

Journal of Information Technology and Applications (BANJA LUKA)



Exchange of Information
and Knowledge in Research



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

 ebscobase.com	 crossref.org
 indexcopernicus.com	 road.issn.org
 citefactor.org/contact	 citefactor.org
 scholar.google.com	 cosmosimpactfactor.com
 doisrpska.nub.rs	

Printed on acid-free paper

Full-text available free of charge at <http://www.jita-au.com>

CONTENTS

TIME COMPLEXITY ANALYSIS OF THE BINARY TREE ROLL ALGORITHM	53
<i>ADRIJAN BOŽINOVSKI, GEORGE TANEV, BIJANA STOJČEVSKA, VENO PAČOVSKI, NEVENA ACKOVSKA</i>	
MANET vs. ZIGBEE: SOME SIMULATION EXPERIMENTS AT THE SEAPORT ENVIRONMENT	63
<i>SANJA BAUK, DIEGO GARCIA GONZALEZ, ANKE SCHMEINK, ZORAN Ž. AVRAMOVIĆ</i>	
BIOMETRIC SYSTEM TO SECURE THE INTERNET OF THINGS	73
<i>OLJA LATINVIĆ</i>	
FRAMEWORKS FOR AUDIT OF AN INFORMATION SYSTEM IN PRACTICE	78
<i>DALIBOR DRLJAČA, BRANKO LATINVIĆ</i>	
USING OPEN SOURCE SOFTWARE FOR WEB APPLICATION SECURITY TESTING	86
<i>KSENIJA ŽIVKOVIĆ, IVAN MILENKOVIĆ, DEJAN SIMIĆ</i>	
THE IMPACT OF FELDER'S LEARNING STYLES INDEX ON MOTIVATION AND ADOPTION OF INFORMATION THROUGH E-LEARNING	93
<i>ŽELJKO PEKIĆ, SRĐAN JOVANOVIĆ, NAĐA PEKIĆ</i>	
INSTRUCTIONS FOR AUTHORS	101

EDITORS:



**GORDANA
RADIĆ, PhD**
EDITOR-IN-CHIEF



**ZORAN
AVRAMOVIĆ, PhD**



**DUŠAN
STARČEVIĆ, PhD**

The content of this issue of JITA journal consists of six papers covering different areas of information processing.

In the first paper, entitled “**Time Complexity Analysis of the Binary Tree Roll Algorithm**”, by Adrijan Božinovski, George Tanev, Biljana Stojčevska, Veno Pačovski and Nevena Ackovska outline the time complexity analysis of the Binary Tree Roll algorithm. The time complexity is analyzed theoretically and the results are then confirmed empirically. The theoretical analysis consists of finding recurrence relations for the time complexity, and solving them using various methods. The empirical analysis consists of exhaustively testing all trees with given numbers of nodes n and counting the minimum and maximum steps necessary to complete the roll algorithm. The time complexity is shown, both theoretically and empirically, to be linear in the best case and quadratic in the worst case, whereas its average case is shown to be dominantly linear for trees with a relatively small number of nodes and dominantly quadratic otherwise.

The second paper, “**MANET vs. ZigBee_Some simulation experiments at the seaport environment**”, by Sanja Bauk, Diego Garcia Gonzalez, Anke Schmeink, Zoran Ž. Avramović, presents the results of some OPNET simulation experiments realized with an aim to benchmark MANET and ZigBee networks’ performances at the seaport environment. The MANET is formed among workers’ and supervisors’ personal digital assistants. On the other side, the ZigBee is established between end-nodes or employees’ body central units, which collect signals from several active and passive devices embedded into ID badges and personal protective equipment pieces; several moving and fixed routers; and the coordinator mounted at the appropriate seaport location.

The third article “**Biometric system to secure the Internet of Things**”, by Olja Latinović puts the focus on Security of Internet of Things by the biometrics system. Suggested system is easy way to secure authentication. This process is established on biometric feature matching and sink in IoT nodes which provide stable security system.

The fourth paper “**Frameworks for audit of an information system in practice**”, by Dalibor Drljača and Branko Latinovic, introduces new model of processing and selling insurance over the Internet. The new model has been developed with the aim to eliminate imperfections of the previous processing system having in mind that most of the current models of selling insurances contain manual processing.

In the fifth paper “**Using open source software for web application security testing**”, by Ksenija Živković, Ivan Milenković, and Dejan Simić, non-functional testing of web applications using software tools is presented. The importance of web application testing is correlated with the increase of hacker attacks. First part of this paper describes the process of application testing. After that, two available software tools for non-functional application testing, Vega and ZAP, are described. Detailed analysis of a case study is given in the remaining part of this paper. In the case when application contains confidential data, testing should be done with extreme care, because unidentified problems can have serious financial, legal or reputation consequences for organization.

In the last paper “**The impact of index Felder learning styles for adoption information through e-learning**”, by Željko Pekić, Srđan Jovanovski and Nađa Pekić, the nature and distribution (direction and intensity) of motivation for using e-learning, focusing the connection between the independent variables on one side and the Felder’s learning style on the other is examined. The most relevant information that was examined and presented is the individual ways of the respondents in adopting the same material. The paper also deals with the ways to technically adjust the information delivery. The results confirm the statistical significance of the initial idea. These data leave place for further research in the same and similar fields.

TIME COMPLEXITY ANALYSIS OF THE BINARY TREE ROLL ALGORITHM

Adrijan Božinovski¹, George Tanev¹, Biljana Stojčevska¹, Veno Pačovski¹,
Nevena Ackovska²

¹*School of Computer Science and Information Technology, University American College Skopje,
Macedonia*

²*Faculty of Computer Science and Engineering, University "Sv. Kiril i Metodij", Skopje, Macedonia*
bozinovski@uacs.edu.mk, george.tanev@uacs.edu.mk, stojcevska@uacs.edu.mk, pachovski@uacs.edu.
mk, nevena.ackovska@finki.ukim.mk

Contribution to the state of the art

DOI: 10.7251/JIT1602053B

UDC: 519.857:004.021

Abstract: This paper presents the time complexity analysis of the Binary Tree Roll algorithm. The time complexity is analyzed theoretically and the results are then confirmed empirically. The theoretical analysis consists of finding recurrence relations for the time complexity, and solving them using various methods. The empirical analysis consists of exhaustively testing all trees with given numbers of nodes and counting the minimum and maximum steps necessary to complete the roll algorithm. The time complexity is shown, both theoretically and empirically, to be linear in the best case and quadratic in the worst case, whereas its average case is shown to be dominantly linear for trees with a relatively small number of nodes and dominantly quadratic otherwise.

Keywords: Binary Tree Roll Algorithm, time complexity, theoretical analysis, empirical analysis.

INTRODUCTION

Binary Tree Roll is an operation by which all of the nodes of a binary tree are rearranged in such a way, so that two of the depth-first traversals of the newly obtained binary tree yield the same results as other two traversals of the original binary tree. The graphical representation of the newly obtained binary tree is that it appears to be rolled at a 90 degree angle (either counterclockwise or clockwise, depending on the direction of the applied roll operation) relative to the original binary tree; hence the name "Binary Tree Roll".

This operation was introduced and defined in [1]. There are two variants of the Binary Tree Roll Operation: a counterclockwise (CCW) and a clockwise (CW) roll. The counterclockwise roll of a binary tree, abbreviated as $CCW()$, is defined as follows. Given two binary trees T_1 and T_2 , as well as their respective $preorder()$, $inorder()$ and $postorder()$ traversal functions, operation $CCW()$ is defined as in Definition 1:

$$CCW(T_1) = T_2 \Leftrightarrow (preorder(T_1) = inorder(T_2) \wedge inorder(T_1) = postorder(T_2)) \quad (1)$$

In other words, upon $CCW()$, the preorder traversal of the original tree is identical to the inorder traversal of the tree obtained by the counterclockwise roll, and the inorder traversal of the original tree is identical to the postorder traversal of the tree obtained by the counterclockwise roll.

Likewise, the clockwise roll of a binary tree, abbreviated as $CW()$, is defined as in Definition 2:

$$CW(T_1) = T_2 \Leftrightarrow (inorder(T_1) = preorder(T_2) \wedge postorder(T_1) = inorder(T_2)) \tag{2}$$

Similarly, upon $CW()$, the inorder traversal of the original tree is identical to the preorder traversal of the tree obtained by the clockwise roll, and the postorder traversal of the original tree is identical to the inorder traversal of the tree obtained by the clockwise roll.

A graphical explanation was given in [1], showing how the resulting binary tree is obtained visually, so as to comply with definition (1) or (2), depending on the direction of the roll. The downshift visual operation, illustrated in Figure 1, was also presented. It was shown that $CCW()$ and $CW()$ are inverses of each other, and algorithms for $CCW()$ and $CW()$ were given, which didn't require obtaining the traversals of the input tree in order to generate the rolled tree.

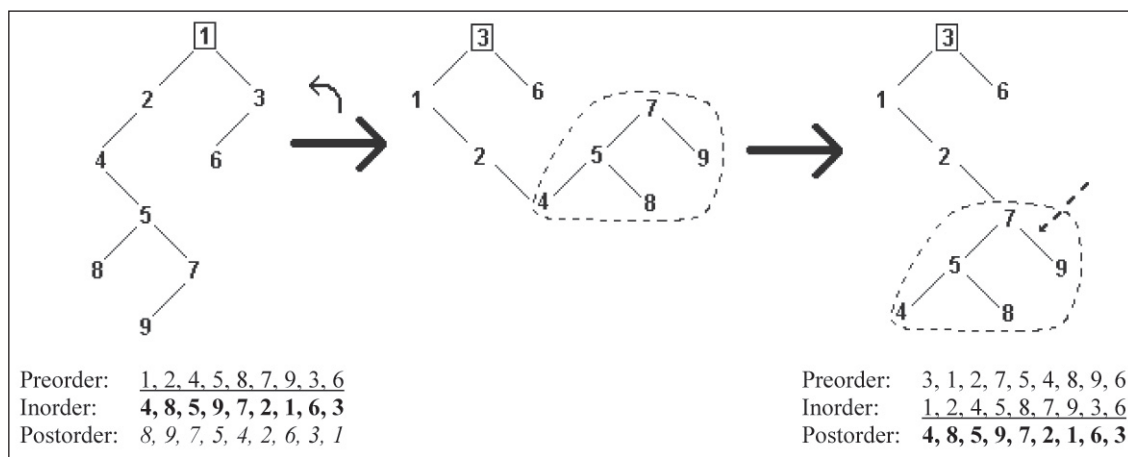


Figure 1. Graphical explanation of the $CCW()$ algorithm, and an example of a downshift [1]

Structurally, the algorithm presented in [1] contains a trivial case, two basic cases, and a third, more complex one. The pseudocode for both the $CCW()$ and $CW()$ variations of the algorithm are shown in Figure 2.

The algorithm takes two input parameters, which represent two binary tree nodes: the `root` of the tree to be processed, and its `predecessor`. The predecessor's initial value is always `NULL`, since the root of the input tree never has a predecessor node. However, the value of the `predecessor` parameter changes as further recursive calls to the algorithm are being invoked from inside the function itself. Moreover, the values of both the `root` and the `predecessor` nodes are guaranteed to change within subsequent recursive function calls, since the entire structure of the binary tree is rearranged after the roll operation executes fully.

