systems. An overview of Kerberos protocol, state of the art of identity management systems and different generic architectures for identity management is given in the paper. Also, we present a Single Sign-On identity management architecture proposal based on Kerberos protocol, and discuss its properties. Special attention was given to authentication, authorization and auditing.

Keywords: identity management, authentication, Kerberos, Single Sign-On.

Introduction

In modern corporate environment, identity management systems are of an utter importance. Today, many companies have hundreds or thousands of employees. With the advent of distributed systems, each user has accounts for several different applications, which are accessed remotely over the network [6]. These applications vary from webmail to inventory management, and may use various authentication methods. As the number of applications and users rises, the risk of attacks such as identity theft or identity disclosure also increases. Therefore, an appropriate set of policies, methods and rules must be applied [3].

Most applications require separate authentication, and do not provide means for centralized management. For example, let us consider a following scenario. To use several applications, user has to memorize separate password for each of the applications. This situation has several consequences. As first, the more passwords users have to memorize, the greater is the likelihood of using insecure passwords, which are easy for attackers to guess. Even strong password policies can be compromised by use of birthdays, personal id numbers or personal name derivatives. As second, the more passwords user has to memorize, the greater is the likelihood of forgetting some of them. For large enterprises, helpdesk expenses can raise to a significant amount. Moreover, users waste their time because they need to separately authenticate to each application.

In order to solve this problem, an identity management system should be used. Identity management system is responsible for different activities - identification, authentication, authorization, user provisioning and auditing [7]. Identification is the process of claiming user identity, while the process of verifying user identity is labeled as authentication. Some authors, like [13], refer to identification as a part of authentication process. User authentication methods can be divided in three categories - password based authentication, use of digital certificates or tokens and biometric based authen-

tication. Password based authentication methods use something that user knows, tokens are based on something that user poses, while biometric authentication uses person's physiological or behavioral characteristic - something that user is. Authorization is the process of asserting user rights to access resources or services. User provisioning is correlated with authorization, as it manages user authorization privileges to be consistent with user role in the enterprise. The last, but not the least important activity is user auditing, the activity of tracking and logging system events.

Another advantage of using identity management system is the Single Sign-On (SSO) functionality. Single Sign-On allows users to authenticate only once, and freely use all services and resources available to them afterwards. In that way, users have to manage only one set of authentication credentials in order to access SSO-enabled services and resources [12]. Single Sign-On authentication has several benefits, such as increased security and usability. Problematical scenario described before in this section can be solved by the use of SSO.

A possible implementation of Single Sign-On functionality can be achieved by the use of Kerberos protocol. This paper will present a SSO architecture based on the Kerberos protocol. In the next section problem statement is given, and main reasons for the use of Single Sign-On are given. In section 3 a description of the Kerberos protocol is given. Section 4 describes state of the art of both of brand-name and open source identity management systems. Section 5 describes generic Single Sign-On architectures for identity management. In section 6, an architecture proposal is given. The last section summarizes our conclusions and gives recommendations for future work.

Problem definition

In this paper the problem of Single Sign-On, primarily for corporate environment, is considered. There are several reasons for using the Single Sign-On functionality. Possible benefits gained by the use of Single Sign-On can be substantial.

As the number of applications per system user increases, it gets more difficult to manage authentication credentials. In the case of password based authentication, users have to memorize password they use for each application. This is a possible threat for system overall security, as some of the users may choose passwords that are easy to guess [4]. Another downside of this approach is the increased number of help desk calls because of forgotten passwords. It is estimated that an average help desk call costs about US$25 [10].

Each time system user has to authenticate to a service, the login process consumes some time. Although this fact may seem of a minor significance, if there is a large number of authentication requests, total time consumed may sum up to a significant amount. Unsuccessful authentication attempts because of improperly entered credentials can additionally extend this waste of time and productivity. User experience also suffers from a large number of required login attempts. If the authentication and authorization process is more convenient, then users will be more inclined to use available applications and services more frequently.

Single Sign-On is also tightly connected with user provisioning and authorization. The use of the SSO functionality allows easier maintenance of user accounts and privileges. However, when implementing Single Sign-On functionality, it is necessary to take special care of security of authentication credentials. If these credentials are compromised, potential imposter gains access to a wide range of system applications and services. Also, mutual authentication needs to be implemented [2], in order to prevent spoofing attacks. In following sections of this paper, an SSO architecture proposal based on the Kerberos protocol will be presented. The main goal of the proposed architecture will be to address these issues.

Kerberos protocol

Kerberos was developed at MIT under the Project Athena and became the most widely deployed system for authentication and authorization in modern computer networks. The first three versions were used internally at MIT. The primary designers of Kerberos version 4 are Steve Miller and Clifford Neuman [11]. They published that version in the late 1980. Version 5 was designed by John Kohl and Clifford Neuman

in 1993 and finally MIT made an implementation of Kerberos freely available. Kerberos uses symmetric-key cryptography (system where both the client and the server share a common key that is used to encrypt and decrypt network communication) to authenticate users to network services [8].

Kerberos authentication protocol offers the possibility of reliable authentication over an open network. It provides a mechanism for authentication - and mutual authentication - between a client and a server, or between two different servers. Kerberos protocol uses specially formatted data packets, which are known as tickets where they pass through the network instead of passwords. Kerberos messages are encrypted with encryption keys to ensure that no one can tamper with the client's ticket or with other data in a Kerberos message.

Kerberos authentication process is conducted like this: The client sends a request to the authentication server (AS) for "credentials" for the server. The result is a coded key for the client. Credentials consist of a "ticket" for the server and a temporary encryption key ("session key"). The client transmits the ticket to the server. The session key is used to authenticate the client and may optionally be used to authenticate the server.

If the client machine can decrypt the ticket encrypted in user password, then it is considered that the user is authenticated. If a target service is able to decrypt an encrypted ticket using its own secret key, the service may presume that the user who presented the ticket is authentic. The main benefit of such protocol architecture is that no system or party in the Kerberos exchange has access to sufficient information to impersonate any other system or party. There is no password passing through the open network.

Authorization model is based on the principle that every service knows the user, so that each one can maintain its own authorization information. In fact, the Kerberos Authentication System can be expanded by information and algorithms that can be used for authorization.

Protocol implementation requires that one or more authentication servers run on physically secure hosts. The authentication servers maintain a database of principals and their secret keys. Code libraries provide encryption and implement the Kerberos protocol. Typical network application calls the Kerberos library directly or through the Generic Security Services Application Programming Interface.

Figure 1 is a description of the Kerberos protocol, which looks like this:

1. The client must first contact an authentication server (AS) to receive a ticket and an encryption key.
2. Client receives a ticket granting ticket (TGT) and an encryption key. The encryption key, called the session key, is used to unlock communication between the client and the server and thereby authenticate that communication.
3. Client requests a service ticket from the Kerberos server. Service ticket includes ticket-granting ticket obtained from the previous message and an authenticator generated by the client and encrypted with the session key. When the client wants to access a particular service, it sends the ticket to a ticket-granting server (TGS).
4. The TGS gives the client a ticket that securely identifies the client to the requested service
5. The client presents the ticket to the network service it is trying to access and is granted access to the resource as many times as desired until the ticket expires.
6. Access is authorized and gives to the client prove it really is the server the client is expecting. This packet is not always requested. The client requests the server for it only when mutual authentication is necessary.

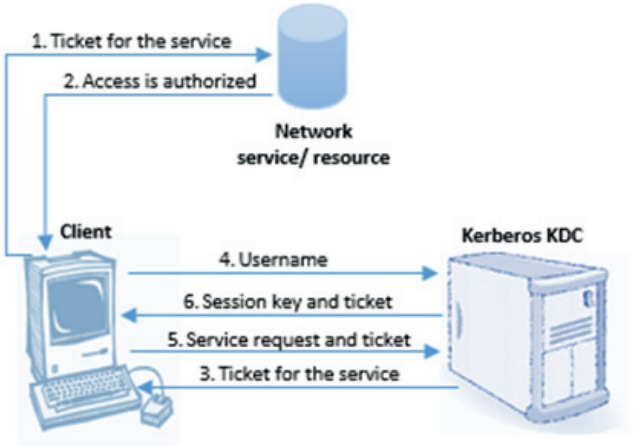


Figure 1 Kerberos protocol

Ticket-granting ticket (TGT) is the ticket for the full ticket-granting service. TGT presents credential in the form of an authenticator message and a ticket. It is a small amount of encrypted data that is issued by a server in the Kerberos authentication model to begin the authentication process.

Identity Management - state of the art

Identity management has grown up over the years. Critical issue around the world is how to achieve effective identity management. Most identity management systems are designed for a narrowly defined set of goals. There are many different vendors of proprietary identity management systems and open-source solutions, and their solutions offer various benefits. Today's available technology is good, but there is still room for improvements, in order to achieve better privacy protection and security.

Identity management solutions from Microsoft offer: Efficient and secure delivery of e-services, seamless user experience across boundaries, simplified management, application development efficiency and Single Sign-On (SSO) experience across borders, platforms, and various authentication methods. Microsoft account enables users to log into many websites using one account.

Hewlett Packard provides a single, unified technology platform which offers the movement of biometric information from the device to the database, from the edge to the enterprise. HP's identity management solutions incorporate identity lifecycle management, federation services, directory management and access management, with reporting and auditing services. HP IceWall SSO is Web Single Sign-On software of Hewlett Packard Company.

IBM's Identity management solutions allow operative management of the entire identity lifecycle: assessing, planning, implementing, auditing, monitoring and maintaining identities and access privileges. Among SSO solutions provided by IBM, the most relevant representative is the IBM Tivoli identity management [1]. It provides the ability to combine Single Sign-On, strong authentication and audit tracking without change of the existing infrastructure.

OpenIAM is an open source identity management solution. There are two types of products: Identity Manager (Password Management, Provisioning, Audit and Compliance, Self-Service, Delegated Admin) and Access Manager (RBAC, XACML, Federation and SSO, Web Access Control, SOA Security).

Yale University created an authentication system which is called Central Authentication Service (CAS). Since 2004, CAS is a member of Java Architectures Special Interest Group. Formerly called "Yale CAS", CAS is now also known as "Jasig CAS". When a client wants to authenticate, the application redirects to the CAS, which confirms the authenticity, and checks your username and password in the database (such as Kerberos).

In 2000, MACE working group started Shibboleth project which solved problems in sharing resources between organizations with often wildly different authentication and authorization infrastructures. This project created an architecture and open-source implementation for Identity management and federated identity-based authentication and authorization infrastructure based on Security Assertion Markup Language (SAML).

Another open-source project is FreeIPA by Red Hat which combines Linux (Fedora), 389 Directory Server, MIT Kerberos for authentication and Single Sign-On, NTP, DNS, Dogtag (Certificate System). It consists of a web interface and command-line administration tools. FreeIPA can be used for managing DNS domains, defining password policies and for integration with NIS domains and netgroups.

Generic identity management architectures for Single Sign-On

Single Sign-on functionality largely depends on system architecture. For example federated identity management has some additional requirements, when compared to centralized identity management. In this section, the main elements of identity management systems are described by using block diagrams. However, before we can describe different architectures, it is necessary to define basic components present in every generic architecture.

System user is a consumer of services provided by the system. User must own at least one identity in order to use available services within a context defined by owned identity. To confirm the claimed identity, system user communicates with identity provider. Identity provider is responsible for accepting or denying users identity, but it is also strongly tied with service provider. This way identity provider confirms or propagates identity information to service provider. Depending on the information received from identity provider, service provider allows or rejects usage of requested services.

A traditional approach to identity management is the Centralized identity management system architecture [5]. In this case a centralized identity provider and all system services are provided by a single service provider. This architecture is shown in Figure 2, and process steps are numbered. In Step 1, system user identifies himself to identity provider. After a successful identification of the system user, the system needs to authenticate the user. Identity provider is responsible for both identification, and authentication. After completion of authentication, user receives a token from identity provider (Step 2), which is passed to the service provider in Step 3. Token is valid for a certain amount of time, and users do not need to authenticate each time they send request to the service provider. Therefore, SSO requirements have been met.

Token is used by the service provider to verify user credentials and claims. This is done in Steps 4 and 5, where identity provider and service provider communicate in order to validate information carried by the token. After a successful validation, system user is eligible to use desired services (Step 6).

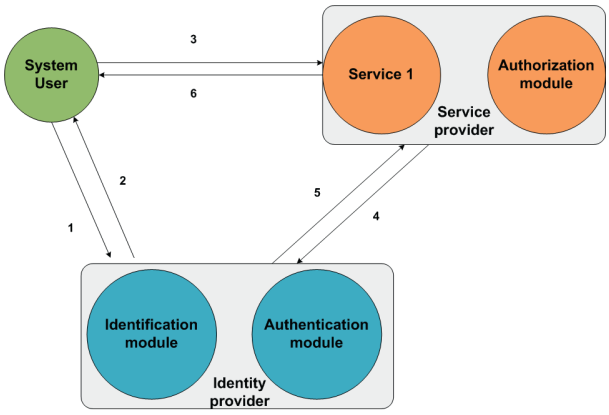


Figure 2 - Centralized identity management system architecture

In this architecture, service provider is responsible for authentication. It is important to notice that all identity management architectures described in this paper follow previously described steps.