The motivation for this paper was the fact that the binary tree roll algorithm, in either its $CCW()$ or $CW()$ variant, has not been analyzed for time complexity so far. That is the goal of this paper and it will be done as follows, focusing on the $CCW()$ variant. First, a theoretical analysis of the time complexity will be given, treating all cases of the algorithm execution. Recurrence relations for the time complexity will be stated and proved using mathematical tools. Afterwards, it will be shown how those results are tested empirically, addressing the analytical results for the time complexities of the worst case, best case and average case of the algorithm. Finally, the paper will end with a conclusion about the material presented herein.

```

1.  CCW(&root, &predecessor)
2.  {
3.    if(root != NULL)
4.    {
5.      if(root.rSn == NULL)
6.      {
7.        root.rSn = root.lSn;
8.        root.lSn = NULL;
9.        CCW(root.rSn, root);
10.     }
11.    else
12.    {
13.      if(root.rSn.rSn == NULL)
14.      {
15.        root.rSn.rSn = root.rSn.lSn;
16.        root.rSn.lSn = root;
17.        root = root.rSn;
18.        root.lSn.rSn = root.lSn.lSn;
19.        root.lSn.lSn = NULL;
20.        if(predecessor != NULL)
21.          predecessor.rSn = root;
22.        CCW(root.lSn.rSn, root.lSn);
23.        CCW(root.rSn, root);
24.      }
25.    else
26.    {
27.      CCW(root.rSn, root);
28.      define leftmost = root.rSn;
29.      while(leftmost.lSn != NULL)
30.        leftmost = leftmost.lSn;
31.      leftmost.lSn = root;
32.      define newroot = root.rSn;
33.      root.rSn = NULL;
34.      root = newroot;
35.      if(predecessor != NULL)
36.        predecessor.rSn = root;
37.      CCW(leftmost.lSn, leftmost);
38.    }
39.  }
40. }
41. }

```

a)

```

1.  CW(&root, &predecessor)
2.  {
3.    if(root != NULL)
4.    {
5.      if(root.lSn == NULL)
6.      {
7.        root.lSn = root.rSn;
8.        root.rSn = NULL;
9.        CW(root.lSn, root);
10.     }
11.    else
12.    {
13.      if(root.lSn.lSn == NULL)
14.      {
15.        root.lSn.lSn = root.lSn.rSn;
16.        root.lSn.rSn = root;
17.        root = root.lSn;
18.        root.rSn.lSn = root.rSn.rSn;
19.        root.rSn.rSn = NULL;
20.        if(predecessor != NULL)
21.          predecessor.lSn = root;
22.        CW(root.rSn.lSn, root.rSn);
23.        CW(root.lSn, root);
24.      }
25.    else
26.    {
27.      CW(root.lSn, root);
28.      define rightmost = root.lSn;
29.      while(rightmost.rSn != NULL)
30.        rightmost = rightmost.rSn;
31.      rightmost.rSn = root;
32.      define newroot = root.lSn;
33.      root.lSn = NULL;
34.      root = newroot;
35.      if(predecessor != NULL)
36.        predecessor.lSn = root;
37.      CW(rightmost.rSn, rightmost);
38.    }
39.  }
40. }
41. }

```

b)

Figure 2. The algorithms for a) CCW() and b) CW()[1]

Time Complexity – Analytical Approach

Depending on the topology of the tree being processed by the roll algorithm, any one of the three cases is equally likely to be invoked (the ones initiated with lines 5, 13 and 25 in Figure 2, respectively). Therefore, the time complexity equation can be written as in Equation 3:

$$T(n) = \begin{cases} T_0(n) \\ T_I(n) \\ T_{II}(n) \\ T_{III}(n) \end{cases} \tag{3}$$

where $T_0(n)$, $T_I(n)$, $T_{II}(n)$, and $T_{III}(n)$ denote the trivial, first, second, and third case of the algorithm, respectively. The trivial case (line 3 in Figure 2) is always executed in constant time and produces no further recursive calls, yielding $T_0 = \Theta(1)$. The three non-trivial cases will be analyzed with the assumption that the trivial case is fulfilled. Furthermore, the number of nodes of the tree will be denoted by n , the line numbers will refer to the algorithm in Figure 2, and the recurrences obtained will be followed by the results obtained by solving those recurrences using the backward substitution method [4], or by the substitution method based on mathematical induction [3].

The analysis will be done upon the $CCW()$ version of the algorithm, i.e. it will concern Figure 2a. As stated in [1], the $CW()$ algorithm is an inverse of $CCW()$; substituting “left” for “right” and vice versa, as well as $CCW()$ for $CW()$ (for the recursive calls), will transform the $CCW()$ algorithm into the $CW()$ algorithm, so the following analysis can thus be used for the $CW()$ variant as well.

First case - lines 5-10

This case is invoked when the root has no right sub-tree (line 5). The following lines of code take the root’s left sub-tree and make it its right sub-tree. Then, a recursive call is made on the new right sub-tree. Figure 3 presents this case visually.

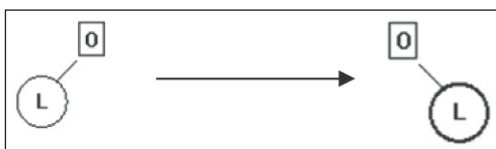


Figure 3. The first basic case in the $CCW()$ algorithm [1]

This case will yield a constant number of operations (two), as well as a recursive call invoked upon a tree containing $n - 1$ nodes (i.e. the root’s only sub-tree). Thus, the time complexity recurrence for the first case can be written as in Equation 4:

$$T_I(n) = 2c + T(n - 1) \tag{4}$$

where the $T(n - 1)$ recursive call implies that any one of the cases of the algorithm may be invoked, depending on the topology of the remainder of the

tree. Solving the recurrence results in a tightly linear complexity as stated in Equation 5.

$$T_I(n) = \Theta(n) \tag{5}$$

Second case - lines 11-24

This case is activated when the root of the tree has a right sub-tree, which does not have a right sub-tree of its own (line 13). There will be 6 or 7 operations needed to roll the root, its right child node, and their respective left sub-trees counterclockwise (6 if the root of the initial tree is rolled using this case, 7 if any sub-tree is rolled using this case), and two additional recursive calls on the two formerly left and ultimately right sub-trees. The number of constant operations can be denoted as Kc (where K is either 6 or 7) and will be included in the time complexity equation for the second case, shown visually in Figure 4.

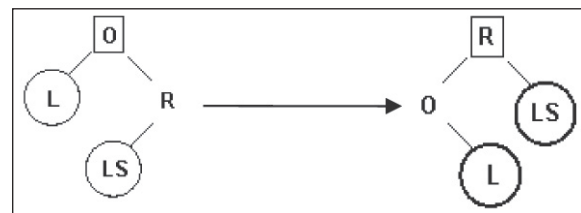


Figure 4. The second basic case in the $CCW()$ algorithm [1]

There are two recursive calls, so it is necessary to determine the extreme scenarios upon which they can potentially be invoked. In the worst-case scenario, all of the remaining nodes will be in one of the sub-trees, whereas the other one will remain empty. This scenario can be described as in Equation 6:

$$T_{II_0}(n) = Kc + T(n - 2) + T(0) \tag{6}$$

where the $T(n - 2)$ denotes that the two nodes already rolled with the constant number of lines (lines 15 to 20 or 21) will not be worked with again. Solving this recurrence gives a result of a tight linear complexity, as shown in Equation 7:

$$T_{II_0}(n) = \Theta(n) \tag{7}$$

The best-case scenario is when both of the sub-trees have an equal number of the remaining $n - 2$ nodes. This can be represented as in Equation 8:

$$T_{II_{\Omega}}(n) = Kc + 2T\left(\frac{n-2}{2}\right) \tag{8}$$

Solving this recurrence again yields a solution of tight linear complexity. This is shown in Equation 9:

$$T_{II_{\Omega}}(n) = \Theta(n) \tag{9}$$

Since both extreme scenarios of the second case have linear time complexities, it follows that the second case of the binary tree roll algorithm has tightly linear time complexity (Equation 10):

$$T_{II}(n) = \Theta(n) \tag{10}$$

Third case - lines 25-38

This case gets invoked when the root has a right sub-tree, which has a right sub-tree of its own. As stated in [1], this case deals with the downshift of stems of right child nodes and transforming them into stems of left child nodes. The algorithm first creates a recursive call upon the right sub-tree of the root and it continues to do so until a basic case is reached (i.e. until a sub-tree with at most one right child node is reached, following the stem of right child nodes from the root towards its rightmost child node). When such a case is handled by the algorithm, the remainder of the third case relocates the former root of the tree to be the “leftmost” child node in the newly rolled tree, and the procedure is then recursively invoked again on the former root (and its entire left sub-tree), now placed as the leftmost node in the sub-tree handled by the third case. Figure 5 shows the third case visually.



Figure 5. The third and most complex case in the CCW () algorithm [1]

How many times the loop in case 3 (lines 29 and 30) will be executed depends on the number of nodes in the stem of right child nodes of the root of the tree on which the CCW () algorithm is invoked, if the third case of the algorithm applies to it. After downshifting, this stem will become a stem of left

child nodes, and the root node will need to be linked as the left child node of the leftmost node in this stem. Since the rightmost node in the original tree will become the root of the new tree after CCW () is performed on it, finding the leftmost node will need to be done from the new root towards the left, which is the reason for the loop in lines 29 and 30 of the algorithm.

To help quantify this and precisely determine the time complexity of the third case of the algorithm, additional variables can be introduced. These are presented visually in Figure 6.

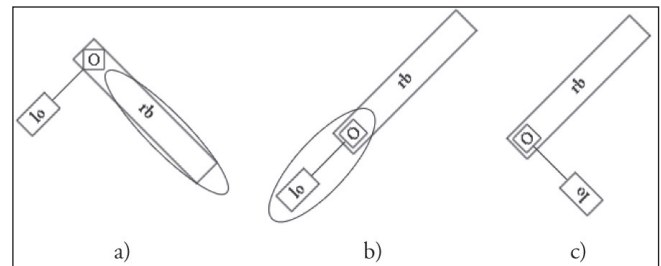


Figure 6. The third case of the CCW () algorithm: a) the head recursion (ellipse) of the third case deals with the stem of right child nodes () and transforms it into a stem of left child nodes via downshift; b) the root () is linked as the leftmost in the stem of left child nodes and the tail recursion (ellipse) of the third case is invoked upon it; c) since the former root does not have a right child node of its own, the tail recursion will invoke the first case, and the left sub-tree of the former root () will become its right sub-tree

As shown in Figure 6, *rb* represents the number of nodes in the stem of right child nodes of the root of the tree (including it), whereas *lo* is the number of nodes in the left sub-tree of the root. Having this in mind, the time complexity recurrence of the third case can be written as in Equation 11:

$$T_{III}(n) = T(n - 1 - lo) + 2c + 2c(rb - 2) + Pc + T(1 + lo) \tag{11}$$

where Constraints 12 and 13 apply:

$$3 \leq rb \leq n \tag{12}$$

$$0 \leq lo \leq n - rb \tag{13}$$

The five terms of the Equation 9 and the constraints in Equations 10 and 11 are explained as follows:

- $T(n - 1 - lo)$ is the head recursion of the third case (line 27). It will be invoked upon all of the nodes in the tree (n), except the root and its left sub-tree (lo), as shown in Figure 6a;
- $2c$ is the constant time needed to invoke the two lines of code 28 and 29;
- $2c(rb - 2)$ is the time needed to invoke the loop in lines 30 and 29 again (the loop condition test).

The two lines of code in the loop will be invoked for all nodes in the stem of right child nodes (turned into a stem of left child nodes after the downshift, i.e., after the head recursion has completed) except for two: the root (the head recursion, i.e., downshift, is invoked for the right child node of the root, meaning that the root does not become downshifted until all other nodes in the stem of right child nodes get downshifted) and the last node in the stem of right child nodes (because when the head recursion reaches the node which is a parent to the last node in the stem of right child nodes, the second basic case of the CCW (\cdot) will be invoked and not the third case, thus initiating the end of the downshift process). That is why this term is $2c(rb - 2)$.

The third case of the algorithm will be invoked only if the stem of right child nodes contains 3 or more nodes (which can be inferred by consecutively following the tests in lines 3, 5, 13 and 25); if it contains only 3 nodes, that is the best-case scenario, whereas if it contains all n nodes of the tree (i.e., the tree is right-degenerated), that is the worst-case scenario; hence Constraint 12;

- P is a constant which is either 5 or 6, depending on whether the third case of the algorithm is invoked upon the root of the tree (i.e., the node having no predecessor) or any other child node of the tree respectively—this signifies inclusion of lines 31 to 35 and 36, respectively;
- $T(1 + lo)$ represents the tail recursion, which is invoked on the former root of the tree (eventually placed as the leftmost node in the stem of downshifted left child nodes) and the nodes in its left sub-tree (lo), as shown in Figure 6b. In the best-case scenario, this left sub-tree will be empty, and in the worst-case scenario it will contain all the nodes of the tree except the ones contained in the initial stem of right child nodes (which includes

the root of the tree as well, as shown in Figure 6), from where Constraint 13 is derived.

In order to analyze Equation 11, the extreme scenarios for Constraints 12 and 13 need to be addressed. The worst-case scenario in Constraint 12 is when $rb = n$, i.e., when the stem of right child nodes contains all of the nodes of the tree (which means that the tree is right-degenerated). This means that there is no left sub-tree to the root, i.e., $lo = 0$, which can be inferred both logically and formally, by substituting $rb = n$ in Constraint 13. Thus, Equation 11 becomes Equation 14:

$$T_{\Omega_0}(n) = T(n - 1) + 2c + 2c(n - 2) + Pc + T(1) \quad (14)$$

Solving this recurrence yields a tightly quadratic complexity, as stated in Equation 15:

$$T_{\Omega_0}(n) = \Theta(n^2) \quad (15)$$

The best-case scenario occurs when the third case of the algorithm is invoked only once for the entire tree, i.e., when $rb = 3$ in Constraint 12. Substituting this in Equation 11 produces Equation 16:

$$T_{\Omega_1}(n) = T(n - 1 - lo) + 2c + 2c + Pc + T(1 + lo) \quad (16)$$

There are two extremes of the best-case scenario to consider:

- The first extreme is when $lo = 0$ in the constraint in Equation 11, which means that there is no left sub-tree to the root. Then, the head recursion would handle all of the nodes of the tree except the root (which are not in the left sub-tree of the root and do not form a stem of right child nodes), whereas the tail recursion would handle only the root; this can be inferred by substituting the aforementioned value for lo in Equation 16 and thus obtaining Equation 17:

$$T_{\Omega_1}(n) = T(n - 1) + 2c + 2c + Pc + T(1) \quad (17)$$

Solving the recurrence in Equation 17 results in a tightly linear complexity (since $T(1) = \Theta(1)$, i.e. it is a constant), as stated in Equation 18:

$$T_{\Omega_1}(n) = \Theta(n) \quad (18)$$

- The second extreme is when $lo = n - 3$ in Constraint 13, which means that the left sub-tree of the root contains all of the nodes of the tree, ex-

cept the three nodes (including the root) placed in the stem of right child nodes, which would invoke the third case of the algorithm. Thus, the head recursion would handle only two nodes (the lower two nodes of the stem of three right child nodes, handled by the second case), whereas the tail recursion would handle the remaining $n - 2$ nodes of the tree; this can also be inferred by substituting the aforementioned value for l_0 in Equation 16 and thus produce the recurrence in Equation 19:

$$T_{III\Omega_2}(n) = T(2) + 2c + 2c + Pc + T(n - 2) \quad (19)$$

Solving this recurrence again results in a tightly linear complexity (since, again, $T(2) = \Theta(1)$, i.e. it is also a constant), as stated in Equation 20:

$$T_{III\Omega_2}(n) = \Theta(n) \quad (20)$$

Thus, since both extremes of the best-case scenario for the third case have linear time complexities, the best-case scenario for the third case, as a whole, has linear time complexity, as stated in Equation 21:

$$T_{III\Omega}(n) = \Theta(n) \quad (21)$$

Comparing Equations 15 and 21, it can be seen that the third case of the algorithm is not robust, i.e. that its time complexity can range from quadratic in the worst case to linear in the best case. Assuming that all of the aforementioned cases of the algorithm (consisting of their worst- and best-case scenarios, including the extreme sub-variants) are equally likely to be invoked, one can undertake a probabilistic approach to the time complexity analysis. More specifically, the complexities of the following cases need to be considered: $T_I(n)$ (Equation 5), $T_{II_0}(n)$ (Equation 7), $T_{II\Omega}(n)$ (Equation 9), $T_{III_0}(n)$ (Equation 15), $T_{III\Omega_1}(n)$ (Equation 18) and $T_{III\Omega_2}(n)$ (Equation 20). It can be seen that, out of the six possible extreme cases that can arise during the processing of a random binary tree with the CCW () algorithm, only one is quadratic and all the others are linear. In other words, it can be assumed that, whenever a random tree is processed by the CCW () algorithm, five times out of six the algorithm will have a linear time complexity, and once out of six times it will have a quadratic time complexity.

Of course, this is a simplified model of the time complexity of the algorithm, and further research

into the topic is needed. Specifically, experimental research needs to be conducted, where the number of steps to execute the algorithm needs to be counted for certain topologies of the binary tree structure, in order to obtain a clear picture into the time complexity of the algorithm.

Time Complexity – Empirical Approach

It is reasonable to expect that not all topologies of binary trees with certain amounts of nodes will require the same amounts of time to have the binary roll operation fully performed on them. Figure 7 presents all possible topologies of binary trees for $n = 3$ and $n = 4$. For every binary tree with n nodes there are C_n possible binary tree topologies, where C_n is the n -th Catalan number.

Based on the equations for time complexity, a logical assumption would be that, for a tree with $n = 3$ nodes, one out of $C_3 = 5$ trees would need quadratic time complexity to have CCW roll performed on it (Figure 7a) — it would be the one containing three nodes in the stem of right child nodes, i.e. the topology of a right-degenerated tree. Also, for a tree with $n = 4$ nodes, four out of $C_4 = 14$ trees would need quadratic time complexity to have CCW roll performed on them (Figure 7b) — the ones that have stems of three and more right child nodes.

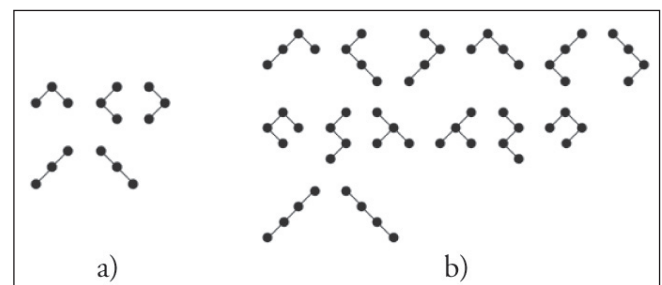


Figure 7. The topologies of binary trees for a) $n = 3$ and b) $n = 4$

In order to be certain about how much time is needed to perform CCW roll on a tree with n nodes, an exhaustive analysis needs to be performed. This includes obtaining all topologies of binary trees with n nodes and performing CCW roll on all of them, while counting the steps (i.e., time units) until the CCW roll completes. For this, it is necessary to first generate all topologies of binary trees for a

given n and then execute CCW roll on all of them, while counting the steps during the CCW roll executions. Following the theoretical analysis, it is expected that there will be a quadratic time complexity for the worst case and a linear time complexity for the best case, and it is therefore necessary to collect information for both. It is also appealing to know whether the time complexity of the algorithm would be more dominantly linear or quadratic, i.e., whether the best case or worst case of the algorithm would be more likely to be invoked during the execution of the CCW roll. For this reason, an average time complexity would also be extracted, as an average of the time complexities for all topologies of binary trees for a given number of nodes n .

In order to obtain all topologies of binary trees with a given number of nodes, the Catalan Cipher Vector approach is used in this paper. A Catalan Cipher Vector [2] is a vector which uniquely determines a binary tree's topology. For a tree with n nodes, there will be C_n topologies of binary trees and thus C_n Catalan Cipher Vectors. Table 1 shows all the ranks, their corresponding Catalan Cipher Vectors, and the appropriate binary trees, for $n = 4$ nodes.

Since the initial Catalan Cipher Vector for a tree with n nodes is always $[0\ 1\ 2\ \dots\ n - 1]$ [2], it is possible to generate the corresponding binary tree for it, and count the number of steps it would take to complete the $CCW()$ on it. Then, the subsequent Catalan Cipher Vector can be obtained, the corresponding binary tree can be generated from it, have $CCW()$ executed on it and count the number of steps needed and so on, until all C_n binary tree topologies are processed this way. Throughout the process, the maximum and the minimum number of steps needed are tracked, as well as the total number of steps for all the C_n topologies of the binary trees with n nodes. These can be plotted on a graph for different subsequent values of n , in order to provide a graphical representation of the best case, worst case and average case of the time complexity of the $CCW()$ algorithm, respectively.

The results for such an analysis have been performed and the results are given in Table 2.

Table 1. Ranks and enumerations of the binary trees with $n = 4$ nodes using the Catalan Cipher Vector approach

Rank	Catalan Cipher Vector	Binary Tree
0	[0 1 2 3]	
1	[0 1 2 4]	
2	[0 1 2 5]	
3	[0 1 2 6]	
4	[0 1 3 4]	
5	[0 1 3 5]	
6	[0 1 3 6]	
7	[0 1 4 5]	
8	[0 1 4 6]	
9	[0 2 3 4]	
10	[0 2 3 5]	
11	[0 2 3 6]	
12	[0 2 4 5]	
13	[0 2 4 6]	

Table 2. Numbers of steps necessary to perform $CCW()$ on all topologies of binary trees with given numbers of nodes

n	$C(n)$	Min	Max	Avg	$Total$
2	2	9	11	10	20
3	5	13	29	18	88
4	14	17	49	26	360
5	42	21	71	34	1.430
6	132	25	95	43	5.610
7	429	29	121	51	21.890
8	1.430	33	149	60	85.228
9	4.862	37	179	68	331.630
10	16.796	41	211	77	1.290.640
11	58.786	45	245	85	5.025.880
12	208.012	49	281	94	19.586.720
13	742.900	53	319	103	76.399.836
14	2.674.440	57	359	112	298.274.350
15	9.694.845	61	401	120	1.165.544.550
16	35.357.670	65	445	129	4.558.478.100
17	129.644.790	69	491	138	17.843.217.150
18	477.638.700	73	539	146	69.899.012.040
19	1.767.263.190	77	589	155	274.028.145.600
20	6.564.120.420	81	641	164	1.075.046.854.800

The results are interpreted as follows. In the first data row, for a tree with $n = 2$ nodes (first column), there are $C(n) = 2$ (second column) total topologies of binary trees. Executing $CCW()$ on all of them yields a *Total* (sixth, i.e. last column) of 20 time units, leading to an *Avg* (average – fifth column) of 10 time units per binary tree topology. Of all topologies, the *Min* (minimum – third column) number of time units necessary

to complete $CCW()$ on a binary tree topology with 2 nodes is 9, and the *Max* (maximum – fourth column) number of such time units is 11. This interpretation follows all rows of the table, up to and including binary tree topologies for $n = 20$ nodes.

Plotting the obtained data results in a chart like in Figure 8.

The results concur with the theoretical analysis: the algorithm has a quadratic time complexity in the worst case and a linear time complexity in the best case, whereas the average case has a near-linear complexity. It is possible to interpolate precise equations from the data for the worst and best case, and these are $T_{max}(n) = n^2 + 13n - 19$ and $T_{min}(n) = 4n + 1$, respectively.

For the average case, the most accurate interpolation is a quadratic one, since the plot indicates such a complexity, which is also confirmed using the least square error method. The equation thus obtained is $T_{avg}(n) = 0.0129n^2 + 8.3308n + 0.8554$. This shows that the quadratic term of the function will be shadowed by the linear term for smaller values of n , but that it would eventually become dominant when n grows beyond a certain threshold. The threshold would be the value of n for which the quadratic term becomes larger than the linear term, or the value of n for which $0.0129n^2 > 8.3308n$. This is true for $n > \frac{8.3308}{0.0129} \approx 645,798 \geq 646$, since n is an integer. In other words, for trees up to 645 nodes there is a higher probability that the $CCW()$ will perform a binary tree roll in linear time, whereas for trees with 646 and more nodes there is a higher probability that the $CCW()$ will perform binary tree roll in quadratic time.

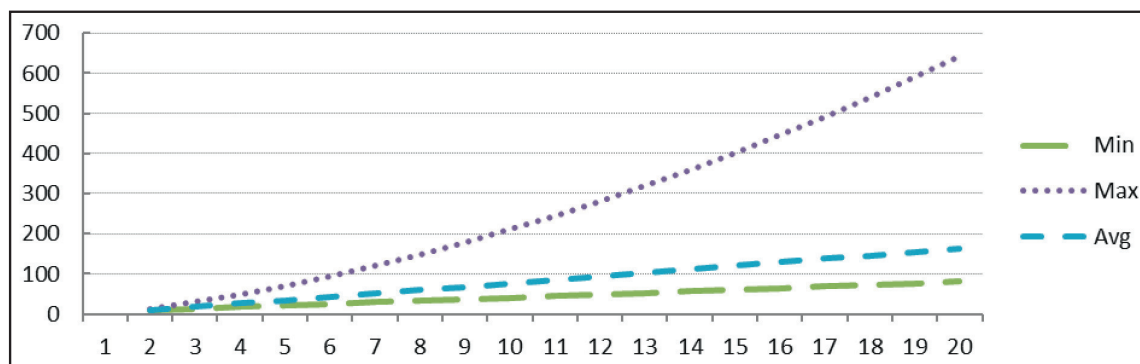


Figure 8. A plot of the results given in Table 2

CONCLUSION

This paper presented an analysis of the time complexity of the binary tree roll algorithm, specifically its counterclockwise (CCW ()) variant, with the note that the analysis for its clockwise (CW ()) variant is analogous. For the time complexity analysis, the trivial and the three non-trivial cases of the algorithm were presented and recurrence relations for them were derived and solved. The results from the theoretical analysis were checked empirically, by performing exhaustive testing on all trees with given numbers of nodes n , counting all the steps while performing the algorithm. The theoretical results, that the time complexity of the CCW () algorithm is linear in the best case and quadratic in the worst case, were confirmed by the empirical results. Furthermore, the average case analysis showed that the CCW () algorithm is dominantly linear for trees with $n \leq 645$, whereas for trees with higher numbers of nodes the quadratic time complexity becomes more dominant.