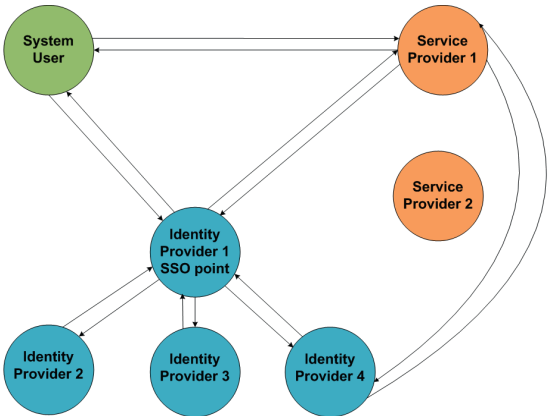


Figure 3 - Centralized SSO architecture with independent identity providers

In an alternative scenario, there is a centralized identity provider which represents a Single Sign-On point. Beneath it, on the lower level, there are numerous service specific identity providers. System user identifies and authenticates with centralized identity provider, while authorization process is delegated to service specific identity provider. It is important to highlight that centralized identity provider does not care about authorization, nor its data. After initial sign on, user only needs to authorize with service specific identity provider in order to get access to a desired service.

Next identity management architecture exploits the fact that multiple identity providers could share information they have. By sharing the information and agreeing to work together, identity providers form a "federation", thus allowing system users to identify with any identity provider belonging to the federation. Because of that, this architecture is called Federated identity management architecture [14]. The main advantage of the Federated identity management architecture is that it enables system to work even if the service provider and identification provider are not in the same organization. The Federated identity management architecture is shown in Figure 4.

Kerberos authentication - Architecture proposal

Among described architectures, Kerberos is most suitable for the use in centralized SSO architectures

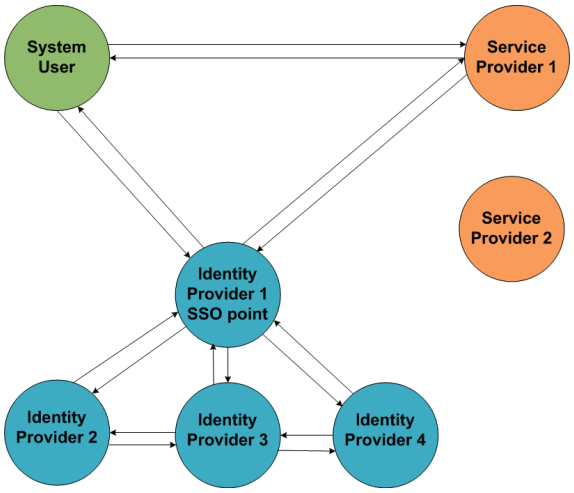


Figure 4 - Federated identity management architecture

with independent identity providers responsible for authentication. We propose the usage of Kerberos as identification and authentication module, as there are several benefits from such choice.

As first, system user authenticates with the Kerberos authentication server and receives ticket granting ticket and session key. When authenticating to service providers, system user requests service tickets from Kerberos ticket granting server. System user uses service tickets to authenticate with service providers. Independent identity providers are used for authorization. Different solutions could be used for storing authorization data, for example an LDAP directory. For example, Free IPA uses 389 Directory

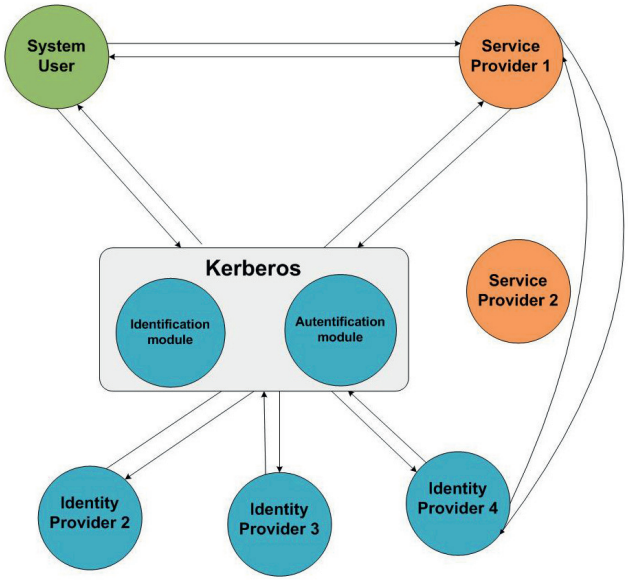


Figure 5 - Centralized SSO - Kerberos authentication

service for this purpose. Various extensions of this architecture are possible, such as the use of Security Assertion Markup Language, an XML-based open standard data format for exchanging authentication and authorization data between parties.

Architecture allows use of different authentication methods. PKI (Public Key Infrastructure) can be used for initial, or cross realm authentication [15]. Use of PKI infrastructure allows easier administration of Kerberos key distribution center, revocation of certificates, and various other benefits. Kerberos provides mutual authentication, which makes phishing and man in the middle attacks difficult and not likely to succeed. Ticket system provides safe communication through open network, as system users do not have to send unencrypted passwords.

Kerberos offers flexibility with forwardable, renewable and proxiable tickets [9]. Identity theft risks can be lowered by the use of renewable tickets. At each renewal, Kerberos KDC can check if the ticket was compromised. Proxiable tickets allow services to do task on behalf of system users, while forwardable tickets allow complete use of client's identity.

Kerberos does not provide authorization functions or auditing functions. Therefore, it is necessary to use other tools and applications for this task. In a workstation environment, one of the Kerberos weaknesses is a Spoofing Login where intruder very simple can replace the login command with a version that records users' passwords before employing them in the Kerberos dialog. Also, each network service with a different hostname will need its own set of Kerberos keys. This complicates virtual hosting and clusters.

Conclusions

In this paper, various important aspects of the Single Sign-On functionality are revised. Special attention is given to the Kerberos protocol and its use in identity management systems. Several generic Single Sign-On architectures are presented, and an architecture proposal based on the Kerberos protocol is described.

Centralized Single Sign-On architecture based on

the Kerberos protocol offers various benefits. Secure mutual authentication, various authentication methods, real-world interoperability, possible integration with PKI are just some among many. Kerberos has been widely used by both academic and enterprise organizations for many different tasks. Therefore, Kerberos use is not limited only to centralized identity management. Federated SSO architecture could benefit from the use of Kerberos as well. Cross realm authentication allows user of one Kerberos realm (administrative domain) to access services from other realms. This functionality is based on sharing keys, so it has some limitations, although these restrictions can be stretched by using transitive trust relationships. Another approach for federation is based on the use of PKI.

Primary objective of this paper was not a detailed analysis of Kerberos integration with other solutions for authorization and auditing. Such analysis should be done in future research. Future work could also include a comparison of Kerberos with possible authentication alternatives, such as Distributed Computing Environment (DCE). Moreover, challenges concerned with the use of biometric authentication in Kerberos are an important problem, and should be investigated.

Acknowledgment

This work is a part of the project Multimodal biometry in identity management, funded by Ministry of Education and Science of Serbia, contract number TR-32013.

Authorship statement

Author(s) confirms that the above named article is an original work, did not previously published or is currently under consideration for any other publication.

Conflicts of interest

We declare that we have no conflicts of interest.

References

[1] Buecker, A. et al. (2008). Integrated Identity and Access Management Architectural Patterns, Retrieved from http://www.redbooks.ibm.com/redpapers/pdfs/redp4423.pdf (Accessed: May 2013).

[2] Dhamija, R. & Dusseault, L. (2008). The Seven Flaws of Identity Management: Usability and Security Challenges," IEEE Security and Privacy, vol. 6, March/April, pp. 24-29.

[3] Elliot, J. et al. (2011). Managing multiple electronic identities, retrieved from www.enisa.europe.eu (Accessed: May 2013).

[4] Haley, K. (2010). Symantec Security Response Password Survey, Retrieved from http://www.symantec.com/connect/blogs/password-survey-results (Accessed: May 2013).

[5] Hermans, J. & Valkenburg, P. (2009). "European Identity and Access Management Survey", KPMG and Everett, 2009, Retrieved from http://www.everett.it (Accessed: May 2013).

[6] Milenković, I. et al. (2012). Identity management in cloud computing, ITEO 2012, Proceeding of ITEO 2012, ISBN 978-99955-49-94-7, pp 81-87.

[7] Milenković, I. et al. (2012). Architectures of comprehensive identity and access management, EIIC 2012 (Electronic International Interdisciplinary Conference), Proceedings of the EIIC 2012, ISSN:1338-7871, ISBN 978-80-554-0551-3.

[8] MIT Kerberos Consortium, (2008). The Role of Kerberos in Modern Information Systems, Retrieved from http://www.kerberos.org/software/rolekerberos.pdf (Accessed: May 2013).

[9] Neuman, C. et al. (2005). The Kerberos network authentication service (V5). RFC 4120, retrieved from http://tools.ietf.org/html/rfc4120, (Accessed: May 2013).

[10] Oracle, Implementing Enterprise Single Sign-On in an Identity Management System, Retrieved from http://www.oracle.com/us/products/middleware/identity-management/wp-esso-idm-207215.pdf (Accessed: May 2013).

[11] Pachghare, V.K. (2009). Cryptography And Information Security, New Delhi, pp. 184-185.

[12] Pashalidis, A. & Mitchell, C.J. (2003). A taxonomy of single sign-on systems. In Information Security and Privacy (pp. 249-264). Springer Berlin Heidelberg.

[13] Prasad, G. & Rajbhandari, U. (2011). Identity Management on a Shoestring, Retrieved from http://www.infoq.com/minibooks/Identity-Management-Shoestring (Accessed: May 2013).

[14] Shim, S. et al. (2005). Federated Identity Management," IEEE Computer, vol. 38, 2005, pp. 120-122.

[15] Zhu, L. & Tung, B. (2006). Public key cryptography for initial authentication in Kerberos (PKINIT), Retrieved from http://www.ietf.org/rfc/rfc4556.txt (Accessed: May 2013).

Submitted: May 27, 2013.
Accepted: June 19, 2013.

A Case Study on Introducing E-learning into Seafarers' Education

Sanja Bauk[1], Michael Kopp[2], Avramović Zoran[3]

[1]*Faculty of Maritime Studies, University of Montenegro, bsanjaster@gmail.com*

[2]*Academy for New Media and Knowledge Transfer, University of Graz, michael.kopp@uni-graz.at*

[3]*Faculty of Traffic and Transportation Engineering, University of Belgrade, zoran.avramovic@sf.bg.ac.rs*

Case study

DOI: **10.7251/JIT1301034B** UDC: **37.018.43:004.738.5**

Abstract: This paper considers beginning steps in introducing e-learning into seafarers' education, as additional mode of acquiring knowledge at the Faculty of Maritime Studies which is a part of the University of Montenegro. Related activities are the result of the enthusiasm of few professors and they are partly supported by a small, initial project of bilateral scientific and technological cooperation between Austria and Montenegro. The paper is conceived in a way that it considers following issues: (a) a brief discussion of some current shortages in maritime education and training in general; (b) possibilities of getting advantages through introducing e-learning into this respectable field of education; (c) some advantages and disadvantages of Moodle which has been used as a technological platform for introducing e-learning in the analyzed case; (d) results of the surveys conducted among involved students, teachers, and professionals in the field of employing new media techniques into the knowledge transfer, and (e) some conclusion remarks regarding possibilities of optimal combining maritime and virtual education.

Key words: seafarers' education, e-learning, surveys' analysis.

Introduction

The education and training of seafarers should represent very responsible posts, and consequently appreciated ones. However, it is evident that in the world, at the level of national legislation, there are large differences in the interpretation of the STCW (Standards of Training, Certification and Watchkeeping) Convention and its realization through teaching programs at MET (Maritime Education and Training) institutions [3]. This causes the issuance of a large number of certificates, which do not correspond to objectively sufficient knowledge, skills and competencies of future seamen, that is, of those who may in the perspective educate the next generations of seafarers. This is, of course, a serious problem that could be overcome only by serious top-down approach and far greater investment in education and training (i.e. wages and mobility of teachers/trainers; simulators and other supporting equipment; literature; providing training onboard ships, or so called *underway* training, etc). It is necessary to engage and motivate competent teachers in the field of theoretical teaching (education) of seafarers (people with academic titles and corresponding references) as well as experienced (active) captains and officers in the field of practical teaching (training) to establish active cooperation with referential METs in EU and worldwide, and also with successful shipping companies that should provide students with the appropriate training. All mentioned above is far beyond the scope of this paper in which the authors can only focus on one small segment related to the improvement of education of (future) seafarers based on the implementation of e-learning. So, the following chapters contain the discussion about the motives for the introduction of blended learning at the

Faculty of Maritime Studies (FMS), University of Montenegro, and the potential benefits that primarily students (active and future sailors), then teachers, and consequently, the MET at which such kind of education is realized, might have.

Motives For Implementing E-Learning

The main motive for the introduction of e-learning in the case examined in the paper were numerous seafarers' demands to enable them to have an alternative possibility of upgrading the education that goes beyond the limits of the Bologna Declaration, which has been applied at the FMS since 2006 year. Namely, the strict requirements for attendance of lectures and exercises and limited number of terms for the exams are absolutely inappropriate to the needs of active sailors, who are for a few months, half a year, or longer onboard ships but would like to, or are pressured to improve their knowledge in order to preserve their jobs and/or get career advancement. Another motive was quite natural attempt of a few professors to do something about modernizing traditional ways of teaching through the introduction of new technological solutions. What also has contributed is the fact that the FMS indirectly participated in the Tempus project: "Enhancing the quality of distance learning at Western Balkan higher education institutions" (http://www.dlweb.kg.ac.rs), since it is a part of the University of Montenegro as one of the formal partners on this project. Though, this was a big project, based on which the FMS got the possibility of using the University server by means of which Moodle system was 'set up' and a few teachers had the opportunity to attend short training courses being dedicated to e-learning several times. In addition, the FMS and the Academy for New Media in the Transfer of Knowledge – ANMKT (University of Graz), have successfully implemented a project of bilateral cooperation: "Developing an e-learning module for the educational needs" (2011-2012) and they are currently working on preparations for the realization of the second, follow-up one: "Distant learning implementation at the Faculty of Maritime Studies (University of Montenegro) as an additional mode of education" (2013-2014). Colleagues from Graz transferred very useful practical skills on the use of Moodle in the effective implementation of e-learning to the teachers and system engineers of FMS through several trainings. The results of polls conducted among students during the past (2011-2012) and this academic year (2012-2013), which are depicted and analyzed in the separate parts of this article, speak in favor of success of this collaboration.

Advantages and Disadvantages of the Used Platform

In the implementation of e-learning at the FMS as an additional type of education the Moodle platform (1.9.4.) has been used [1;4;5;6;11]. The Web portal to access the on-line courses is available on the location: http://fzp.moodle.ac.me. Moodle is an open source course management system, also known as a learning management system or a virtual learning environment. It can be relatively easily used by teachers for creating online dynamic web sites for students. It is very sound tool to manage and promote learning. Some institutions use it as the platform to conduct fully online courses while some use it simply to augment "face-to-face" courses, i.e. as blended learning, what is in fact the case of the FMS as a MET institution. In other words, Moodle is used to support and combine "face-to-face" interaction with e-learning, mobile learning and other forms of learning. According to enabling mobile learning there were some plans at the FMS for implementing Windows 7 Phone application [9] that can be viewed as a proxy for Moodle sites, simplifying and adapting user interface for mobile devices. But this currently remains only on the level of the potential future solution.

Within the following parts of the paper some advantages and disadvantages of a Moodle (1.9.4) will be listed. It is indisputable that the number of benefits is larger, but after dealing with some limitations of the used version of Moodle, in this particular case, we started work on the "raising" of the new (experimental) server with more advanced Moodle (2.3) version. However, since a lot of information on Moodle can be found on the website: https://moodle.org, so much attention will not be given to them, but to some of our personal observations and experiences related to the use of Moodle (1.9.4).

Since the currently released version of Moodle is 2.4 it has to be explained why at the FMS there is still a rather old version of the platform in use. When Moodle was installed at the FMS release 1.6 was the current version. This version was regularly updated until version 1.9.4. Since the program surface of Moodle rather changed with the release of Moodle 2.x FMS decided to stick to the older version. Mainly this is due to two reasons: 1) Teachers and students are used to the look and feel of the 1.9.x versions and it seemed problematical for them to grow accustomed to a new surface especially at an early stage of working with the platform; and/or 2) The installation of Moodle 2.x demands an enhanced technical environment which is not totally available at the FMS at the moment.

Advantages of Moodle (1.9.4.)

From the standpoint of teachers (educators) the advantages of Moodle (in comparison of not using a course management system) are numerous. First of all using electronic boards, forums and/or mail teachers can very elegantly direct students to the sites which contain meticulously prepared materials (textual, audio and video recordings) including links to the relevant Web sites, educational games, tests for self-evaluation and others. In the considered case, students are mostly sailors, who spend most of the time of the year on the ship (i.e. at the sea or in the ports located all around the world). While students use on-line educational materials available and mostly are self-taught (here we are talking about students at the postgraduate level), teachers may do the research work, or e.g. work on projects. Thus, they improve their own competence and enhance the reputation and quality of the MET institution at which they are employed. So, the benefits are undeniable manifold. From the standpoint of students, especially seafarers among them, the availability of materials and the opportunity to learn while they are on board is of up most importance. That enables them to work, learn and gain achievements in the career, in parallel. In acquiring new knowledge they can be guided by their own living and working paces because they are in a "classroom without walls" and not in a traditional one with, abstractly saying, „multiple walls".

In using Moodle (1.9.4) platform, the possibilities of students' self-testing and playing educational games (of course, with the automatic generation of the results in both cases) are of particular importance and worth. When it comes to educational games, we used a special software package Hot Potatoes (which includes options: JCloze, JQuiz, JCross, JMatch, and JMix). More about this package can be found on the Web location: http://hotpot.uvic.ca. At the first sight, one might conclude that the last is a trivial tool, but it is in fact a very useful didactic approach, which encourages students to achieve a better result by continuously playing the game and consequently to learn more. What some of the involved students have concluded in the affirmative sense according to this (for them new) aspect of the knowledge acquisition, readers can find out from the section in which the analysis of students' surveys are given.

Disadvantages of Moodle (1.9.4)

When the disadvantages of using Moodle, specifically of version 1.9.4., are on the board, we should say that our experience in working with mathematical expressions, lessons, wikis and the setting up of an online survey for students were not completely satisfying in the sense that we have encountered (in fact as the end users) some obstacles in the implementation of some of our ideas. That actually encouraged us to start thinking more intensively about the rapid transition to Moodle 2.3 version. What some of the involved students have noticed as shortcomings (not only for the Moodle as a platform, but in general for the whole concept of blended learning) readers also can find out in the section where the results of students' surveys are analyzed.

Realization of the Surveys

In order to obtain a feedback on the realized program of e-learning for students of the specialist studies at the FMS we conducted several surveys. One survey was conducted among professors at the FMS and experts in developing new IT-supported didactic methods from the ANMKT. The other one was realized among students (seafarers), i.e. users of this new IT tools enriched type of education, in two different time intervals, i.e. in the academic years 2011-2012 and 2012-2013.

Survey Conducted Among the Teachers and the Experts – Based on the Ahp Approach

The survey conducted among the teachers at the FMS and the experts from the ANMKT is based on the Saaty AHP (Analytical Hierarchy Process) method [12-18] and this approach has actually enabled us to rank some features of e-learning, which are in the framework of this study identified as important. But certainly we are not limited by them in the sense that we underline the need for further, more extensive and detail research in this area.

Namely, the idea of certain e-learning features (eFs) ranking is associated with AHP with respect to the estimates of the respondents (here professors at the FMS and professionals from ANMKT). In general, ranking is a procedure, where the most significant e-learning feature is given the highest rank and the last significant feature is given the lowest rank while the other considered features are somewhere in between these two upper and down rank boundary values. Here, the respondents were asked to compare each pair of the criteria sets eF1-eF6 (Table 1) according to the Saaty scale by using grades: 1-same importance; 3-weakly more importance, 5-moderately more importance, 7-strongly more importance, and 9-absolutely more importance of the first than the second considered criterion; or, by the corresponding reciprocity values depending on the mutual importance of the compared elements composing the certain pair(s).

Table 1. Considered e-learning features

eFs	Features
eF_1	Stability and speed of the Internet connection (what is not always the case at the sea)
eF_2	Availability on-line of all necessary materials for preparing the exam in a subject
eF_3	The existence of the tests for self evaluation of the acquired knowledge
eF_4	Conducting regular students' surveys
eF_5	Possibility of regular communication with teachers via forum, chat and/or e-mail
eF_6	Possibility of making tests and final exam on-line

The example of the Saaty matrix created by one of the respondents (experts) for the purpose of the conducted case study and then used in determining the rank of criteria is given below:

$$\begin{bmatrix} eFs & eF_1 & eF_2 & eF_3 & eF_4 & eF_5 & eF_6 \\ eF_1 & 1 & 1 & 1 & 1 & 1 & 3 \\ eF_2 & 1 & 1 & 1 & 3 & 3 & 5 \\ 1eF_3 & 1 & 1 & 1 & 3 & 3 & 5 \\ eF_4 & 1 & 1/3 & 1/3 & 1 & 1/3 & 3 \\ eF_5 & 1 & 1/3 & 1/3 & 3 & 1 & 5 \\ eF_6 & 1/3 & 1/5 & 1/5 & 1/3 & 1/5 & 1 \end{bmatrix}.$$

Although, for the purpose of this research work, twenty competent persons were asked to create the Saaty matrixes, only ten of these matrixes have been taken into further consideration since they were consistent. By the normalized eigenvector values calculus [19;20], the ranks of the considered criteria eF1-eF6 (per each respondent) have been calculated (Table 2), along with the values of the largest eigenvalue λ_{max}, and the ratio of consistency index CR, while the random index RI is equal to 1.24 in all cases, since the number of criteria is constant and equal to six, in this case. It is obvious that all λ_{max} values, for each considered matrix, are less than 0.01, which is to be fulfilled in order to provide a satisfying degree of the Saaty matrix consistency (Table 3). For these calculus, the appropriate Mathematica (5.1) programs have been used [2].

Table 2. The ranks of the considered eFs assigned by each of the ten competitive respondents

eFs/Rs	R_1	R_2	R_3	R_4	R_5	R_6	R_7	R_8	R_9	R_{10}
eF_1	2	1	1	1	2	1	3	1	2	1
eF_2	1	1	1	1	1	2	1	2	1	2
eF_3	1	2	1	2	3	3	4	3	3	2
eF_4	4	5	3	5	5	5	5	4	4	3
eF_5	3	3	1	3	1	4	2	2	2	4
eF_6	5	4	2	4	4	2	6	5	5	5

The results presented in Tables 2 and 3 have been realized in Mathematica (5.1) program, and the following pseudo-code is given in Table 4 [2].

Table 3. The largest eigenvalue and relative consistency index for each matrix estimated by the respondents

Rs	R_1	R_2	R_3	R_4	R_5	R_6	R_7	R_8	R_9	R_{10}
λ_{max}	6.36016	6.60484	6.03873	6.56456	6.53663	6.53540	6.54947	6.54948	6.05530	6.56732
CR	0.05809	0.09755	0.00625	0.09106	0.08655	0.08862	0.08862	0.08866	0.09766	0.09150

Table 4. Mathematica program pseudo-code for determining eFs rank per each responder [2]

```
Pseudo-code 1: Off[General::spell1]
(*n=Input["Number of criteria is (n):"];*)
(*A=Table[0,{n},{n}];
For [i=1,i≤n,i++,
For [j=1,j≤n,j++,
A[[i,j]]=Input["Input Saaty matrix A ["<>ToString[i]<> ","<>ToString[i]<> "]:"];
If [A=[[i,j]]= =$ Canceled ∨ A[[i,j]]= =Null, Abort[]]];*)
n=6;
A={{1,5,9,3,5,5},{1/5,1,7,3,3,3},{1/9,1/7,1,1/5,1/5,1/3},
{1/3,1/3,5,1,3,3},{1/5,1/3,5,1/3,1,3},{1/5,1/3,3,1/3,1/3,1}};
wn=Table[0,{n}]; wp=Table[0,{n}];
For[i=1;ws=0,i≤n,i++,wn[[i]]= ∏_{j=1}^{n} A[[i,j]] ;wp[[i]]=wn[[i]]^(1/n);ws=ws+wp[[i]]]
w=Table[0,{n},{1}];
For[i=1;i≤n,i++,wn[[i,1]]=wp[[i]]/ws]
V=A·w; l=V/w;
λ=(1/n) Σ_{i=1}^{n} l[[i,1]];
CI=( λ-n)/(n-1);
RI={0,0,0.58,0.9,1.12,1.24,1.32,1.41,1.45};
CR=CI/RI[[n]];
Print ["λ= ",N[λ]];
Print ["CI= ", N[CI]];
Print ["RI= ", N[RI]];
Print ["CR= ", N[CR]]; If CR≤0.1,
Print ["Saaty's matrix is consistant"],
```

The main point is to determine the overall rank of in the paper considered features of e-learning (Fe1-Fe6) on the basis of the individual ranks establish by Saaty matrix, i.e. given by each of the experts individually. For this purpose it is necessary to determine the weight coefficients for each of the considered eF criteria and the process of their determination follows.

The idea of evaluating above mentioned weight coefficients is associated with the sum of ranks of each criterion c_q, with respect to the estimates of respondents (1):

$$c_q = \sum_{r=1}^{10} c_{qr}, q = \overline{1,6}. \quad (1)$$

Where,

c_q - is the sum of ranks of each criterion (eF), while q is the number of considered features (here 6), and r is number of experts, or respondents (here 10); and,

c_q - is rank of the q-th criterion estimated by the r-th respondent. Now, the average weight coefficient for each criteria (q = 1,6) can be calculated by the following formulae (2):

$$w_q = \left[\frac{c_q}{\sum_{q=1}^{6} c_q} \right]^{-1}. \quad (2)$$

Finally, the normalized average weight coefficients are to be calculated for each concerned criterion (3):

$$\overline{w}_q = \frac{w_q}{\sum_{q=1}^{6} w_q}. \quad (3)$$

The overall ranking of eF_1-eF_6 criteria according to their significance, carried out by ten respondents, is demonstrated in Table 5.