BIOGRAPHY

Adrijan Božinovski works as an Associate Professor at the School of Computer Science and Information Technology at University American College Skopje, where he is currently the Dean. He obtained his BSc from University "St. Cyril and Methodius" in Skopje, Macedonia, and his MSc and PhD from University of Zagreb, Croatia.

George Tanev is an MSc graduate student of the School of Computer Science and Information Technology at University American College Skopje, Macedonia, where he acquired his BSc in Computer Science. Also works as a software developer in Skopje, Macedonia.

Biljana Stojčevska works as an Associate Professor at the UACS School of Computer Science and Information Technology. She received her BSc, MSc and PhD degrees in Computer Science at the Institute of Informatics, Faculty of Natural Sciences and Mathematics, at "Sts. Cyril and Methodius University" in Skopje, Macedonia.

Veno Pachovski (1965) graduated, completed MSc and got his PhD from Faculty of Natural Sciences and Mathematics, University "Sts. Cyril And Methodius", Skopje, Macedonia.

Since 2009, he teaches a variety of courses at the University American College – Skopje, mainly within the School of Computer Sciences and Information technology (SCSIT).

Nevena Ackovska is Associate Professor at the Faculty of Computer Science and Engineering at "St. Cyril and Methodius" University in Skopje, Macedonia. She holds B.Sc. in Computer Engineering, Informatics and Automation from Electrical Engineering Faculty (2000), M.Sc. in Bioinformatics (2003) and a Ph.D. in Bioinformatics (2008) from Faculty of Natural Sciences and Mathematics at "St. Cyril and Methodius University" in Skopje, Macedonia.

REFERENCES:

- [1] Božinovski, A. and Ackovska, N. (2012) The Binary Tree Roll Operation: Definition, Explanation and Algorithm, International Journal of Computer Applications, 46(8):40-47.
- [2] Božinovski, A., Stojčevska, B. and Pačovski, V. (2013) Enumeration, Ranking and Generation of Binary Trees Based on Level-Order Traversal Using Catalan Cipher Vectors, Journal of Information Technology and Applications, 3(2):78-86.
- [3] Cormen, T. H., Leiserson, C. E., Rivest, R. L. and Stein, C. (2009) *Introduction to Algorithms, Third Edition*, The MIT Press.
- [4] Puntambekar, A. A. (2010) *Design and Analysis of Algorithms*, Technical Publications Pune.

Submitted: December 1, 2016.

Accepted: December 12, 2016.

MANET vs. ZigBee: SOME SIMULATION EXPERIMENTS AT THE SEAPORT ENVIRONMENT

Sanja Bauk, Diego Garcia Gonzalez, Anke Schmeink, Zoran Ž. Avramović

bsanjaster@gmail.com; diego.kmp@gmail.com; anke.schmeink@rwth-aachen.de;

zoran.avramovic@sf.bg.ac.rs

Critical review

DOI: 10.7251/JIT1602063B

UDC: 539.163:504.03]:001.892

Abstract: The paper presents the results of some OPNET simulation experiments realized with an aim to benchmark MANET and ZigBee networks' performances at the seaport environment. The MANET is formed among workers' and supervisors' personal digital assistants (PDAs). On the other side, the ZigBee is established between end-nodes or employees' body central units (BCUs), which collect signals from several active and passive devices embedded into ID badges and personal protective equipment (PPE) pieces; several moving and fixed routers; and the coordinator mounted at the appropriate seaport location. The simulation experiments are realized over the layout of the Port of Bar (Montenegro) container and general cargo terminal by taking into account the real number of workers and supervisors engaged at the terminal per each shift. This research work should give an insight to the seaport's managers and stakeholders into some advantages and disadvantages of these two considered wireless networks' schemes, and to motivate them to provide conditions for implementing these or similar on seaport and backend info-communication solutions for uprising the level of occupational safety and overall seaport's environmental management system.

Keywords: MANET, ZigBee, seaport, occupational safety.

INTRODUCTION

This paper is a kind of follow-up of several previously published papers [2-5], which consider possibilities of adopting new info-communication technologies in improving on seaport (afterwards port) workers' and supervisors' safety at the Port of Bar (Montenegro). The Port of Bar functions during the decades in transitional environment that implies permanent reproduction of different crisis and prevents the port's development. Such circumstances have, among other impacts, negative implications to the employees' and environmental safety. By proposing variety of contemporary safety monitoring and controlling info-communication models, we have in mind a need for positive and progressive transfer and adoption of new technologies from developed environments into a developing one [1]. In other words, we were trying to propose affordable, i.e., cost-effec-

tive solutions, which have to be *smart*, safety and sustainable ("3S") at the same time [19]. In this paper, firstly, we shall give a short overview of the MANET and ZigBee networks' concepts and their functionality. Then, we shall propose simple models for employing them at the above mentioned developing, invasive port environment, along with presenting some simulation experiment results obtained for both proposed networks' by using OPNET simulation modeler.

THE MANET: IN BRIEF

A Mobile Ad-hoc NETWORK (MANET) is a self-configuring network where nodes are connected wirelessly and move freely by changing network topology constantly and unpredictably. Ad-hoc wireless networks suffer not only the same problems of

wireless and mobile communications, like power control, bandwidth allocation and optimization, transmission quality, etc., but also others due to the lack of fixed infrastructure and the multi-hops, such as configuration advertising, ad-hoc addressing, self-routing, etc. MANET nodes rely on batteries and remain in a continuous awake mode in order to be ready for either transmission or reception of packages, thus energy savings are among the relevant system design criteria [7]. Apart from these, it is to be pointed that the multi-hop paradigm characteristic for MANET extends the possibility to communicate to any couple of network nodes, without the need to develop any ubiquitous network infrastructure. Nearby users communicate directly, not only to exchange their own data, but also to relay the traffic of other network nodes that cannot directly communicate. At the beginning stage of its development, MANET was one of the most innovative and challenging network paradigm and was promising to become one of the major technologies, increasingly present in everyday life. However, after more than three decades of intense research efforts, the pure general-purpose MANET concept suffers from scarce exploitation and relatively low interest in the industry and among the users, except military and disaster recovery applications. Additionally, the number of manuscripts focused on MANET, published in top quality journals, is decreasing [6]. Since a great body of knowledge about MANET has been produced, many researchers in the field are now trying to apply it to the field of wireless sensor networks. Besides, up to the current moment, several networks concepts have emerged from the MANET field, like: mesh, opportunistic, vehicular, sensor ones, etc. MANET is usually close to humans, in the sense that most nodes in the network are devices that are meant to be used by human beings (e.g., laptops, PDAs, mobile radio terminals, etc.). We used this in exploring channel performances, at physical and MAC layers, over the set of on port workers and their supervisors equipped with their personal digital assistants (PDAs) at the port terminal.

THE ZIGBEE: IN BRIEF

The ZigBee is a global hardware and software standard designed primarily for Wireless Sensor

Networks (WSNs). WSNs topology may change dynamically, not only due to the node mobility like in MANET, but because some nodes can fail [15]. Especially in some harsh and inaccessible environments, the nodes are prone to fail. Beside failures, topology may also change due to the sleep-awake circle characteristic for these networks. Through these cycles, energy savings are to be achieved. Today, ZigBee technology is used in almost every appliance. It is embedded in a wide range of products and applications across customer, commercial, industrial and government markets worldwide. Predominantly it is used for monitoring and control applications. It is easy to install and maintain (self-organizing); it is reliable (self-healing); it scales to thousands of nodes; it is low cost; it uses open standard and provides multi-vendor availability; batteries operate for several years, etc. This technology is simpler and less expensive than other W-P/L/M-ANs (Wireless- Personal /Local/Metropolitan-Area Networks) like Bluetooth, Wi-Fi, Wi-Max, etc. [20,14] In the paper, we have made some simulation experiments in OPNET with ZigBee standard at the physical and communication layers between on port workers' and supervisors' body area sub-networks composed of a set of active and passive sensors, RFID tags, ID badges, BCUs, several moving and fixed routers, and the coordinator, in order to allow permanent insight into employees' and their personal protective equipment (PPE) garment presence and functionality at the terminal.

CASE STUDY

The paper compares some MANET and ZigBee performances at the harsh and dynamic developing port environment through the simulation experiments while the layout of the Port of Bar container and general cargo terminal, including its real workload, mechanization and personnel capacity, is taken as an exemplar (Figure 1). It is well known that ports are dangerous places, especially for on port workers and pedestrians, in terms of operational risks connected to un-loading operations, managing on port traffic and transportation, including hard manipulative mechanization, warehousing dangerous cargoes, etc. Work at ports takes place through the day and night, in two or three shifts sometimes, in all weather conditions. It involves a number of different employees

and contractors carrying out different activities. This requires highly synchronized co-operation and communication between all involved parties. Ports also tend to be associated with emerging environmental problems: water and air pollution, soil contamination, problems related to dust and noise, generation of waste, dredging operations, warehouse storage of hazardous substances, etc. Thus, a comprehensive management of these risks can help improving safety, reducing accidents and saving lives [7,11,17]. The Port of Bar suffers the lack of contemporary infra- and supra-structural capacities, including advanced info-communication solutions which could optimize working processes and reduce occupational and environmental risks. Relatively low turnover of the port saves workers of some risks, but this fact should not be *recommended* as a desired state of the port's operational and business outcomes. Working conditions at the port should be improved through effective and progressive adoption of new transportation and manipulative technologies including info-communication ones. Therefore, through the previous research works in the field [2-5] we proposed several models for enhancing on port workers safety. As a continuation of these pioneer research endeavors, a comparative analysis between potential MANET and ZigBee applications for supporting on port employees' occupational safety measures has been realized. It is very important that workers have available possibility of uninterrupted interpersonal communications and communications with their supervisors (e.g., via MANET PDAs), and also it is very important to provide continuous monitoring of workers' presence at the terminal, as well as, monitoring if required PPE is used, and if it is functional during the operational process at the terminal (e.g., via ZigBee BCUs).

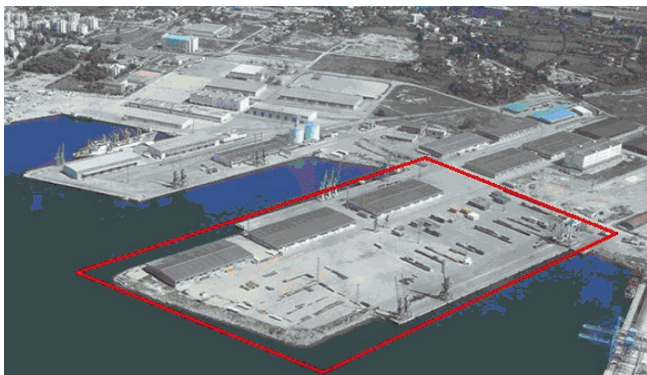


Figure 1. The container and general cargo terminal at the Port of Bar (Source: web)

The container and general cargo terminal at the Port of Bar (Figure 1) has a quadrilateral form, which is approximated for our research work by a rectangle with dimensions 650 x 350 m. Workers can move with high level of freedom over the terminal, while their movements are only restricted by the physical structures present on the surface, which are in this case three industrial warehouses, moving vehicles, vertical mechanization structures, and several container blocks. The industrial warehouses are not a serious problem for the mobility freedom of the workers, since they can go inside and through the warehouses; moving vehicles is also not a big problem; but, the containers are, since they are usually located in blocks and can cause interference to the communication devices by reducing the range.

In experiments with the MANET, IEEE 802.11 standard for the physical and MAC layers is used, while some of the key network performances are analyzed for DSR, AODV, OLSR and TORA routing protocols [10]. The simulation experiments with the ZigBee are realized by using IEEE 802.15.4 standard for the physical and MAC layers, too. The analyses are done considering two ISM frequency bands allowed in the port region, i.e., 868 MHz and 2.4 GHz, along with three common topologies: star, cluster three and mesh.