Table 5. The final rank of the eF_1-eF_6 criteria formed on the basis of the respondents' questionnaires

eFs	Features	$\overline{w}_q$	Rank
eF_1	Stability and speed of the Internet connection (what is not always the case at the sea)	0.244808	**2**
eF_2	Availability on-line of all necessary materials for preparing the exam in a subject	0.282471	**1**
eF_3	The existence of the tests for self evaluation of the acquired knowledge	0.153005	**3**
eF_4	Conducting regular students' surveys	0.085398	**6**
eF_5	Possibility of regular communication with teachers via forum, chat and/or e-mail	0.146885	**4**
eF_6	Possibility of making tests and final exam on-line	0.087432	**5**

In order to examine the level of consistency of the respondents' estimates, the concordance coefficient W is to be calculated by (4):

$$W = 12S/r^2q(q^2-1). \quad (4)$$

Where,

$S = \sum_{q=1}^{6}\left(c_q - \sum_{q=1}^{6} c_q\right)^2$ - is analogue to the variance of the ranks;

r – is the number of the respondents (10); and,

q – is the number of the considered eF criteria (6).

Now, the smallest value of W, i.e. W_{min} is to be calculated by the formulae (5):

$$W_{min} = \chi^2_{\alpha,\nu} / r(q-1). \quad (5)$$

Where, $\chi^2_{\alpha,\nu}$ - is critical chi-square statistics, found in the table [7] by assuming the degree of freedom $\nu = 6 - 1 = 5$, and the significant level $\alpha = 0.010$. Here, it is . By taking into account the previous assumptions $W_{min} = 0.3018$, while $W = 0.476571$. Since the condition $W_{min} \leq W$ has been satisfied, it implies that the estimates of the respondents are consistent, what means the previously obtained rang of criteria eF1-eF6 (Table 4) is the valid one. The previous calculi have been realized by Mathematica (5.1) program and the associated pseudo-code is given in Table 6 [2].

Table 6. Mathematica program pseudo-code for testing the consistency of the respondents' estimates [2]

Quantified results of the survey among the experts in the field of e-learning could be qualified as follows:

Pseudo-code 2: Off[General::spell1]
n=Input["Number of criteria is(n):"];
m=Input["Number of respondents is (m):"];
Cm=Table[0,{n},{m}];
For [i=1,i≤n,i++,
For [j=1,j≤n,j++,
Cm[[i,j]]=Input["Input rank for the criterion "<>ToString[i]<> "and respondent"<>ToString[i]<>":"];
If [Cm=[[i,j]]==$Canceled ∨ Cm[[i,j]]==Null,Abort[]]]];*)
c=Table[0,{n}];

For[i=1;cs=0, i≤n,i++,c[[i]]= $\sum_{j=1}^{m} Cm[[i,j]]$;cs=cs+c[[i]]]/n

$S = \sum_{i=1}^{n} (c[[i]] - cs)^2$;

$W = \frac{12S}{m^2 n(n^2-1)}$;

$\chi^2 = Wm(n-1)$;

$\chi^2_{\alpha,\nu}$ =Input["Input the critical chi-square, from the statistical table: "];

$W_{min} = \frac{\chi^2_{\alpha,\nu}}{m(n-1)}$;

Print["S= ",S];
Print["W= ",W];
Print[" χ^2 = ", χ^2];
Print["", W_{min}];
If[W_{min} ≤W, Print["The estimates of the respondents are consistent."],
Print["The estimates of the respondents are not consistent"].

- The experts involved in this research assigned numerically by the largest marks and gave consequently the greatest importance in the qualitative sense, to the availability of educational materials (which implies their appropriateness and quality).
- In the second place, the experts positioned stability of Internet connection, which is understandable, since in the paper very specific application of e-learning related primarily to the needs of seafarers has been considered. Namely, it is often not possible to establish Internet connection on the vast sea, or it is usually unstable. Another reason for the second highest rating of this parameter might be that the experts might consider a stable Internet connection as a fundamental basis for the establishment of e-learning offers.
- Experts put on the third position the availability of tests for students' (here seafarers') self-evaluation, which is also a very important segment of e-learning, which indirectly should involve the existence of smart educational games, as well.
- The fourth position is reserved here to the possibilities for the students to communicate with teachers via forum, chat, e-mail, etc, which is of course very important segment of e-learning, but it is sometimes difficult to achieve this due to the previously mentioned problems with Internet connection and its stability at the sea (and sometimes in the ports). On the other side, teachers are usually too busy, and they are practically sometimes physically prevented to devote more time for communication with students.
- On the last positions are technical possibilities of doing exams on-line, and conducting regular on-line (or classical) surveys among the students, related to their degree of satisfaction with offered e-learning services, respectively. This is understandable, since the Internet as an open communication channel is not perfect for testing students on-line. In addition, surveys conducted among students are very important, but in comparison with the previously considered components of e-learning are for sure slightly less important. However, this does not mean at all that they should be ignored.
- This survey reflexes profoundly very subtle nuances in mutual positions of the analyzed e-learning features, and it remains us to associate them to the high degree of expertise and sensitivity of the interviewed experts in this field.

Survey Conducted Among Students

The survey was implemented among the students at the FMS and it was done on a larger sample than the previous one. It is considerably simpler in terms of the content and results analysis, but not less revealing. Respondents were students from the different FMS departments and with different experiences according to their employment and the length of the navigation service. The survey was conducted in two rounds, i.e. in two different time sections: during the academic years 2011-2012 and 2012-2013.

Some of the results are presented in Table 7. Thus, the table shows the percentage of surveyed students who had opted for the offered advantages and disadvantages of e-learning. Distinctly the highest percentage of students opted for "the possibility of learning from home and working place", while for the disadvantages of e-learning the highest percentage of students opted for "lack of direct contact with teachers" (2011-2012) and "inability to interrupt the class, put a question, and get the answer immediately when there is some ambiguity in knowledge transfer" (2012-2013).

Table 7. The results of the students' surveys (conducted in 2011-2012 and 2012-2013 academic years)

	Academic year:	**2011-2012**	**2012-2013**
No.	**Advantages of e-learning**	„Yes" answers	„Yes" answers
1.	The possibility of learning from home and working place (during the breaks)	60.78 %	91.38 %
2.	Reducing the traveling costs and time saving	25.49 %	79.31 %
3.	Easier access to the instructional materials	27.45 %	74.14 %
4.	Possibility of self knowledge evaluation through on-line tests	13.73 %	79.31 %
5.	Ability to communicate via the net with teachers and other candidates	15.69 %	63.79 %
6.	More effective learning	13.73 %	65.52 %
No.	**Disadvantages of e-learning**	„Yes" answers	„Yes" answers
1.	Lack of direct contact with teachers	45.10 %	53.45 %
2.	Inability to "interrupt" the class, put a question, and get the answer immediately when there is some ambiguity in knowledge transfer	43.14 %	60.34 %
3.	A nonstandard form of learning that requires a strong will, self-discipline, and high level of concentration	13.73 %	31.03 %
4.	Some colloquiums are taken on-line, which is sometimes stressful, due to limited time, and present fear if the technique will/will not function properly	11.76 %	29.31 %
	Number of students involved into the survey:	51	58

When it comes to the results of surveys conducted among students, some inconsistencies have to be noticed, as for example a quite large discrepancies in some results obtained in (2011-2012) and (2012-2013). The largest differences are observed when it comes to e-learning advantages regarding the possibilities of students' self-evaluation of acquired knowledge, and more effective learning that allows e-learning. This discrepancy inspired us to think about it, and led to the conclusion that the results obtained in (2012-2013) should be taken, however, as more reliable. The question is why? – The e-learning facilities that are offered to students this year are far more extensive and of higher quality than those of the previous year. Additionally, some of interviewed students were using e-learning services at the FMS for two years continuously, and therefore they should be treated as more competent to judge what is important to them due e-learning and to what extent. Though, if we focus on the assessment of the students in the "second round" (2012-2013), then we should make the following conclusions:

- Due to the benefits of e-learning, the opportunity to learn from home or from work or at leisure time was identified as the greatest advantage. This is not really remarkable because learning anytime and anyhow is an – meanwhile well known – essential benefit of e-learning.
- The second position in terms of the students surveyed is shared by the reduction of commuting costs and the possibility of self-evaluation (either through on-line tests and different educational games). Again, reducing travelling costs and saving time is a rather obvious advantage of e-learning. More interesting is the fact that the availability of self-evaluation is very important for almost 80% of the students. This rating shows that students are very well aware of additional educational possibilities that come along with e-learning and that students are willing to use these possibilities for their own learning purposes. Moreover evaluations of the use of the Moodle courses show that self evaluations are very popular among the students especially immediately before exams.
- The third place belongs to the greater availability of educational materials than in the case of traditional teaching. This good rating is probably owed to the fact that the polled students are seafarers with a lot of travel activities who do not have the chance to spend much time in the classroom.
- In the fourth position is placed the possibility of learning more effective, which could mean that it is still in some ways easier to the students to learn if they have a teacher "in front of them", i.e. physically

present (even this conclusion should be treated as hypothetical one).
- The last place among the advantages of e-learning belongs to the ability to communicate (regularly) with teachers. How can this be explained? - Teachers are often not able to meet the requirements of the students (all their questions sent by e-mail, e.g.) and to be available though the chat and/or forum sessions. Therefore, the most likely students agreed that this possibility is not (unfortunately) of essential importance to them. This should of course be considered and corrected in the perspective.
- Due to the disadvantages of e-learning, students have cited the inability to directly ask the teacher what they do not understand in the learning materials as the greatest shortcoming. Thus, this greatly complicates their understanding and learning processes. Anyway, the rating is consistent with the rather poor rating of the ability to communicate with teacher as an advantage.
- In the second place, students positioned the lack of physical presence of the teacher, which is directly linked to the previous and therefore quite logical. And this can be explained as indeed the biggest and the most profound dilemma concerning traditional vice-versa e-learning.
- The necessity of students' strong will, concentration and learning self-discipline is placed in the third position. This should be fortunately interpreted in the way that most of the students fulfilled these very important preconditions of successful e-learning.
- The fourth place among the disadvantages of e-learning, students have associated to the stress caused by taking some colloquiums and tests on-line. This is logical, since most of the students are familiar with PCs and doing the tests on-line, in the technical sense, is not a big problem for them.

Within the additional survey conducted at the end of the semester of 2012-2013 the students should respond affirmatively/negatively to these three questions [10]:
- E-learning has a future in the sense that it will be increasingly used? (Answer "Yes": 100%);
- E-learning will lose its importance in the coming years? (Answer "No": 100%); and,
- Do you (personally) prefer e-learning than traditional lecture "face-to-face"? (Answer "Yes": 76%).

In the brackets next to these questions are given the percentages of surveyed students (58 of them) who responded affirmatively/negatively (depending on question). There is no doubt, according to the results of this short survey conducted among the students at the FMS, that the future learning channels shall be based on novel technical and didactical e-learning solutions.

Conclusions

By comparing some observations from the first part of the paper to those of the following sections, it could be concluded that it is about building *a new roof on the old and damaged walls*. And what does it really matter? – A vain job, or however something else? - We believe, it is still something else. All this effort over the introduction and development of e-learning at the FMS should be one more in a series of incentives toward improving the educational process at the MET institutions in terms of recommendations which are generally given in the introduction. Thus, the need for greater investment in seafarers' higher education in terms of personnel and infrastructure is indisputable. Additionally, the networking is very important, not just for networking, but a real one is essential, based on professional cooperation and reciprocity on the EU level and among the referential MET institutions, exchanges of teachers and students for the sake of mutual enrichment of knowledge, the launch and implementation of joint projects, etc. All of this is to be done to the extent that is feasible and before it becomes too late. Also, it is necessary to establish a connection with the maritime industry, e.g. shipping companies interested in providing practical training onboard ships. The national legislation has to be modernized in the sphere of higher education in terms of recognition and proper interpretation and implementation of the STCW Convention requirements and in terms of faster deployment of virtual learning as a supplement to the traditional education and training of the seafarers. Within this context we should not lose the sight of the fact that STCW Convention itself calls for a proper education as the foundation of successful training and acquiring competences [8]. In order to confirm this observation the quotations from the STCW Manila Amendments, Chapter II, Section B-II / 1, Paragraph 14 are given: "Scope of knowledge is implicit in the concept of competence. This

includes relevant knowledge, theory, principles and cognitive skills which, to varying degrees, underpin all levels of competence. It also encompasses proficiency in what to do, how and when to do it, and why it should be done. Properly applied, this will help to ensure that a candidate can: work competently in different ships and across a range of circumstances; anticipate, prepare for and deal with contingencies; and adapt to new and changing requirements." Additionally, of importance within the context of this paper is that the newest STCW Code amendments concern and not only concern, but strongly recommend - the introduction of modern training methodology including distance learning and web-based learning in seafarers' knowledge acquiring and upgrading.

Acknowledgement

The authors would like to thank colleagues from the ANMKT and from the FMS as well as the students at the FMS since their kindness enabled successful implementation of the surveys and the sub sequential analysis of the obtained and in the paper presented results, which can serve as a stimulus for further more profound research in this area.

Authorship statement

Author(s) confirms that the above named article is an original work, did not previously published or is currently under consideration for any other publication.

Conflicts of interest

We declare that we have no conflicts of interest.

References:

[1] Bauk, S., Dlabač, T. & Pekić, Ž. (2012). Implementing e-learning modes to the students and seafarers education: Faculty of Maritime Studies of Kotor case study, *IMSC*, 14th International Maritime Science Conference, 16-17th June, Split (Croatia), 98-104.

[2] Bauk, S., Šekularac-Ivošević, S. & Jolić, N. (2012). Seaport positioning supported by the combination of some quantitative and qualitative approaches, *Transport* (accepted for publishing on 23rd October, 2012).

[3] Bergquist, C. (2008). Training of future seafarers – new challenges for MET:s, *IMLA*, 16th International Maritime Lecturers Association Conference, 14-17th October, Izmir (Turkey), 207-211.

[4] Blagojević, M. (2010). Web-mining Applications in Education, *ICTTIE*, 3rd International Conference on Techniques and Informatics in Education, 7-9th May, Čačak (Serbia).

[5] Buzađija, N. (2011). The Way of Students' Efficiency Improvement in Knowledge Acquisition and Transfer Knowledge Model in Clarolina CMS, *JITA – Journal of Information Technology and Applications*, Vol. 1, No. 2, 127-135.

[6] Lakhan, S. & Jhunjhunwala, K. (2008). Open Source Software in Education, *Educause*, Vol. 31, No. 2, April-June.

[7] Montgomery, D.C. (2008). *Introduction to Statistical Quality Control*, 6th Edition, USA, Wiley.

[8] Murray, G. (2012). *Does e-learning work?*, Internet resource (www.marinels.com; downloaded in November).

[9] Pekić, Ž. (2011). Windows mobile application as support for e-learning in education, *POWA*, 6th International Symposium: Ports and Waterways, 12th October, Zagreb (Croatia).

[10] Radović-Marković, M. (2010). Advantages and disadvantages of e-learning in comparison to traditional forms of learning, *Annals of the University of Petrosani*, Economics, 10(2), 289-298.

[11] Rice, W.H. (2006). *Moodle E-Learning Course Development*, Packt Publishing, Inc.

[12] Saaty, T. (1977). A scaling method for priorities in hierarchical structures, *Journal of Mathematical Psychology*, 15, 234-281.

[13] Saaty, T. (1980). *Multicriteria decision making: the analytic hierarchy process*, New York, Mc Graw-Hill.

[14] Saaty, T. (1980). *The Analytic Hierarchy Process*, New York, Mc Graw-Hill.

[15] Saaty, T. (1990). *Multicriteria decision making: The Analytic Hierarchy Process*, Pittsburgh, RWS Publications.

[16] Saaty, T. (1994). Homogeneteity and clustering in AHP ensures the validity of the scale, *European Journal of Operational Research*, 72, 589-601.

[17] Saaty, T. (1994). How to make a decision: The Analytic Hierarchy Process, *Interfaces*, 24(6), 19-43.

[18] Saaty, T. (2003). Decision-making with the AHP: Why is the principal eigenvector necessary, *European Journal of Operational Research*, 145, 85-91.

[19] Sivilevičius, H. & Maskeliunaite, L. (2010). The criteria for identifying the quality of passengers' transportation by railway and their ranking using AHP method, *Transport*, 25(4), 368-381.

[20] Шикин, Е.В. & Чхартишвили, А.Г. (2000). *Математические методы и модели в управлении* [Shikin, E. V.; Chhartishvili, A. G. Mathematical methods and models in management]. Москва: Дело. 440 с. (in Russian)

Submitted: February 16, 2013.
Accepted: May 29, 2013.

The innovation ICT strategy in agri-food sector

Luisa Sturiale[1], Alessandro Scuderi[2]

[1]Department of Civil and Environmental Engineering (DICA), Faculty of Engineering, University of Catania, Italy, e-mail: luisa.sturiale@dica.unict.it

[2]Departemet of Agri-food and environmental systems and management (DIGESA), Faculty of Agriculture, University of Catania, Italy, e-mail: alessandro.scuderi@unict.it

Case study

DOI: **10.7251/JIT1301043S** UDC: **005.3:004.738.5]:631.15**

Abstract: The achievement of Information Communication Technology (ICT) as a new ground for economic competition is deeply affecting the trade organization in many merchant sectors. For Italian agri-food products it is of absolute importance for Internet marketing to be undertaken and to foresee the consequent scenarios. The aim of this research is to exactly assess the opportunities and problems of the distribution circuit based on the virtual scenario, with a methodological and empirical approach, working on the analysis of experiences already begun by agri-food companies established in Italy and engaged in "business to consumer" and "business to business". The ICT is configured as a phenomenon in a continuous and rapid evolution, which makes it necessary for companies to continually adapt to it and to the habits of web-consumers. This means that it is necessary to effectively enter the network of agri-food firms, and to strategically revise marketing methods focusing on the market place.

Keywords: web marketing, e-business, agri-food , web site.

Introduction

Development of digital technology and spreading of computer networks have transformed production processes, access to, transfer and use of information. Communication technologies allow the easiest access to knowledge and the easiest way to create it due to the simple sharing of information from e-mails to forums to social networks with the consequent reduction of space-time barriers.

Characteristics of the Knowledge Age reflect everywhere on today's society. ICT, Internet protocols, spreading of new electronic services have been affecting every sector of our life, deeply changing settled habits and systems. In the latest years, much has been invested in terms of energy and funds to develop and promote new technologies in order to embrace opportunities and teach society how to follow changes. According to Netcomm and Assinform researches [12], the average percentage of GDP destined to invest in ICTs in Europe amounted to 23.0 %; Germany, France and United Kingdom with 28.0% and Italy with 19.0%.

At the end of the 20th century, two huge phenomena revolutionized economy and everyday life: globalization which brought more and more interdependence among world's economies and, technological revolution with Internet and ICT, Information and Communications Technology.

Then, a shift has occurred from the society of communication and information to the society of knowledge, that is, from a build-up of information to the elaboration and comprehension of information.

ICT opened new lands to economic competition which is deeply affecting trade in different sectors and in some cases also altering the very competition rules themselves.

Cultural aspects, safety and health of products represent obstacles to the diffusion of ICT and web tools within the agri-food sectors, as well as the lack of quality of web sites and the scarce attention paid to the "interactivity" with web-consumers, which is fundamental instead of web-marketing. Besides, there is a poor level of standardization for these sector products and several difficulties for managing the quality by e-commerce (among works of literature we mention, in order of the year of publication, a few concerning farms and agri-food SMEs in Italy and abroad: [3], [4], [5], [11], [18], [19]).

The aim of this paper is to shortly trace the role of ICT within the Italian economic system, in particular in the agri-food one, and then to present the results of our research, still in progress, which has allowed us to reveal how agri-food companies have exploited the new technologies and how they have adapted to it (or will) after more than a decade since the beginning of the digital revolution. In particular, we focused on the way e-commerce has spread into the market and the web-marketing strategies, by means of specific surveys carried out by field operators and the analysis of sample web sites of agri-food companies and producers of local products, supported by the special model of 7Cs [19].

ICT APPLICATION: NEW STRATEGY IN AGRI-FOOD COMPANIES

ICT applied to medicine, education, politics, and economy is deeply changing the settled habits and by doing so starting the so-called digital revolution, which has caused democratization of decisional processes, immateriality of culture, open mindedness and freedom. Those aspects can then be framed in a perspective of worldwide social development and improvement of man's welfare. It is clear that such a phenomenon has not had the same effects everywhere. In fact, the mass media talk of digital divide refers to the gap between those who can access and use the tools of the Knowledge Age and those who are cut out for different reasons: age, location, economical status, internet access. At a global level, developing countries experience a bigger gap, followed by emerging ones, while E.U. countries experience delay, such as Italy, Spain, Portugal and Eastern Countries. The digital divide may, to a greater extent, affect the deep social inequalities of each country. According to the "Connectivity scorecard", which monitors the web impact on the national economy (London Business School), among 25 industrialized countries, Italy was 22nd. Sweden, United States, Norway and Denmark, are at the top of the list, while Hungary, Poland and Greece are behind Italy. In particular, the Connectivity Scorecard estimates the use of wire technologies - optic fiber, telephones and PCs - made by governments, companies and consumers, in order to boost the economy and improve social life, the so-called "useful connectivity". Italy has got a low score in all categories here analyzed - the use of the web made by citizens, governments and companies in the country - so it is behind all other G7 countries. The lowest score is that for the use of e-Banking service and e-commerce; while companies have unsafe servers and PCs. This means they do not rely on e- commerce and people do not buy or sell on line [21].

It is important to highlight the e-commerce gap. As far as web-consumers are concerned, in fact, in Italy, in 2011, only 12.0% of citizens bought on line once, while in the United Kingdom the percentage was 66.0%, in Germany 56.0% and in France 54.0%.

Within the new virtual scenario, e-commerce is one of the most important and dynamic aspects of the bigger process called e-business [18].

Internet, although maintaining the basic rules of economy, enlarged the information revolution [16], which is still in progress, not only at the company level, by forcing companies to transform their business processes, but also at the sector level, influencing structures and dynamics of competition [13], [20].

Companies are internalizing the new market and technology's culture by modifying their business models in different steps: from e-trade, to e-commerce, to e-business. In detail, the "e-trade" is intended as the electronic channel complementary to the traditional

ones; the "e-commerce" is one of the ways that allows interacting with the market in order to understand the demands and meet its requirements; the "e-business" includes the technologic lever within the internal and external process of a company to obtain a long-lasting competitive advantage [17].

In the last few years Internet started its third-phase of life, as the result of a new relational paradigm between merchants and customers where the engagement of the latter is part of the trading process, but also of the product. The first phase was characterized by the presence of the very players, who created new business models that ate away physical market shares, Amazon for example, with young, well-educated and technologically-advanced customers. The second phase, more recently, experienced the arrival of web technicians, in which, Italian companies of Made-in-Italy and large-scale retail trade are investing in order to recover the competitive gap. Multichannel customers are much more transversal than those of the first phase, more aware, informed, and watchful for prices and services [14].

IT systems are engaging tools and space for more interaction to meet the new needs of companies and consumers. For example, Web 2.0 tools, which, first of all, include social networks, are a global phenomenon which is changing e-business. Social networks, in fact, are deemed as a real support for the company strategy, because they offer a media mix approach that works in synergy with different channels and tools (CRM - stands for Customer Relationship Management; - CMS - Content Management System, a software installed on a server that makes management of web site- content easier, e-mail, intranet), besides being always and everywhere present, with one main goal: listening to customers and their needs.

Today, there are 1.5 billion people connected worldwide, potential customers who, on the web, look for information and then to buy. In Italy there are 18 million web-surfers that look for information and compare products and services offered, the so-called info-commerce. Only 6 millions, then, really buy on line.

This is the real shopping potential of the web, still unexpressed. 6.5 billion euros, in fact, represent 1.0% of the whole sale turnover to final consumers, with a big difference compared to the rest of the Europe where B2C value is on average equal to 4.0%. According to Eurostat sources, against the European average share of the total retail turnover of 4.0% of e-commerce, Ireland got 10.0%, followed by the United Kingdom with 6.0%, Spain and Germany with 5.0%. [7]. It is important to specify that in Europe, e-commerce includes grocery, home goods, furniture, do-it- yourself, while in Italy does not, as well as it does not include modern retail trade (e-commerce Observatory B2C, 2012). Among the reasons for this gap there are the structural limits of our country (Internet access and broadband, costs of distribution logistics), Italians' habits (fear to use credit card on line, not liking distance buying), and the difficulty to sell on line certain typologies of products, including agri-food ones. Furthermore, we should not forget the system of offer that barely renovates. International companies still dominate the web market, together with the Italian service companies, but Made-in-Italy and agri-food companies do not. ICT can represent interesting development opportunities, especially for the Made-in-Italy and, in particular, for companies of the agri-food sector. We refer to e-commerce B2C, which may activate exportation of the Italian agri-food products, wellknown worldwide for their tipicity and exclusivity; e-commerce is a valid integration of traditional trade channels in order to improve customer service and renovates the offer, but also web-marketing and Web 2.0 tools for the promotion.

Italian companies should embrace the opportunities offered by social networks considering that 2/3 of the Italian internet users (more than 12 millions) belong to a social network. According to the Facebook Observatory [15], after 7 years of existing, Facebook counts 600 million members. Italy is ninth at the global level with 18 million Italian users (about 32.0% of the residing population), while 12 millions are those who use it daily. Other sources report different figures, but Facebook is for sure a huge social phenomenon that started social advertising.