For both approaches, the application traffic contains the information taken by the sensors or RFID tags attached to the workers/supervisors PPE garments, or their ID badges. That information contains important data to be analyzed, such as ID of each worker/supervisor, ID and sensors' functionality of each worker's/supervisor's PPE piece (hard helmets, safety vests or protective shoes), data on plantar pressure, ambient light, temperature, etc. All these data are collected by BCU (body central unit) attached to the employee's belt. The content of the information is not clear at the present moment and it may vary in the future, depending on the port's real needs. Therefore, it will be abstracted here and treated as a payload that the network has to transmit to a certain point where it will be analyzed. This payload in the application level for each packet transmitted by each worker/supervisor is approximated by 32 bits, which is enough to transmit the IDs of the employees and a

few more data collected from the sensors attached to PPE garments [12].

SIMULATION ANALYSIS

Both MANET’s and ZigBee’s simulation experiments are realized in OPNET Reverbed Modeler Academic Edition 17.5 over the plot of general and cargo terminal at the Port of Bar. The Port of Bar consists in fact of seven different terminals that are used for different purposes and it has about 200 employees in total on port operations. We assumed that there are mostly 20 employees at analyzed container and general and cargo terminal per shift. We analyzed this terminal since it is exposed to the highest operational risks. Although we did experiments for 5, 10 and 15 employees, or better say networks’ PDAs (MANET) and end-nodes/routers (ZigBee), the results obtained in the cases of 15 and 20 moving devices should be put in focus, since they appear more challenging in terms of evaluating the networks’ usual performances.

Experiments with MANET

The analyzed scenario for 20 workers, including their supervisor(s), is shown in Figure 2. There is no fixed infrastructure in MANET. Thus, the network is formed just by PDAs of employees who can move freely around the terminal. Nevertheless, the traffic is to be centralized to a certain destination in order to be routed to an external server by using another interface. This device is PDA carried symbolically by worker_1 in our scenario. The whole traffic must be sent towards the worker_1 (market with a laptop icon in Figure 2). In fact, any PDA could play this

role since this node is exactly the same as any other PDA node; it is just marked with a different icon to visualize which is the device that receives the traffic from other nodes, what will be done by using the IP direction of the node. The blue rectangle around the network (Figure 2), defines the mobility domain for the nodes within which the employees can move freely. In OPNET environment, some characteristics shared by all nodes in MANET are to be defined by using “configuration nodes” that group all common features, but they do not represent any physical node. In our scenario, it was necessary to define three different configuration nodes: mobility configuration node, IP configuration node and reception configuration node. The attributes of these nodes are shown in Figure 3. The detail description of used devices, their parameters and OPNET basic interface information are given in reference [8].

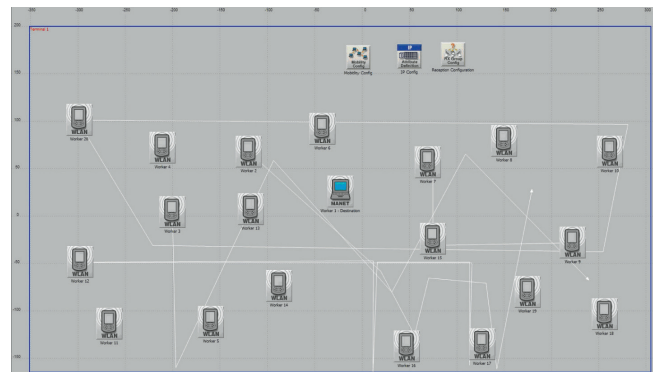


Figure 2. The MANET scenario: 20 workers and supervisor(s) at the seaport terminal (Source: own)

Frequency band is determined by the IEEE 802.11, and it is set at 2.4 GHz. Simulation time is set to one hour. After several series of simulations

(Mobility Config) Attributes		(IP Config) Attributes		(Reception Configuration) Attributes	
Attribute	Value	Attribute	Value	Attribute	Value
Random Mobility Profiles	(...)	IP Route Table Export	(...)	Transceiver Selection	(...)
Number of Rows	1	Status	Enabled	Affected Transmitter Set	(...)
Random Waypoint		Export Time(s) Specification	(...)	Number of Rows	1
Profile Name	Random Waypoint	Number of Rows	13	All Transmitters	
Mobility Model	Random Waypoint	40	...	Receiver Group Name	All Transmitters
Random Waypoint Parameters	(...)	300	...	Initial Receiver Set	All Possible Receivers
Mobility Domain Name	Terminal 1	600	...	Duration	
x_min (meters)	-350	900	...	Begin Time (seconds)	Start of Simulation
y_min (meters)	-150	1,200	...	End Time (seconds)	End of Simulation
x_max (meters)	300	1,500	...	Refresh Interval (seconds)	5
y_max (meters)	200	1,800	...	Receiver Selection Parameters	
Speed (meters/seconds)	constant (2)	2,100	...	Selection Parameters	
Pause Time (seconds)	None	2,400	...	Channel Match Criteria	All Channels
Start Time (seconds)	constant (10)	2,700	...	Distance Threshold (meters)	120
Stop Time (seconds)	End of Simulation	3,000	...	Pathloss Threshold (dB)	None
		3,300	...		
		End of Simulation	...		

Figure 3. Some attributes of the mobility, IP and reception configuration nodes (Source: own)

for 5, 10, 15 and 20 nodes, it is observed that MANET performances are quite poor for lower number of nodes (especially for 5 and 10 nodes). The absence of fixed infrastructure for small number of nodes requires establishing longer range communications that is not always possible due to the maximum range inherent to the devices, leading to the isolation of some nodes. By increasing the number of nodes (e.g., to 15 or 20), the MANET considerably improves its performances. The simulation results are shown in Figure 4. They present the network load (i.e., amount of control, routing and traffic data being carried by the network) for different routing protocols: AODV, DSR, OLSR and TORA. In Figure 4 can be seen that TORA and AODV are the protocols with the lowest network load while OLSR and DSR mostly charge the network in the considered case. The difference is quite big if we compare DSR with AODV or TORA, e.g., DSR doubles the network load comparing it to AODV, and triplicates it when it is compared to TORA, e.g. By comparing the traffic received by the destination, it can be concluded that AODV and DSR are a bit stronger against topology changes than OLSR, and that the weakest is TORA, under the same conditions.

Additionally, by comparing the total end-to-end delay, OLSR and TORA represent a big improvement over the other two considered protocols. For networks with fewer nodes, TORA would not be that effective, but as the number of nodes increases, the delay rapidly decreases [8]. The values of the end-to-end delay for different routing protocols and different number of nodes are given in Table 1. A common trend which can be noticed on the basis of conducted simulation experiments is that end-to-end delay decreases as number of the MANET nodes increases.

Table 1. The MANET end-to-end delay maximal values for different routing protocols and number of network nodes [sec/msec] (Source: own)

OLSR	TORA	AODV	DSR
5_nodes: 40 msec.	5_nodes: 1 sec.	5_nodes: 1.7 sec.	5_nodes: 2 sec.
10_nodes: 30 msec.	10_nodes: 0.3 sec.	10_nodes: 3 sec.	10_nodes: 0.5 sec.
15_nodes: 0.2 msec.	15_nodes: 0.05 sec.	15_nodes: 10 sec.	15_nodes: 0.3 sec.
20_nodes: 0.8 msec.	20_nodes: 0.00 sec.	20_nodes: 0.04 sec.	20_nodes: 0.015 sec.

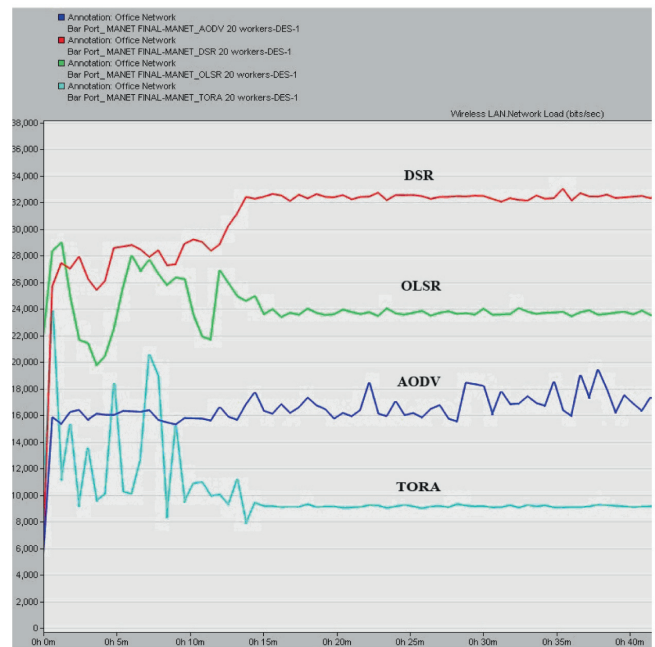


Figure 4. The MANET network load for 20 nodes in the case of AODV, DSR, OLSR and TORA routing protocols (Source: own)

Generally, total end-to-end delay is the time from the moment of generating packages at the source to its receiving at the destination. Some applications, e.g., voice transmissions, are more susceptible than others to the end-to-end delay of packages, and therefore they require its lower average value. Due to the weak signals at the nodes, frequent creation and termination of connections, as well as, the mobility of nodes, the total delay in the MANET network usually increases. It should be noted that there are in fact four different types of delays [18]:

- *transmission delay* - the time which the transmitter needs to deliver all bits of data packages;
- *propagation delay* - the time which is necessary to transfer one bit from the source to the destination;
- *processing delay* - the time which is necessary for processing package before its delivery at the source node, at any intermediate node, and at the end node for processing package before its proceeding to the application; and,
- *queuing delay* - it is the delay which occurs due to queuing at any node along the transmission path.

Accordingly, total delay might be expressed by the following model (1):

$$T_{Total_Delay} = N \cdot (T_{Trans_Delay} + T_{Prop_Delay} + T_{Process_Delay} + T_{Queu_Delay}) \quad (1)$$

Where,

N - is a number of nodes in the network;

T_{Total_Delay} - is the total delay;

T_{Trans_Delay} - is a transmission delay;

T_{Prop_Delay} - is a propagation delay;

$T_{Process_Delay}$ - is a processing delay; and,

T_{Queu_Delay} - is a queuing delay.

The traffic received by destination in the cases of 5, 10, 15 and 20 nodes in the case of using DSR routing protocol is given in Figure 5. It indicates that it is necessary to increase the number of nodes (at least 15 to 20 nodes) to establish functional network, in terms that nodes can route traffic smoothly to the destination. By analyzing the number of hops and global delay, it is also observed that they decrease, as the number of nodes increases.

Experiments with ZigBee

Some simulation experiments with ZigBee are realized for three different topologies: star, cluster tree and mesh [13,16], and for two different frequencies 868 MHz (with max. bit rate of 22 kbps) and 2.4 GHz (with max. bit rate of 250 kbps). The scenario includes: a coordinator, three fix routers, mounted at the warehouses' roofs, one or two moving routers attached to the forklift(s) which operate(s) at the terminal, and 4(+1), 9(+1), 13(+2), and 18 workers (+1 or 2 forklifts). More or less, the location of a co-



Figure 5. Traffic received by destination in the case of DSR routing protocol in MANET for the scenarios with 5, 10, 15 and 20 nodes (Source: own)

ordinator and fixed routers might vary depending on the eventual changes of the physical conditions at the port perimeter in the future. The detail description of network devices, physical and MAC layers parameters, packet size, packet interval time, etc., is given in [8]. The ZigBee scenario in OPNET environment with 18 workers and 2 moving routers attached to the forklifts is shown in Figure 6.

Some ZigBee network performances' analyses are done for star, tree and mesh topologies, while the following might be observed:

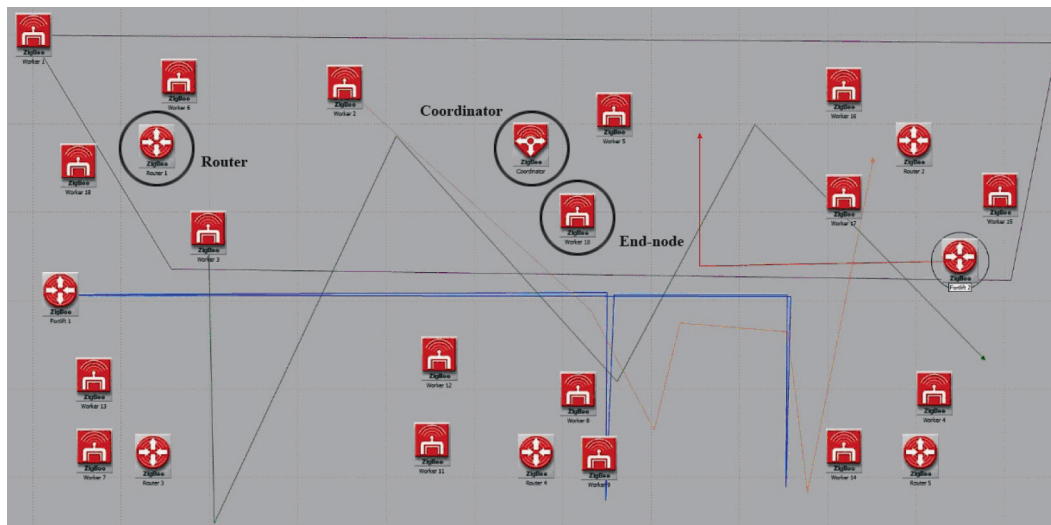


Figure 6. The ZigBee scenario: 18 on port workers and 2 moving routers mounted at the forklifts (Source: own)

- Star topology:** The traffic received by the coordinator is among the most important features for this application. It is not so important if some packages are lost, as long as a node is not isolated. The experiments showed that in the case of 5 nodes there are no loses; for 10 nodes there are a few; for 15 nodes the package loses are higher, but the network still works. The problem comes with 20 nodes, since loses are quite high. When we analyzed the traffic received by the destination from a single worker in the case of 20 nodes, the traffic from some workers that are far from the coordinator is completely lost and some workers became in such way isolated. These package loses are caused primarily due to the interference and the distances between some nodes and the coordinator, but also due to the star topology that forces direct communication. The global end-to-end delay increases with the number of nodes, too. In the case of 20 nodes, the traffic falls when the nodes get isolated and they are not able to communicate. It is important to note that 2.4 GHz frequency brings in general some benefits over 868 MHz to this topology.
- Tree topology:** The traffic received by coordinator is between 13-15 packages in the cases with 15 and 20 nodes, which represents the important improvement in comparison to star topology, due to the possibility of routing traffic through the routers. Concerning the global delay, in comparison to the global delay in the star topology, it is rather similar. It is important to emphasize that there are considerable differences in these network parameters in the case of 868 MHz and 2.4 GHz. The 2.4 GHz band provides the important performance enhancements. This means that 50% more packages is received for 15 nodes, and double the amount of packages received in the case of star topology for 20 workers. In terms of global delay, 2.4 GHz band provides more than 60% lower delay than in the star topology for the same frequency. This huge reduction is caused by multiplication of the number of packages received, which reduces the number of transmissions. Another important moment is increase in the maximum bit rate from 20 kbps (868 MHz) to 250 kbps (2.4 GHz).

- Mesh topology:** The traffic received by coordinator does not show a big improvement in comparison to tree topology. The global delay is slightly reduced, due to new connections between routers. It can be concluded, that there are no considerable differences in the network performances, in general, with tree and mesh topology within the considered scenarios. However, the differences between network performances in the case of 868 MHz and 2.4 GHz are to be pointed again, especially for the larger number of nodes, i.e., 15 and 20 (see Figure 7). It happens since the data rate is considerably higher at 2.45 GHz, and since more efficient modulation scheme, i.e., Quadrature Phase-Shift Keying (QPSK) is used, in comparison to Binary Phase-Shift Keying (BPSK) one, which is used in the case of 868 MHz frequency band.

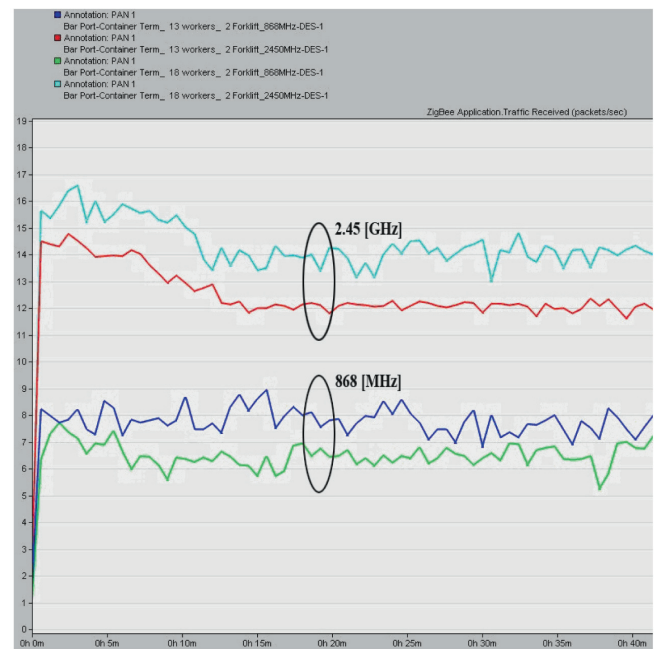


Figure 7. Traffic received by a coordinator for ZigBee mesh topology: 868 MHz vs. 2.4 GHz (Source: own)

Some experimentally obtained values of end-to-end delay for different topologies of the ZigBee network for 5, 10, 15 and 20 end nodes and 1 or 2 moving routers, depending on the scenario at the analyzed port terminal, are given in Table 2. There are some variations, but it is obvious that for each topology a negative correlation between the number of nodes and end-to-end delay exists. The main reason is that ZigBee is primarily projected for low traffic density, and this implies bigger delay for the larger number of end-nodes and routers.

Table 2. The ZigBee end-to-end delay minimal and maximal values (bold) for different topologies and number of end-nodes and moving routers [sec] (Source: own)

No. of nodes	Star		Tree		Mesh	
	868 MHz	2.4 GHz	868 MHz	2.4 GHz	868 MHz	2.4 GHz
5_nodes	0.065 -0.085	0.065 -0.085	0.090 -0.120	0.090 -0.150	0.050 -0.100	0.100-0.110
10_nodes	0.140-0.150	0.135-0.150	0.150-0.210	0.140-0.220	0.150-0.200	0.140- 0.220
15_nodes	0.180-0.210	0.065-0.110	0.250-0.360	0.850- 0.950	0.250-0.350	0.070 -0.100
20_nodes	0.130- 0.480	0.100- 0.155	0.350- 0.490	0.130-0.140	0.370- 0.480	0.120-0.140

Table 3. Resume of the MANET and ZigBee comparisons for 5,

10, 15 and 20 moving nodes (Source: own)

Scenario	Most suitable technology
Five nodes	ZigBee (star topology; 868 MHz and 2.4 GHz)
Ten nodes	ZigBee (mesh topology; 2.4 GHz)
Fifteen nodes	MANET (generally OLSR routing protocol)
Twenty nodes	MANET (generally AODV routing protocol)

MANET and ZigBee comparison

In the attempt to determine which of the considered wireless technologies has more capabilities under given assumptions, it is possible to compare the MANET and ZigBee by using different routing protocols, different network topologies and different number of nodes (nodes here include: workers, supervisors, i.e., their PDAs and BCUs, and moving routers at the forklifts in the case of ZigBee). It is absolutely clear that ZigBee has better performances than MANET for the lower number of nodes, i.e., 5 and 10 nodes, in the analyzed port scenarios.

The traffic received by the destination for 15 nodes scenario shows a change in the performance of the MANET and ZigBee, in comparison to the scenarios with 5 and 10 nodes, and supports the idea of better performance of the MANET. Only tree and mesh ZigBee topologies at 2.4 GHz for 15 nodes, e.g., are close to the performance of the MANET. The global end to end delay also shows a change in the performance. In general, the MANET is more suitable technology for this scenario.

The traffic received by the destination for 20 nodes again shows opposed results in comparison to the scenario with 5 and 10 nodes. In this scenario, all MANET routing protocols show better performance than the ZigBee with any topology and frequency band, while only at 2.4 GHz and by using tree and mesh topologies, the ZigBee is let us say comparable to the MANET. The values of the global end to end delay are similar to those obtained in 15 nodes scenario.

The resume of the MANET versus ZigBee performances in the considered developing port environment is given in Table 3.

Conclusion

The results obtained from different scenarios and by various simulation experiments within the developing port environment (the Port of Bar in Montenegro) can give some new landmarks in the process of the optimal wireless network(s) technology selection, including specific requirements as: the number and mobility of nodes, package size, package inter-arrival time, etc. On the basis of the presented simulation results, the following can be extracted:

- The ZigBee performances are better than the MANET ones for the low density of nodes (here workers, supervisors mobile devices and/or moving routers). The main reason lies in the fact that the ZigBee relies on rather fixed infrastructure, while MANET does not have it. Therefore, for the relatively small number of nodes, it becomes necessary to establish longer communication range that is not always possible due to the maximum range inherent to some MANET devices, leading to the isolation of the nodes;
- As the number of nodes increases, an opposite trend is observed, i.e., the MANET shows better performances than the ZigBee. As the number of nodes rises, it becomes easier for the MANET to establish communication between nodes and to route the traffic towards the destination. On the other side, the ZigBee finds it harder in such case to route the traffic towards the single destination. A ZigBee is conceived to be used for low traffic

applications with low requirements, and the increase of traffic is a threat to its low maximum data rate;

- The simulation results undoubtedly show that 2.4 GHz frequency band improves the efficiency compared to 868 MHz one, due to the higher bit rate and advanced modulation schemes that make 2.4 GHz more suitable to the networks with higher load. When it comes to the ZigBee topologies, tree and mesh topologies increase the range of the communications to the detriment of the delay. Besides, the mesh topology enables the connection between routers that allow the traffic in the case when one router fails. Therefore, when the complexity of the ZigBee network is increased, the best choice should be to select a mesh topology, which operates at the 2.4 GHz;
- Concerning the MANET, the choice of a routing protocol has influence on the network performances. The results show that in the case of larger number of workers, the most efficient routing protocols are AODV and OLSR. DSR is also able to route the traffic with similar delay as AODV or OLSR, but at the cost of increasing the routing traffic which leads to triplication of the network load in comparison to AODV, and its duplication in comparison to OLSR. Thus, for larger

networks, where the risk that a node can become isolated is low, the protocol that might offer the best qualities is AODV, etc.

In further analysis, behavior of the larger number of network nodes should be examined. This might be achieved by connecting networks at different terminals within the port and analyzing them as a whole, within the considered-real scenario(s). Also, the experiments with larger packages' inter-arrival intervals should be done. The content of the network payload, i.e., the content of each package should be specified, as well. The managers and stakeholders at the port should be introduced in detail to the basic pros and cons of both here analyzed networks' structures and performances. Their real needs and preferences should give proper directions for further more intensive and rigorous research studies in the field. The workers'/supervisors' willingness to become part of such wireless network(s) is to be assessed, too, as a part of non-technical, or more *soft*, further examinations. Of the key importance is, in any case, top managers' and stakeholders' interest in adopting new, advanced wireless networks and back-end information communication systems for improving both on port workers' and integral port's environmental safety measures.

REFERENCES:

- [1] Avgerou C. 2011. Discourses on innovation and development in information systems in developing countries research, in Galliers R.D., Currie W.L. (Eds.), *The Oxford Handbook of Management Information Systems – Critical Perspectives and New Directions*, published in the United States by Oxford University Press Inc., New York, Chapter 25, pp. 647-671.
- [2] Bauk S., Gonzalez D.G., Schmeink A., Examining some ZigBee/RFID safety system performances at the seaport, Proc. of the 58th IEEE International Symposium Electronics in Marine (ELMAR), Zadar, Croatia, 12-14 September, 2016, pp. 133-137.
- [3] Bauk S., Schmeink A., Colomer J., An RFID Model for Improving Workers' Safety at the Seaport in Transitional Environment, Transport, doi:10.3846/16484142.2016.1233512, article in press, 2016.
- [4] Bauk S., Schmeink A., Džankić R., Port workers' safety monitoring by RFID technology: A review of some solutions, Proc. of the 7th International Conference on Maritime Transport (MT), Barcelona, Spain, 27-29 June, 2016, pp. 570-580.
- [5] Bauk S., Schmeink A., RFID and PPE: Concerning workers' safety solutions and Cloud perspectives - A reference to the Port of Bar (Montenegro), Proc. of the 5th IEEE Mediterranean Conference on Embedded Computing (MECO), Bar, Montenegro, 12-16 June, 2016, pp. 35-40.
- [6] Conti M., et al., From MANET to people-centric networking: Milestones and open research challenges, *Computer Communications*, 71, 2015, pp. 1-21.
- [7] Ecoport 8, Project documentation: Ecoport 8 - Environmental management of transborder corridor ports, Code: SEE/A/218/2.2/x, Port of Bar (Montenegro) Final Report, 2013.
- [8] Garcia Gonzales D., *Wireless Sensor Networks (WSNs) vs. Mobile Ad-hoc Networks*, Master thesis, Lehrstuhl für Theoretische Informationstechnik, RWTH Aachen University, Aachen, Germany, 2016.