It may be a privileged tool for a privileged relation with customers; in particular, considering the characteristics of the most familiar social networks, it is possible to match each one with a specific market-

ing function: Facebook is the most suitable tool for developing customer relations; Twitter allows a direct contact with sensitive customers (one-to-one-to-a lot of marketing); YouTube is for emotional marketing.

Survey Method

In order to highlight the delay for agri-food sector to adopt ICT at the national level and the consequent company adjustment [2], after ten years of web revolution, a survey was carried out in two phases.

The first phase drew a short picture of the relationship between the agri-food sector and ICT, presenting the results of surveys of big Italian companies of the sector and modern retail trade.

The second one consisted of the empiric analysis of the web sites of a sample of a small group of agri-food SMEs in order to analyze the use of Internet for marketing and communication, to understand, on one side, which are the strategic goals of online companies, and on the other, to verify the efficacy of a web site for marketing [9].

Survey was carried out by visiting the web sites, analyzing the aspects that may drive consumers' choice and improve web-marketing [8] by adopting the 7C model [19], [4]. The identification of the main parameters that characterize a web site was carried out by means of an ad-hoc layout, which allowed obtaining information on the different aspects that help characterizing its image. In particular: Content - site size, updating frequency, graphic quality; Context - type and site function, market typology; Choice - products offered, product range, characterization of the offer; Comfort - access, surfworthiness, languages, way of purchase and payment methods, shipment and costs, delivery time; Convenience - shipment costs; Customer service and support - product information, services offered, shipment traceability, customer satisfaction, payment security; Community - links, customer relation. For each category we considered micro-variables for each point. Quality variables were evaluated with a parametric scale from 0 (absence) to 5 (excellent). In particular, 1 very bad, 2 scarce, 3 medium, 4 good, 5 excellent. This survey was carried out in 2012 and included 500 representative web sites of companies that were selected through the main national search engines as well as through other web information sources like specific and institutional links. A guided sampling and not a probable one was chosen due to the lack of a defined sample framework as well as the impossibility of knowing the choice probability of each company. Companies analyzed were specialized in different typology of agri-food products: cereals, meat, fruits and vegetables, oil, wines, beverages, including all sub-products. However, only companies' private web sites were analyzed and not virtual malls, due to the specificity of the survey.

The survey included a final questionnaire in order to point out the company's internet plans and targets.

Marketing strategy and ICT application of the Italian agri-food system

Our research allowed obtaining information and data, here shortly summarized, by means with which it was possible to outline today's relation between ICT and the agri-food sector, especially focusing on e-commerce and web-marketing integration within company marketing strategy.

Surveys, which involved some big Italian agri-food companies and some of modern retail trade, allowed pointing out opportunities and limits of ICT application within the system, especially with reference to the adoption of e-commerce B2C and web-marketing strategies in order to intensify customer relation.

The agri-food system, in the last ten years, has joined the virtual scenario, at the beginning with a progressive spreading of web sites, about which some big historical failure was registered concerning the creation of informative-group portal, followed by the spreading of onlinesale of some imperishable products, such as wines.

Despite such approaches we assisted companies joining the web with strategically unclear modalities, and Internet, which instead of being a competitive advantage, is used as a completion of the company's

competitive strategies. SMEs use Internet more for image than as an instrument to relate and interact with customers and suppliers. Potentially, Italian companies could make a better use of the web opportunities.

At the beginning, when many web sites appeared, the error was probably that of considering Internet as a sale channel, while now companies are discovering its strategic potential as an information tool. In fact, it may activate interactive marketing that perfectly meets web-consumer needs, by creating a close one-to-one relation.

The survey revealed that in Italy people restrain from purchasing food products on the web because of skepticism. Overall turnover of this sector has been estimated around 200 million euros in 2010 and despite being higher than in previous years, it is behind other countries, as said before. Wine, beer, biscuits, tea and coffee cover almost 60.0% of on line sales, even if the global network offers Italian niche products (such as excellent wines and pine nut oil), while fresh products are poorly represented such as fruits and vegetables, that people prefer to buy personally.

More than 90.0% of modern retail trade companies are not involved in any e- commerce project. Actually, there is only one big company at the national level, which is successfully investing in it: Esselunga; together with some interesting local ones such as Basko, Prontospesa, Spesaon line (one case is experimental: that of "driveAuchan" in Turin, where the customer can order on line and then pick up the goods from the closest Auchan). Reasons why so few invest in e-commerce is the lack of competence and structures within the company to start a correct e-commerce project; fear of cannibalizing the traditional sale channel; or, in case the e-commerce is already active, the lack of boosting the onlinechannel. Besides, there are difficulties in arranging a logistic-operative process allowing cost control - order execution, delivery, etc.

E-commerce could represent an important lever to export Made in Italy worldwide, as demonstrated by the results obtained so far by those companies that have properly interpreted and exploited the online channel. One such company is Esperya, an online shop created in 1998 as a dotcom with the only aim of selling food-and-wine as traditional Italian products at the national and international level. In September 2007, Esperya started its first shop in Milan selling high quality food products where customers could also taste them. Esperya has more and more foreign customers: from 16.0% in 2006 to more than 30.0% in 2010. Another experience based on the use of ICT is that of Fratelli Carli, whose project OlioCarli.it was created in 1996 in order to join traditional and technologic innovation. E-commerce in this case, positively affected the turnover and customer retention together with an online strategy of integrated multichannel operators.

In the last ten years, however, there has been a reduction of the number of shop-window like sites and an increase of web sites aiming at developing direct marketing and more recently conversational marketing.

Marketing has changed in terms of adapting to the new characteristics of the new tools and has focused on the "information" as a resource for the company and the company customer relation in an integrated version that may increase the value. Recently, according to a research carried out by Netcomm/Contactlab, social networks have gained the power to steer online purchase choice.

Within the marketing strategy, customer-company relation becomes central because it activates a privileged information channel and because it is a base for customer retention. In a competitive and strongly dynamic environment, immaterial factors become basic sources of the competitive advantage since they make companies evolve, meet consumers' demands and foresee changes [6].

Our survey pointed out some history cases of agri-food companies that have embraced the opportunities offered by the Internet and social networks. In fact, several brands have chosen to establish a company-customer relation so that customers can turn from simple users of content to the creators of the content and experience.

Hence, the aims of the web-marketing strategy are those of building up, involving and widening

company-customer relation by means of the web; of increasing the brand awareness; of acquiring more and more information in order to develop targeted communication and activate e-commerce. Many companies have different institutional sites, according to the different targets, and sites for prize contests. Many others create communities based on the principle of Internet and Social Media, that is, that of sharing. In some cases, the site was visited by many people, 50.0% of which were foreigners with the average age of 28. Others joined the web via Web 2.0 tools, such as Facebook and Twitter with the aim of starting a specific relation with customers, making them feel the creators, co-creators and users of their know-how.

Results

Information acquired by analyzing a sample of web sites opened a quite articulated scenario concerning both the company presentation and the services offered to consumers by using ICT.

Out of all data gathered according to the 7C model, we here present only the most important results in order to point out the strong and sore points characterizing the web-marketing of our sample agri-food companies.

The analysis of the first C, Content, in particular of the "size of the site", has shown that most of the web sites include 8-15 pages, while few have 16-25 pages. Less visited are those sites with a lower or higher number of pages. The overall score was 3.8, which is a positive one. As far as "updating" is concerned, it is deemed as one of the most important elements for customer retention, 90.0% of the web sites do not mention it, while 4.3% update their site weekly and 2.7% daily. The remaining percentage does it on a monthly basis. However, data obtained from documents' dates, has shown an overall updating frequency which was very low, with a score of 1.9. In contrast, graphic quality varies a lot, with excellent sites and home-made ones, with an overall score of 2.6.

The analysis of the Context divided the web sites into two categories: institutional and commercial. Based on their different function, the institutional ones are better articulated with a score of 4.3, while the commercial ones have a score of 2.3 with limit cases of 0.4. As far as the "market typology" is concerned, almost 63.0% of the web sites belong to B2C, 7.1% to B2B, the remaining share the both.

Among the aspects examined, concerning the Choice parameter, the most important results are those related to the "typology of commercialized products". The most favorite ones are those certified DOP, IGP, organic with 42.0%, and those bound to specific territories. Web sites concerning their range of products got a score of 3.2, which is good, while 2.2 was assigned to the characterization and description of each product due to the limited information presented.

The Comfort includes many interesting elements. Here, we included just a few of them. Accessibility got a score of 3.9 since it is quite easy to find the web sites, but once entered it is difficult to visit most of the sites, even to open pages. 60.0% of the web sites have language limitations, which prevents internationalization, offering only Italian or at most English. Score: 1.1, meaning that this is one of the most important points to work on in order to reduce the gap with the rest of the world.

The Convenience parameter is different for each site. In general, however, the online offer is huge. Hence, the "online offer" was scored 2.7 according to what has been said above and due to the shop-window function adopted by many companies. However, the advantages compared to the traditional channel are not pointed out, if not completely absent. The score in this case is 1.2.

The approach to Customer Service and Support was careless, which is very important for web marketing strategies, instead, the virtue of the specific characteristics of e-commerce interactivity was compared to the traditional ones. In fact, except for the information system, which got the score of 3.9, the rest of the parameters, such as traceability, claims, customer satisfaction and payment security, got the score ranging from 1.1 to 2.1.

Last but not least, the Community, on which, online companies have focused the most. In fact, all such companies intended, by their online presence, to es-

tablish an interaction with customers, besides carrying out market research, spreading technical information and targeted communication. However, the score obtained by this factor was 1.8 due to the wrong policy adopted that prevents customer retention.

Overall, the analysis of the results pointed out that on line companies aim at spreading their brand name without focusing on customer retention or product sale (Table 1).

Table 1. 7C evaluation scale from 0 to 5

Categories	Mean value
Content	
Site size	3,8
Updating frequency	1,9
Graphic quality	2,6
Context	
Institutional site	4,3
Commercial size	2,3
Choice	
Product range	3,2
Offer characterization	2,2
Comfort	
Accessibility	3,9
Surf-worthiness	2,1
Languages	1,1
Offer typology	1,6
Convenience	
Offer range	2,7
Advantages compared to the traditional	1,2
Customer service and support	
Information	3,9
Traceability	2,1
Claims	1,4
Customer satisfaction	1,2
Payment security	1,1
Community	
Customer retention	1,8
Links	2,9
Entertainment	3,4

Source: results processed out of direct surveys

Conclusion

Internet has created a quick selection mechanism of the offer, cutting out unprofessional competitors. For a successful competition in this new area of market it is necessary, based on the results of the realized research, at least to pay attention to and promote some essential initiatives:

a. to invest in site visibility, by means of advertisement and offline promotion, as many companies are already doing with a good turnover;
b. to target the right customers in order to better meet their needs by using the Internet, and in order to know and put them into the right category;
c. create a community where customers can share with their strategic partners, by integrating activities and supplying chains.

In this sense, we have to repeat that communities are a social phenomenon before being an economic one and can be useful from two points of view: the social one, based on shared values and one main explanation; the economic ones based on a business model that may take the economic value out of the relational one [10].

In order to exploit the web, it is necessary for all people involved to be flexible, including politics, especially in such a period characterized by this economic global crisis against which, it is very important to show courage by investing in innovative sectors such as ICT. This will reduce the cultural and structural gap typical of the Italian companies, southern SMEs above all, which include agri-food ones.

For this, it will be fundamental to refer to an active and interactive on line model to analyze and revise the company's business structure as a whole, to take into account the company's characteristics, in our case the specificity of agri-food products and the local size of it. In this way, a source of competitive advantages within a global context will be created.

Authorship statement

Author(s) confirms that the above named article is an original work, did not previously published or is currently under consideration for any other publication.

Conflicts of interest

We declare that we have no conflicts of interest.

References

[1] Assinform-School of Management. (2008). *Il Made in Italy e le tecnologie informatiche.* Milano: Politecnico di Milano.

[2] Baskerville, R. & Dulipovici, A. (2006). The theorical foundation of knowledge management. *Knoledge Mangement Research & Practice,* Vol. 4.

[3] Brush, G.J. & McIntosh, D. (2010). Factors influencing e-marketplace adoption in agricultural micro-enterprises. *International Journal of Electronic Business,* vol. 8, n. 4/5, p. 405-432.

[4] Bucca, M., Scuderi, A. & Sturiale, L. (2006). Metodologie di analisi delle strategie di web marketing delle imprese agroalimentari nelle Regioni dell'Obiettivo 1.

[5] Rivista di Economia Agro-Alimentare, n. 1, p. 101-125.

[6] Canavari, M., Pignatti, E. & Spadoni, R. (2008). Nuove dinamiche nel commercio dei prodotti agroalimentari: resistenze all'adozione dell'e-commerce nelle relazioni B2B. Proceedings of XVI Meeting SIEA, Trieste, 5-6 June.

[7] Di Vittorio, A. (2002). Innovazione tecnologica e informazione per le imprese. *Economia Italiana.* Banco di Roma, Rivista quadrimestrale, n. 1.

[8] EUROSTAT. (2010). Information Society Statistics [On line]. Available: http://epp.eurostat.ec.europa.eu/portal/page/portal/information_society/data/main _tables [Accessed: 31 March 2011].

[9] Ferrandinam, A. (2002). *Web Marketing Planning.* Milano: FrancoAngeli.

[10] Fritzm, M., Hausenm, T. & Schiefer, G. (2004). Development and development directions of electronic trade platforms in US and European Agri-food market: Impact on Sector organization. *International food and agribusiness management review,* n. 7.

[11] Mandelli, A. (1998). *Internet marketing.* Milano: McGraw Hill Italia.

[12] Neilson, L.C., Madill, J. & Haines, G.H. (2010). The development of ebusiness in wine industry SMEs: an international perspective. *International Journal of Electronic Business,* vol. 8, n. 2, p. 126-147.

[13] Netcomm, School of Management. (2008). *L'e-commerce B2c in Italia: una crescita che sfida la crisi.* Milano: Politecnico di Milano.

[14] OECD. (2008). ICT and Economic Growth - Evidence from OECD Countries, Industries and Firms. Office for the publications of the OECD, Paris.

[15] Osservatorio e-commerce B2c. (2010). *L'e-commerce B2c in Italia: riprende la crescita!,* Executive Summary of Report 2010. School of Management. Milano: Politecnico di Milano.

[16] Osservatorio Facebook. (2011). *Facebook in Italia* [On line]. Available at: http://www.vincos.it/osservatorio-facebook/ [Accessed: 10 April 2011].

[17] Porter, M.E. & Millar, V.E. (1985). How information gives you competitive advantage. *Harvard Business Review,* Boston, July.

[18] Scott, W.G., Murtula, M. & Stecco, M. (1999). Il Commercio elettronico. Verso nuovi rapporti tra imprese e mercati. Torino: ISEDI.

[19] Sturiale, L. (2000). Il commercio elettronico, vincoli ed opportunity con particolare riferimento al sistema agroalimentare. *Economia Agro-Alimentare,* Anno V, n. 1, p. 140-159.

[20] Sturialem L. & Scuderi, A. (2001). Business to Consumer E-Commerce: problems and opportunities for some typical local products of the "Mezzogiorno " of Italy, Proceedings of the 4th International Symposium AIEA "Perspectivies of the agri-food system in the new millennium", Bologna (Italy), 5-8 September 2001.

[21] Vescovi, T. & Issepon, M. (2002). L'evoluzione di Internet come strumento di comunicazione e di marketing nelle imprese minori. *Micro & Macro Marketing,* n.3.

[22] Waverman, L. & Dasgupta, K. (2010). *Connectivity Scorecard. Research Results 2010* [On line]. Available at: http://www.connectivityscorecard.org/imges/ uploads/media/the connectivity Report 2010.pdf [Accessed: 1 April 2011].

Submitted: April 19, 2013.
Accepted: June 16, 2013.

Software Simulations Usage in Business Decision Making Education

Marko Marković[1], Katarina Plečić[2]

[1]*Singidunum University Faculty of Business Valjevo, mmarkovic@singidunum.ac.rs*

[2]*Singidunum University Faculty of Business Valjevo, kplecic@singidunum.ac.rs*

Case study

DOI: **10.7251/JIT1301051M** UDC: **005.52:004.738.5**

Abstract: Because of great importance in improving business decision making teaching process in educational institutions, a large number of software simulators are developed. Based on that information, it was necessary to present simulations as one of the most modern educational solutions, with possibilities of their usage. The basic features of a software system developed to support the teaching of business decision making and machine learning algorithms used in this field at the the Singidunum University Faculty of Business Valjevo, have been presented in the paper.

Keywords: software business simulations, business decision making, machine learning

Introduction

Nowadays, modern management is unimaginable without business decision making process. Information technology usage is considered as a mandatory tool for that purposes. As interest in this field rapidly grows, more attention has been devoted to its usage in educational purpose. Techniques for effortless learning are being developed and software systems are one of them. Usage of this kind of software in education is covered in detail in this paper - to be precise, software business simulations are the main focus in the research. Usage of these educational tools is popular because it enables users to maintain active approach to learning process from controlled and safe environment.

Software simulations make possible usage of real world situations with strictly defined roles for each user in data-rich environment which helps out business decision making process. In this manner, it is possible to get practical insight in modern company's ways of functioning.

Because of mentioned advantages in software simulations usage, business decision algorithm simulation system (original abbr. SAPO) has been developed at the Singidunum University Faculty of Business Valjevo. This software has been presented in this paper. The SAPO system is designed to generate student interest in business decision-making and allow them to further improve their knowledge of this subject matter.

The paper is organized as follows: Information technology and modern business decision making, Software business simulations in business decision making, Description of the software simulator developed at the Faculty of business Valjevo and Conclusion.

Information Technology And Modern Business Decision Making

Decision making is a part of everyday life. Some decisions have exceptionally big importance (e.g. important business decisions), while others are quite simple, for example, what to eat for dinner. Rational

thinking says that we should devote more time to important decisions, but that is not always the case because decision making is not a rational process by default. There is no way to avoid feeling of regret after making wrong decisions – that is something that each one of us felt at some point. Experienced decision-makers take advantage from wrong decisions - they learn from them.

Many human and every engineering activities have direct or indirect economic goals. Those goals are associated with decision making processes. Because of that, these processes are studied at many universities and big companies. [1]

Information technology role in modern business decision making

It is hard to make good decisions without good data which is necessary in every phase and for every activity in business decision making. If data is processed manually, process would last too long but, mostly, data is necessary in very short terms. Because of that, information technology is gaining importance as an important tool in decision making.

Modern management relies on technology usage. Great amount of data is collected from business transactions. In order to adapt those data for decision making process, data mining techniques are used. These techniques are based on a computer oriented searching and analyzing data in order to find usable patterns. These patterns present new knowledge which improves marketing and sales activities, customer relationship management and decision making. As follows, it is possible to get strategically important data about customers and their interests. For the searching purposes, machine learning algorithms are used.

Companies go even further in collecting customer data so, for example, when purchasing something, information about product that customer ordered is saved, together with order size, purchasing period, customer's interests etc. Online transactions can give even more information about customer and his personal habits during online shopping. Series of purchase, financial history and other personal data are a few mouse clicks away. First step in data mining process is to collect this kind of customer data, whether their source is internet transaction, purchase in the store, or other sources of information about the customer.

Software Business Simulations In Business Decision Making

Business software simulations history

Business simulations usage has been constantly growing, since the mid 1950s. Today, this teaching method has reached a high usage level at many universities. Although there are records of fighting games in China, 3,000 BC, first modern business simulation was presented in 1955. That was *Monopologs* simulation exercise, developed by the Rand corporation. It was focused on U.S. Air Force logistics support system. User's task was to manage the supply chain, and it was similar by structure to what modern solutions in this field offer. [2]

The rapid increase of business simulations happened between 1958 and 1961. It is estimated that over 100 simulations were developed untill 1961. They were used by more than 30,000 executives from different companies. The number of simulations has increased to about 200 until the 1969. The continuing increase in that time pointed to the growing popularity of this area. [3]

Development of the simulation field in education leads to a higher demand for more complex solutions. As a result, there are numerous models for different areas today and increasing number of educational institutions which are trying to provide practical approach to learning in this way.

Software simulations usability

Simulation is defined as an interactive abstraction of real life, or like any attempt to emulate an environment or system. [4] Practically, simulations present exercises within certain knowledge, skills and strategies that must be applied in order to fulfill certain tasks. They present open-ended games within which users are going through a particular situation using

a number of variables. It is necessary that every user takes a certain role, examines certain states, threats and problems and makes decisions based on that. It is also possible to notice effects of every decision that is made. The simulation can be carried out in various directions, depending on the user's decisions.

Simulations are especially useful in explaining complex business situations that can occur, because they are *active* educational tool. They present controlled environment with no forfeiture risk. Thanks to that, students can understand relationships between their decisions and effect on functional areas within the company.

Important characteristics of visual simulations are: [5]

- implementation of an adequate model of real-world situations which participant is faced with;
- defined roles for each participant, with identified responsibilities and limitations;
- data-driven environment that enables users to perform the range of strategies, from very broad to very sophisticated defining of business decisions;
- statement of changes as consequences of actions that participants undertook.

With the appropriate use, simulations present extraordinary tool for e-learning, which forms the basis of modern education. In this way, it is possible to stimulate students to be more actively involved, with the abillity to learn from personal experience. Essentially, they have the possibility to explore real situations that they can expect in the workplace. During the work in simulated environment, teacher is having an exact insight in all activities. This allows him to assist participants as they encounter a problem.

Visual software simulations importance in business decision making

There is an ancient Chinese proverb that says: "Tell me and I will forget, show me and I may remember, involve me and I will understand". This claim is especialy true in the field such as decision making. Participants could understand how certain business decision making algorithm works if they read from the book, or see the algorithm on the board. But if they have the possibilty to try it out, then they can understand much easier and faster.

There are numerous benefits of using visual software simulations in education: [6]

- an interesting way of learning because students can gather and examine data while working with the simulation;
- speeding up the learning process by actively engaging participants;
- combine knowledge from different fields;
- strongly motivating participants towards active learning instead of passive listening;
- interactive character of simulation that enables participants to inspect results of their decisions.

Today, simulations have very important role in education. One of the leading educational and scientific computing societies, ACM, recommends the usage of an appropriate software in laboratory exercises, especially in computer engineering field, as a very important way of allowing students to follow, explore and handle characteristics and behaviours of devices, systems and processes. The use of applications and simulations is recommended in modeling and analyzing real systems which are not practical for the physical implementation. [7] Suitable area for this application is also decision making, so that all of the allegations related to the computer engineering and simulations usage can be applied in this case.

Description of the Software Simulator Developed at the Faculty of Business Valjevo

The SAPO software system uses broad-based algorithms which are expected to best assist students in their studies. The selection of the algorithms takes into account the recommendations of the IEEE International Conference on Data Mining held in 2006 [8]. Based on the recommendations, the following algorithms are chosen: decision trees (ID3), clustering (k-means), Naive Bayes and perceptron.

The system is divided into four logical units. The task of each module is to simulate a specific algo-

rithm, and the first step requires the user to select the desired one. Following selection, the appropriate working area is displayed along with the required toolbars. There are options which allow the user to gradually move through the algorithm - One step forward, One step backward, Go to the beginning and Go to the end.

The screen of the decision tree module is comprised of three blocks: a table containing attribute names and input data, messages about the execution of the algorithm, and a graphical display of the decision tree. Algorithm ID3 [9] is used to generate the decision three (Fig. 1). After the input dataset is entered, the values are stored in the corresponding table and options for moving through the algorithm become enabled. When the algorithm is started, the decision tree is displayed in a separate frame, while a message about each step appears in the frame on the right side.

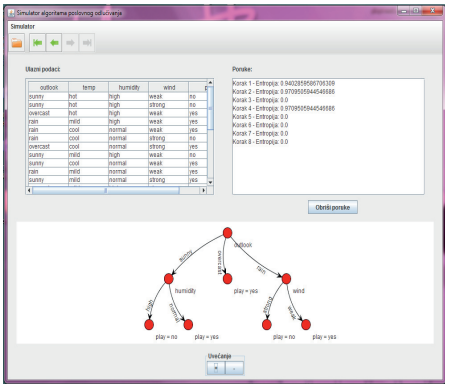


Fig. 1. Decision tree module layout

The name of the attribute is displayed next to each node, while the values of the attribute are shown next to the branches originating at that node. The tree leaves contain the decisions made by the decision tree. After a right click on any of the nodes, the context menu will display the information gain of each child node, showing how the algorithm has split the input dataset. It is possible to enlarge or reduce the tree, and to move it within the frame.

Similar to the decision tree simulation, the screen of the clustering module is comprised of three parts. The first part is used to manipulate the display of points and the history of centroid movement, the second writes messages, and the third draws points as well as clusters with corresponding centroids.

The k-means [10] algorithm is used in this simulator (Fig. 3). Before the algorithm is started, certain parameters need to be adjusted, such as: the initial number of points, the number of clusters, the dispersion of points and the display of history. Sliders are used to limit user input, as they are convenient for easier definition of the values which the user may input. It is important to note that the number of clusters may not be greater than the number of points. If such parameter selection is attempted, a warning message will be displayed. If the history display option is selected, the current centroid and all previous positions connected by lines will be displayed to show the trajectory generated by the centroid.

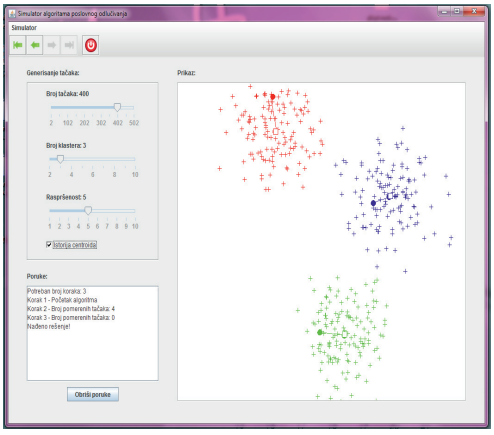


Fig. 3. Clustering module layout

A random function is used to generate random points, but with a fixed seed. This ensures that the same selected numbers of points and clusters, and dispersions, always yield identical positions of the points.