- [9] Garcia-Macias J.A., Gomez J., MANET versus WSN, in *Sensor Networks and Configuration – Fundamentals, Standards, Platforms, and Applications*, Ed. Mahalik N.P., Springer, 2007, pp. 367-388.
- [10] Hakmat P., *Ad-hoc Networks: Fundamental Properties and Network Topologies*, Springer, Dordrecht, The Netherlands, 2006.
- [11] HSE - Health and Safety Executive, *A quick guide to health and safety in ports*, London, UK, May, 2013. (Web resource; last access November, 2016)
- [12] Kelm A., Laußat L., Meins-Becker A., Platz D., Khazae M.J., Costin A.M., Helmus M., Teizer J., *Mobile passive Radio Frequency Identification (RFID) portal for automated and rapid control of Personal Protective Equipment (PPE) on construction sites*, *Automation in Construction*, 36, 2013, pp. 38-52.
- [13] Manpreet J.M., *Simulation Analysis of Tree and Mesh Topologies in ZigBee Network*, *International Journal of Grid Distribution Computing*, 8(1), 2015, pp. 81-92.
- [14] Mihajlov B., Bogdanovski M., *Overview and Analysis of the Performances of ZigBee-based Wireless Sensor Networks*, *International Journal of Computer Applications*, 29(12), 2011, pp. 28-35.
- [15] Pan M-S., Tseng Y-C., *ZigBee and Their Applications*, in *Sensor Networks and Configuration – Fundamentals, Standards, Platforms, and Applications*, Ed. Mahalik N.P., Springer, 2007, pp. 349-367.
- [16] Saha S., *ZigBee OPNET Modeler: An Efficient Performance Analyzer for Wireless Sensor Networks*, *International Journal of Engineering Sciences & Research Technology*, 2(8), 2013, pp. 2032-2036
- [17] TenEcoport, *Project documentation: TenEcoport - Transnational ENhacement of Ecoport8 Network*, code: SEE/D/01889/2.2/x, Port of Bar (Montenegro) Feasibility Study on Improving Environmental Management System at Container Terminal, 2014.
- [18] Tepšić D., *Jedno unapređenje OLSR ruting protokola u mobilnim ad hoc mrežama*, Doktorska disertacija, Univerzitet Singidunum, Beograd, Srbija, 2013.
- [19] Trentesaux D., et al., *Emerging ICT concepts for smart, safe and sustainable industrial systems*, *Computers in Industry*, <http://dx.doi.org/10.1016/j.compind.2016.05.001>, article in press, 2015.
- [20] Vancin S., Erdem E., *Design and Simulation of Wireless Sensor Network Topologies Using the ZigBee Standard*, *International Journal of Computer Networks and Applications (IJCNA)*, 2(3), May-June, 2015, pp. 135-143.

Submitted: December 9, 2016.

Accepted: December 11, 2016.

BIOMETRIC SYSTEM TO SECURE THE INTERNET OF THINGS

Olja Latinović

*Faculty of Organizational Sciences, University of Belgrade, Belgrade, Republic of Serbia,
oljalatinovic88@gmail.com*

Critical review

DOI: 10.7251/JIT1602073L

UDC: 004.738.5.056

Abstract: Today, Internet of Things (IoT) is becoming part of a diverse organization, from academic to large enterprises. Also, we use IoT in our daily lives like home appliances, security monitoring such as baby, smoke detectors, health product measure exercise, traffic systems, industrial uses, etc. Biometric is an important segment of IoT, because it proves user's identity. Biometric security plays the main role in IoT. This paper presents how biometric system secures the Internet of Things and architecture proposal based on one system that connects biometric system and components of Internet of Things.

Keywords: biometrics, Internet of Things, security, authentication.

INTRODUCTION

If we follow possibilities for the *future of technology* and society, we encounter Internet of things concept. It has tendency that everything can be controlled through the Internet. Many devices are connected over the RFID, NFC, Bluetooth etc. [3]. When using biometric system in the identification mode, biometric data collected by acquisition sensors is compared with templates stored in the biometric database.

Modern information systems need more security in their systems without PIN code. The main goal of this paper is how biometric system secures the Internet of Things. Jain [5] presented two types of attacks: Intrinsic limitations and Adversary attacks. Intrinsic limitations contain False non-match (two samples from the same individual have low similarity and the system cannot correctly match them) and False match (two samples from different individuals have high similarity and the system incorrectly declares them as a match). Adversary attacks refer to the Insider attacks (Collusion, coercion...), Attacks on sen-

sor (Spoof attacks), Attacks on feature extractor and matcher (Trojan horse attacks), Attacks on Interconnections between modules (Man-in-the-middle and replay attacks) and Attacks on database (Template leakage). Old user authentication approaches are inadequate in the IoT era. New patterns are needed because the granting of physical access. ZK Research [11] predicts that by 2020, the IoT will consist of 50 billion endpoints. Gartner [13] says that the IoT will drive device and user relationship requirements in 20% of new identity and access management (IAM), with new biometrics to emerge as a key role.

PROBLEM DEFINITION

The most widely way to authenticate users are by using the unique code (which we have chosen by ourselves) or PIN codes. Both methods carry some risk of forgetting, theft, hacking etc. The fact is that traditional passwords are not enough.

Biometrics provides a new method to secure physical and logical access (unimodal or multimodal sys-

tem). The biggest difference between the biometric and other authentication methods is that biometrics truly verifies an individual's identity. Each biometric characteristic is unique and individual [12]. More companies accept biometrics.

At the same time, it develops the Internet of Things (IoT). It represents the concept of smart automation and smart monitoring through the Internet as communication [4]. Biometric identification offers simplicity and other benefits to users who want a safe and secure way to confirm the identity. Recently, there has been an increase in the application's development which are biometric data integrated in various industries (automotive, banking, healthcare, etc.).

Leading research is related to the fact that the Internet of things will launch devices where biometrics plays the main role. It will be necessary because each device requires identity to interact with a user. Security and privacy are the key issues for the IoT applications.

BIOMETRIC SYSTEM

Biometric systems are technical systems that use biometric characteristic of people. These systems can operate in multiple modes. The most interesting modes are biometric data entry, identification mode and verification mode. Biometric data entry mode involves the entry of a new entity (Enrollment) in database through the acquisition. This process occurs if the entity does not exist in the database. Verification (or authentication) mode system performs a one-to-one comparison of captured biometric with

a specific template stored in biometric database in order to verify the individual is the person they claim to be. The following figure represents the difference between identification and verification.

Biometrics is automated method of recognizing a person based on physiological or behavioral characteristic [1]. Physiological characteristics are fingerprint, palm veins, iris recognition, retina, face recognition, DNA, etc. Behavioral characteristics include voice recognition, signature recognition, keystroke dynamics.

Biometric security is mainly implemented in environments with critical physical security requirements or that are highly prone to identity theft. Biometric security-based systems or engines store human body characteristics that do not change over an individual's lifetime. These include fingerprints, eye texture, voice, hand patterns and facial recognition.

While comparing various available biometric methods, it is important to have valid criteria. Expert in biometrics [7] developed seven criteria:

- Uniqueness - the proportion of people that have the characteristics necessary for authentication;
- Universality - any two people should not have the same biometric features;
- Permanence - should not change with time (iris...);
- Collectability - characteristics can be easily measured and quantified;
- Performance - the accuracy and speed of biometric methods;
- Acceptability - the extent to which users are

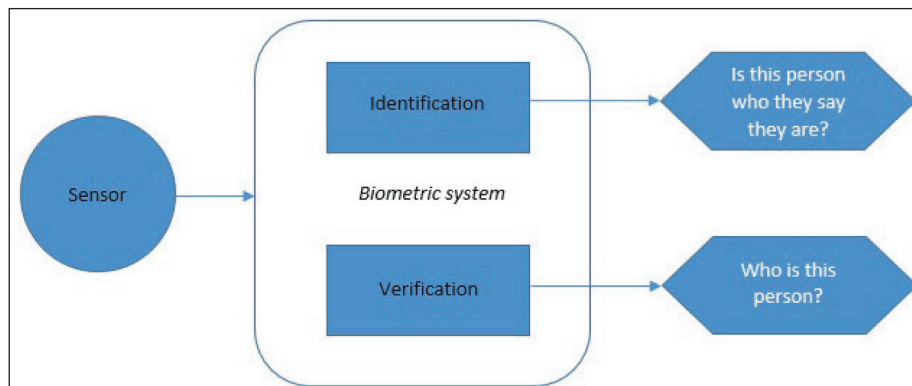


Figure 1. Biometric system - difference between identification and verification

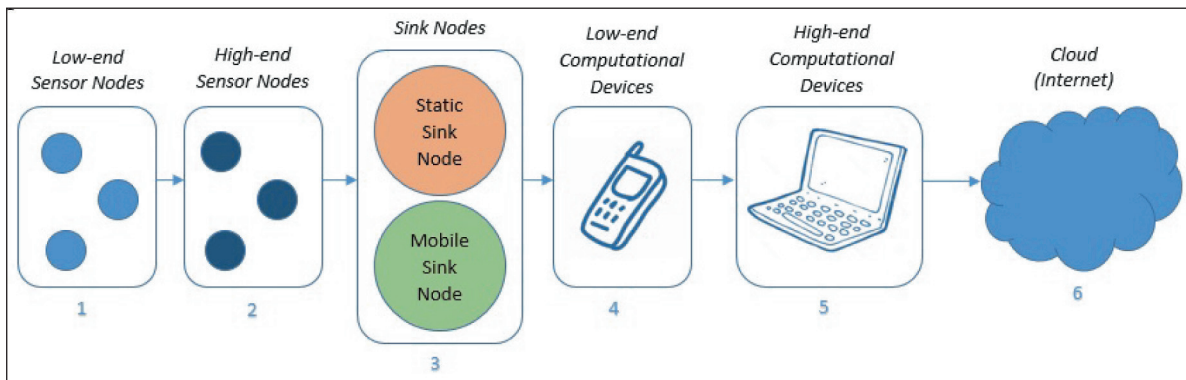


Figure 2. IoT Architecture

ready to allow the system to collect their biometric characteristics;

- Circumvention - how easy it is to fool the system using fraudulent method.

INTERNET OF THINGS

Internet of Things (IoT) is interdependent system of mechanical and digital machines, devices, people with unique biometric characteristics and usability of transfer data across a network. The IoT allows for remote management and exchange of data with different objects which make decisions themselves. The IoT architecture contains six layers (Figure 2). The first and the second layer include sensor nodes to process information. They communicate with the third layer which provides translation between application and devices (layer 4 and layer 5). The latest layer is Cloud which represents the Internet-based services.

Atzori [2] grouped five domains in the IoT about possibility to communicate with each other in different environments. These are:

- Transportation and logistics domains (Logistics, Assisted driving, Mobile ticketing, Environment monitoring, Augmented maps),

- Healthcare domain (Tracking, Identification/Authentication, Data collection, Sensing),
- Smart environment domain (Comfortable homes/offices, Industrial plants, Smart museum and gym),
- Personal and social domain (Social networking, Historical queries, Losses, Thefts),
- Futuristic domain (Robot taxi, City information model, Enhanced game room).

Weber [10] elaborated attacks in data authentication of the Internet of Things. He mentioned sufficient framework with specific technology in account to supplemented specific needs by private sector. The system must contain corresponding measures and rules in the IoT mechanisms.

Suo [8] explained cryptographic algorithms which are encryption mechanism and provide communication security.

BIOMETRIC SYSTEM TO SECURE THE INTERNET OF THINGS –ARCHITECTURE PROPOSAL

It is very important to secure company’s data which uses the Internet of Things. One of the ways

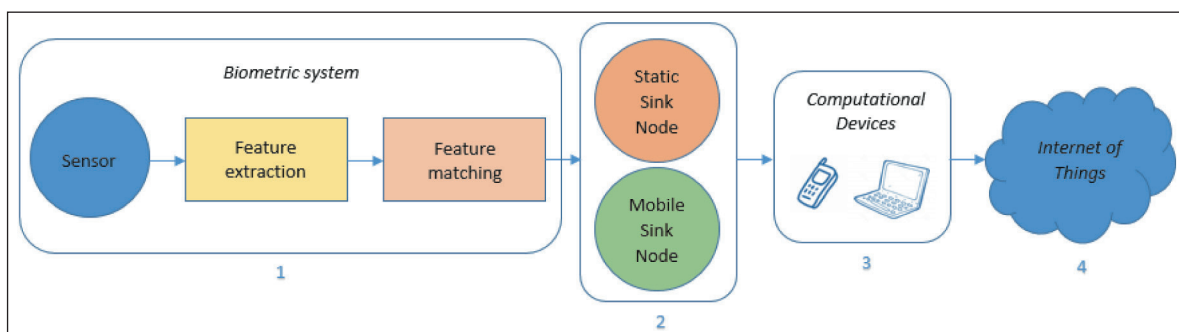


Figure 3. Biometric system to secure Internet of Things

is to plan and design a biometric system. Figure 3 shows how to biometric system secures the Internet of Things. In the first step, there is one biometric system with any biometric authenticator which performs feature extraction and feature matching. When a person is recognized, data is collected by mobile and static sink nodes. Both of them send the data to computational devices (low-end or high-end). Last step is cloud or the Internet of things which has data where it will be stored, shared or processed. Various extensions of this architecture are possible such as the use of more sensor nodes, or special biometric characteristic for exchanging authentication and authorization data between parties.