At the very beginning, upon initiation of the algorithm, the number of steps needed to arrive at the solution will be displayed. Then, the number of points that have moved in each pass is displayed and the points represented by different colors, depending on the cluster to which they belong.

The Naive Bayes [11] module is comprised of several principal parts: frames with input and test data, messages frame and graphical output of the algorithm (Fig. 4). To start this simulation, it is necessary to enter input data into the input data table. The table containing test data will include existing values of attributes in dropdown menus. The user can

select attributes from each of these menus and the algorithm will use them to compute probabilities. If any attribute is changed, the user needs to click on the Refresh test example button to remove the previous test example from the view and display a new example.

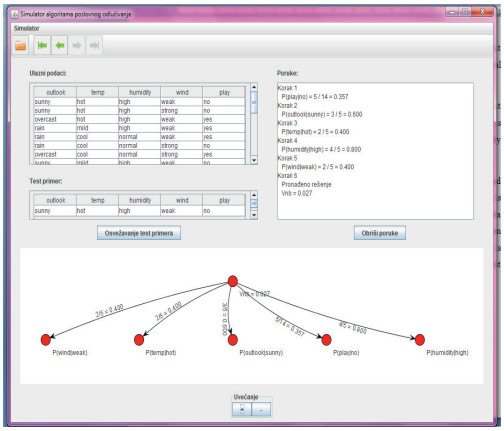


Fig. 4. Naive Bayes module layout

After selecting the desired test example, the algorithm can be started. At each step of the algorithm, the graphical display frame draws the nodes which represent conditional probabilities.

Each leaf shows which conditional probability it represents, while the branch that connects it to the root shows the value of that conditional probability as the number of the corresponding examples divided by the total number of examples. The destination probability is in the tree root, denoted by VNB. While the algorithm is running, the input data table highlights the rows being computed in each steps. Each step is explained in detail in the messages frame.

The screen of the perceptron [12] module is comprised of an input parameter adjustment screen, an input data table, a messages screen, and a graphical display of the perceptron (Fig. 5). The parameters frame allows the initial values of the weights (w1 and w2), the learning rate, the perceptron threshold and the maximum number of iterations of the program to be set. The input table uses a binary function to simulate basic Boolean operations. There are two inputs and one output. The value of the output may be varied by means of a dropdown menu; the allowed values are 0 and 1.

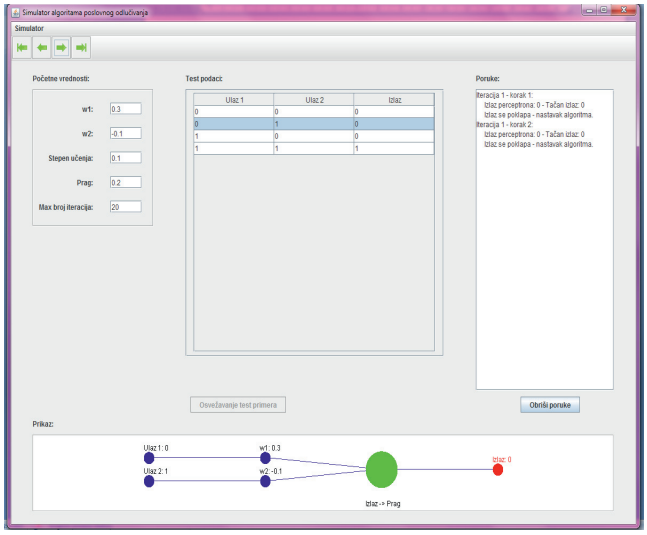


Fig. 5: Perceptron module layout.

The algorithm processes the input data table row by row, and conveys the values to the perceptron. The row currently processed is highlighted. The perceptron receives the values and computes the output. The input values, the weights, the sum of the input values and weights, the threshold and the output are displayed. For better organization and ease of understanding, the various parts of the figure are shown in different colors.

At each step, a textual output from the program is displayed in the messages frame, including the current iteration, the step in that iteration, and indication whether the perceptron output matches the desired output. If there is no match, explanation is provided about how weight changes are computed and what their values are.

Conclusion

In this paper, an attempt is made to better understanding of visual software simulations in business decision making. Nowadays, business decision making is a subject matter at numerous universities. Also, modern business organizations would not be possible without it.

Visual software solutions attain education quallity and better understanding of topics, and they are consequently an option for understanding of this field.

Because of that, as a solution for beter understanding of this field, software simulations are used. They make possible further improvement of education quality and understanding of discussed topics. It is possible to learn from personal experience while working in safe environment.

Since 1950s, software simulations have gained high popularity and they are extensively used in education today. Many universities use these solutions for practical training. Thus, possibility is made for students to try out situations that they can get into after finding a job. This possibility is very important for company, considering that making wrong decisions can cause serious consequences.

As an example of simulations usage, a software system developed at the Singidunum University Faculty of business Valjevo has been presented. The SAPO system allows its users to see how business decision-making and artificial intelligence algorithms are used. It allows for the input dataset to be assigned, the selected algorithm to be applied to this dataset, and then the execution to be monitored step by step. During the simulation, in order to better understand how it works, detailed information is displayed about the current stage of the algorithm. SAPO system can be used as a tool to accelerate learning and test assimilated knowledge.

Authorship statement

Author(s) confirms that the above named article is an original work, did not previously published or is currently under consideration for any other publication.

Conflicts of interest

We declare that we have no conflicts of interest.

Literature

[1] Čupić, M. & Suknović, M. (2010). Odlučivanje, Fakultet organizacionih nauka, Beograd.

[2] Faria, J.A. & Nulsen, R. (1996). Developments in Business Simulation & Experiental Exercieses, Volume 23, University of Windsor, Xavier University.

[3] Faria, J.A. (1990). Business Simulation Games After Thirty Years, Guide to Business Gaming and Experiental Learning, Nichols Pub Co.

[4] Gibson, D., Aldrich, C. & Prensky, M. (2007). Games and Simulations in Online Learning, Information Science Publishing, Hershey.

[5] Gredler, E.M. (2004). Games and Simulations and their Relationships to Learning, Handbook of Research on Educational Communications, Lawrence Erlbaum Associates Publishers, Mahwah, NJ.

[6] Wawer, M., Milosz, M., Muryjas, P. & et al. (2010). Business Simulation Games in Forming of Students' Enterpreneurship, International Journal of Euro-Mediterranean Studies, Volume 3, EMUNI University, University of Nova Gorica, Portorož.

[7] http://www.acm.org/education/education/curric_vols/CE-Final-Report.pdf, date accessed: 23.9.2012.

[8] Wu, X. et al. (2007). Top 10 algorithms in data mining, Springer-Verlag, London.

[9] Quinlan, R. (1986). Machine Learning, Kluwer Academic Publishers, Boston.

[10] MacQueen, J.B. (1967). Some Methods for classification and Analysis of Multivariate Observations, Proceedings of 5th Berkeley Symposium on Mathematical Statistics and Probability, University of California Press.

[11] Duda, R.O. & Hart, P.E. (1973). Pattern classification and scene analysis, Wiley.

[12] Rosenblatt, F. (1957). The perception: A perceiving and recognizing automaton. Report 85-460-1, Project PARR, Cornell Aeronautical Laboratory.

Submitted: May 24, 2013.
Accepted: June 16, 2013.

INSTRUCTIONS FOR AUTHORS

The *Journal of Information Technology and Application (JITA)* publishes quality, original papers that contribute to the methodology of IT research as well as good examples of practical applications.

Authors are advised that adherence to the Instructions to Authors will help speed up the refereeing and production stages for most papers.

- Language and presentation
- Length of submissions
- Submission
- Contact details/biographies
- Title of the paper
- Abstract and keywords
- Figures and tables
- Sections
- Footnotes
- Special characters
- Spelling
- References
- Proofs
- PDF offprint
- Copyright and permissions
- Final material
- Correspondence
- Publication ethics

LANGUAGE AND PRESENTATION

Manuscripts should be written in English. All authors should obtain assistance in the editing of their papers for correct spelling and use of English grammar. Manuscripts should have double spacing, with ample margins and pages should be numbered consecutively. The Editors reserve the right to make changes that may clarify or condense papers where this is considered desirable.

LENGTH OF SUBMISSIONS

Papers should not normally exceed 12 Journal pages (about 8000 words). However, in certain circumstances (e.g., review papers) longer papers will be published.

SUBMISSION

Manuscripts must be submitted through the JITA online submission system.

Please read the instructions carefully before submitting your manuscript and ensure the main article files do not contain any author identifiable information.

Although PDF is acceptable for initial submission original source (i.e. MS Word) files will be required for typesetting etc.

CONTACT DETAILS/BIOGRAPHIES

A separate file containing the names and addresses of the authors, and the name and full contact details (full postal address, telephone, fax and e-mail) of the author to whom correspondence is to be directed should be uploaded at the time of submission (you should select Contact details/Biographies as the file type). This file is not shown to reviewers. This file should also contain short biographies for each author (50 words maximum each) which will appear at the end of their paper.

The authors' names and addresses must not appear in the body of the manuscript, to preserve anonymity. Manuscripts containing author details of any kind will be returned for correction.

TITLE OF THE PAPER

The title of the paper should not be longer than 16 words.

ABSTRACT AND KEYWORDS

The first page of the manuscript should contain a summary of not more than 200 words. This should be self-contained and understandable by the general reader outside the context of the full paper. You should also add 3 to 6 keywords.

FIGURES AND TABLES

Figures which contain only textual rather than diagrammatic information should be designated Tables. Figures and tables should be numbered consecutively as they appear in the text. All figures and tables should have a caption.

SECTIONS

Sections and subsections should be clearly differentiated but should not be numbered.

FOOTNOTES

Papers must be written without the use of footnotes.

SPECIAL CHARACTERS

Mathematical expressions and Greek or other symbols should be written clearly with ample spacing. Any unusual characters should be indicated on a separate sheet.

Spelling

Spelling must be consistent with the Concise Oxford Dictionary.

References

References in the text are indicated by the number in square brackets. If a referenced paper has three or more authors the reference should always appear as the first author followed by et al. References are listed alphabetically. All document types, both printed and electronic, are in the same list. References to the same author are listed chronologically, with the oldest on top. Journal titles should not be abbreviated.

Journal

Avramović ZŽ (1995) Method for evaluating the strength of retarding steps on a marshalling yard hump. *European Journal of Operational Research*, 85(1), 504–514.

Book

Walsham G (1993) Interpreting Information Systems in Organizations. Wiley, Chichester.

Contributed volume

Huberman AM and Miles MB (1994) Data Management and analysis methods. In Handbook of Qualitative Research (Denzin NK and Linkoln YS, Eds), pp 428-444, Sage, Thousand Oaks, California.

Conference Paper

Huberman AM and Miles MB (1994) Data Management and analysis methods. In Handbook of Qualitative Research (Denzin NK and Linkoln YS, Eds), pp 428-444, Sage, Thousand Oaks, California.

Unpublished reports/theses

Nandhakumar JJ (1993) The practice of executive information systems development: and in-depth case study. PhD Thesis, Department of Engineering, University of Cambridge.

Proofs

Proofs of papers will be sent to authors for checking. Alterations to diagrams should be avoided where possible. It will not be possible to accept major textual changes at this stage. Proofs must be returned to the publishers within 48 hours of receipt by fax, first-class post, airmail or courier. Failure to return the proof will result in the paper being delayed.

PDF offprint

Corresponding authors will receive a PDF of their article. This PDF offprint is provided for personal use. It is the responsibility of the corresponding author to pass the PDF offprint onto co-authors (if relevant) and ensure that they are aware of the conditions pertaining to its use.

The PDF must not be placed on a publicly-available website for general viewing, or otherwise distributed without seeking our permission, as this would contravene our copyright policy and potentially damage the journal's circulation. Please visit **http://www.apeiron-journals.com/JITA/authors/rights_and_permissions.html** to see our latest copyright policy.

Copyright and permissions

The copyright of all material published in the Journal is held by Paneuropean University APEIRON. The author must complete and return the copyright form enclosed with the proofs.

Authors may submit papers which have been published elsewhere in a foreign language, provided permission has been obtained from the original publisher before submission.

Authors wishing to use material previously published in JITA should consult the publisher.

Final material

All final material must be submitted electronically in its original application format (MS Word is preferred). The file must correspond exactly to the final version of the manuscript.

Correspondence

Business correspondence and enquiries relating to advertising, subscriptions, back numbers or reprints should be addressed to the relevant person at:

Paneuropean University APEIRON
Journal JITA
Pere Krece 13, P.O.Box 51
78102 Banja Luka
Bosnia and Hercegovina / RS

Publication ethics

We take an active interest in issues and developments relating to publication ethics, such as plagiarism, falsification of data, fabrication of results and other areas of ethical misconduct. Please note that submitted manuscripts may be subject to checks using the corresponding service, in order to detect instances of overlapping and similar text.

JITA

PUBLISHER
Paneuropean University APEIRON,
College of Information Technology
Banja Luka, Republic of Srpska, B&H
www.apeiron-uni.eu
Darko Uremović, Person Responsible for the Publisher
Aleksandra Vidović, Editor of University Publications

ISSN 2232-9625
9 772232 962005