Valera [9] designed architecture to offer great potential and flexibility of communications, monitoring and control. He used 6LoWPAN and RFID/NFC to secure SIM card to authenticate, encrypt and sign the communications with medical devices.

Karimian [6] mentioned reasons of security. Also, he said that incorporation of biometrics to the Internet of Things presents the cost care. His paper introduced ECG biometrics which are highly, more secure and easy to implement.

One biometric tokenization platform should be mentioned, namely the HYPR. It is a solution for safety and integrity user biometric data over mobile, desktop and the Internet of Things.

CONCLUSIONS

In this paper, various important aspects of biometric system functionality are revised. It processed information on the special consideration process and ways of how to apply the said. It processed special consideration about biometric security in the Internet of Things. Biometric sensors on devices are changing user authenticate procedure to services they use every day. Paper described how biometric system can play the main role in the Internet of Things.

The IoT community is growing fast and an authentication needs to be more practical. Having traditional passwords on devices can be stolen. It is clear that a better solution is biometric security. Suggested

system in this paper presents an easy way to secure authentication, possible variation for customers. This process is established on biometric feature matching and sink nodes in the IoT which provides stable security system.

Future research of this topic is detailed analysis biometric open source system integration with the IoT solutions. Potential disadvantage is challenges such as bugs in open source system. Also, it is worth mentioning about possible attacks on the system. It is an important problem, and should be considered. The IoT products represent a possibility for enormous prosperity.

BIOGRAPHY

Olja Latinovic was born in Prijedor in 1988. She studied at the Pan-European University "APEIRON" at the Faculty of information technologies in Banja Luka. Master academic studies finished at Faculty of Organizational Sciences in Belgrade. Since 2010 to 2013 she was assistant at the Pan-European University "APEIRON" (Analysis and Design of Information Systems, DBMS, Microsoft Office). From 2013 to 2016, she worked in "Breza software engineering" as a software engineer. Since 2012, she was at PhD academic studies where researching biometrics, especially voice biometric recognition. She published scientific papers, mostly in biometrics field. In the meantime, she acquired the official "Oracle" certificates as Oracle Database 11g Performance Tuning Certified Expert and Oracle Database 11g Administrator Certified Professional and Oracle Certified Professional Java SE 7 Programmer. During graduate and doctoral studies she participated as a student associate in the Laboratory for multimedia communications in the project "Multimodal biometrics in identity management," TR32013, Ministry of Education, Science and Technological Development of Republic of Serbia. She speaks Serbian, English, German and French.

REFERENCES

Conference papers

- [1] Angle, S., et al. (2005, March). Biometrics: A further echelon of security. In UAE International Conference on Biological and Medical Physics.
- [2] Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, 54(15), 2787-2805.
- [3] Darianian, M., & Michael, M. P. (2008, December). Smart home mobile RFID-based Internet-of-Things systems and services. In 2008 International conference on advanced computer theory and engineering (pp. 116-120). IEEE.
- [4] Gubbi, J., Buyya, et al. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645-1660.
- [5] Jain, A. K., & Nandakumar, K. (2012). Biometric Authentication: System Security and User Privacy. *IEEE Computer*, 45(11), 87-92.
- [6] Karimian, N., et al. (2016, October). Evolving authentication design considerations for the internet of biometric things (IoBT). In Proceedings of the Eleventh IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis (p. 10). ACM.
- [7] Schuckers, M. (2001). Some statistical aspects of biometric identification device performance. *Stats Magazine*, 3.
- [8] Suo, H., et al. (2012, March). Security in the internet of things: a review. In *Computer Science and Electronics Engineering (ICCSEE)*, 2012 International Conference on (Vol. 3, pp. 648-651). IEEE.
- [9] Valera, A. J. J., et al. (2010, January). An architecture based on internet of things to support mobility and security in medical environments. In 2010 7th IEEE Consumer Communications and Networking Conference (pp. 1-5). IEEE.
- [10] Weber, R. H. (2010). Internet of Things—New security and privacy challenges. *Computer Law & Security Review*, 26(1), 23-30.

Journal

- [11] Kerravala Z, “*It’s time for businesses to embrace the Internet of Things*” (2014), ZK Research Whitepaper, pp 3-4
- [12] Kumari, D., & Sharma, R. (2016). “Analysis of Biometric Authentication system-Security, Issues and Working using Visual Cryptography.” *International Journal of Advanced Research in Computer Science*, 7(1).
- [13] Meulen R. and Rivera J. (2015), “*Gartner’s 2015 Predictions Special Report Examines the Significant Impacts of the Evolution of Digital Business*”, Gartner, Inc. (NYSE: IT) (1)

Submitted: November 24, 2016.

Accepted: December 3, 2016.

FRAMEWORKS FOR AUDIT OF AN INFORMATION SYSTEM IN PRACTICE

Dalibor Drljača

Europrojekt centar, drljacad@gmail.com

Branko Latinović

Panevropski univerzitet APEIRON, branko.b.latinovic@apeiron-edu.eu

General survey

DOI: 10.7251/JIT1602078D

UDC: 007:004.65]:005.334

Abstract: The IT function became the backbone of the company and the central driving force of the entire operations of an organization. Modern electronic commerce is very dependent on the quality of information system supported with information technology. Safety aspects of business and electronic transactions transfer (Internet-supported), particularly in the banking sector, require a more complex audit of the organization, both financial and the information system audit. This paper presents the basic and in practice most frequently applied standards and guidelines for checking of security controls in information systems. The work presents the COBIT and ITIL as the two most prevalent methodologies for quality audit of information systems with the presentation of two ISO 27000 series of standards on information security.

Keywords: audit frameworks, IT audit, IT Governance, COBIT, ITIL, ISO27000.

INTRODUCTION

Modern business strongly depends on information technologies (IT) and other relevant auxiliary technologies. The supporting information system (IT supported or not) must be properly established. Weak or bad established information system with corresponding infrastructure not aligned with strategic goals and needs of business ultimately lead to additional and usually not necessary extra costs for the company.

Therefore, information system management must be considered as a very important business process. Proper information management, timely and adequate use of information are providing necessary market advantage, and therefore IT governance and IT auditing are becoming leading concepts today. These concepts are implemented very often in large

and complex organisations in order to have overall insight over organisation's activities and for trend analyses.

Linking management and IT is a key for the success of business. Some of the leading problems for already established information systems are a timely collection of information, processing in most efficient manner, but also storing and keeping it out of sight of competitors. To evaluate the quality of the information system in use and its functionality, it is necessary to implement the process of information system auditing. By its nature, this audit process is very demanding and complex. It is even more complex than a classic financial audit. Today, there are a number of standards and frameworks for this kind of audit. Most known and popular are COBIT, ITIL, set of ISO standards, COSO, VAL IT etc. This paper gives an overview of these most important and used

frameworks for information system audit process enabling quality IT management.

IT GOVERNANCE AND AUDITING

Van Grembergen defines IT governance as „*the organisational capacity exercised by the Board, Executive Management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT*“ [22]

Gartner Inc. consulting company also provided definition that defines IT governance as “*the processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals*” [6]

IT governance includes following areas [14]:

- *Strategic alignment;*
- *Value delivery;*
- *Resource management;*
- *Risk management;* and
- *Performance measurements.*

Strategic alignment ensures adequate linking of business and IT strategies and plans. They define, maintain and confirm or support IT organisational values and also define and manage IT business operations in line with regular business activities.

Value delivery enables IT to provide promised and projected advantages realizing strategies and concentrating on costs optimisation and IT investments.

Resource management aims at optimal investments and adequate governance of critical IT processes, such as applications, information, infrastructure and human resources. Key issues relate to the optimisation of knowledge and infrastructure.

Risk management must be implemented and realized at all levels in the organisation – from employees up to the top level management – in order to achieve risk transparency and their mitigation with a clear definition of measures for risk management responsibility.

Performance measurement is needed in order to follow and monitor implementation of strategies

and projects, use of resources, working processes and provision of services using „*balanced scorecard*“ [16] (measuring and comparing selected indicators) that is used to follow the success of actions and meeting strategy goals along the classical accounting measurement methods. From previous explanation it is obvious that it is necessary to invest a lot of efforts, time and resources to establish a quality information system that will serve a purpose. However, it is not enough to establish the system, but to maintain it is even more important.

Auditing of information systems is relatively new discipline (appearing from the 1960s) intending to become a multidiscipline scientific field that links organisational, strategic and IT aspects of company's business. Historically, auditing of information systems appears as a need for an extension of standard and traditional financial audit in the moment when auditors' limited knowledge of IT requested additional IT knowledge or externally engaged IT professionals. However, there is a significant difference between two types of auditing. The role of the financial audit is **to evaluate if the organisation is complying with standard accounting practices**. From the other hand, the aim of the information system auditing is **to evaluate design and effectiveness of the system using organisation's internal controls**. Therefore, it is not possible to equalize this auditing with the internal auditing.

The definition of information system auditing states that it a process of collecting and evaluating claims on how information system **preserves properties of the company, data integrity and enables more effective and more efficient use of resources for the achievement of business goals** [3].

From the definition, it is obvious that the object of audit is systematic, quality and careful review of controls within all parts of information systems. From this, we can draw basic auditing tasks [18]:

- To evaluate and estimate present status of the system (maturity, level of success),
- To discover risk areas and level of risk, and
- To provide recommendations to the management on practice for the improvement of the governance.

The information system auditor must have broad knowledge and experience not only of business and local legislation, but he/she must also have a broad knowledge of information and communication technologies and modern trends in the field in order to evaluate properly the possible risks.

Given that this is a very complex area and that it requires a holistic approach to problem solving, the practice shows a number of standards and frameworks for auditing of information systems.

INFORMATION SYSTEM AUDITING FRAMEWORKS

Frameworks of information system auditing represent guidelines for the auditor’s work and the model of implementation of the audit process for systematic (qualitative and quantitative) collecting and processing data required for the preparation of the audit findings. As there are different schools and approaches to the study of certain areas, it is clear that the frameworks for revision occur in multiple forms. In this paper, we will mention only three most important - COBIT, ITIL, and ISO related standards.

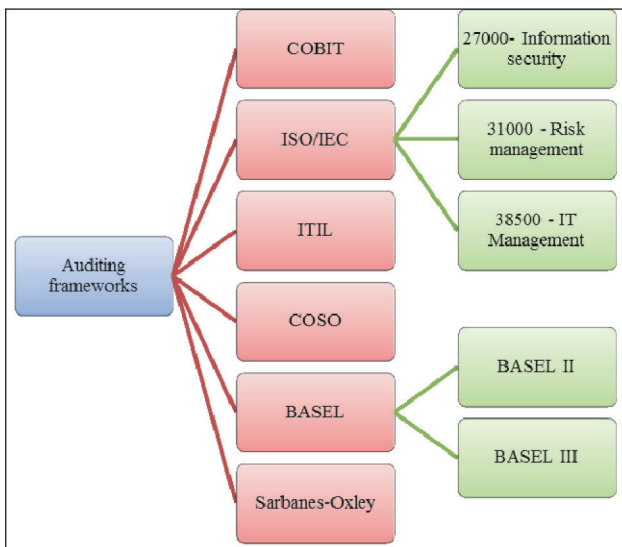


Figure 1. Most used auditing frameworks (author)

COBIT

COBIT (*Control Objectives for Information and Related Technologies*) is a framework made by ISACA (*Information Systems Audit and Control Association*, <http://www.isaca.org>) and ITGI (*IT Governance Institute*, <http://www.isaca.org/itgi/Pages/default.aspx>)

with the aim to assist management of information technologies (systems). It represents one of the most popular frameworks for information system control, published for the first time in 1996, while actual version 5 was published in 2012. [8]

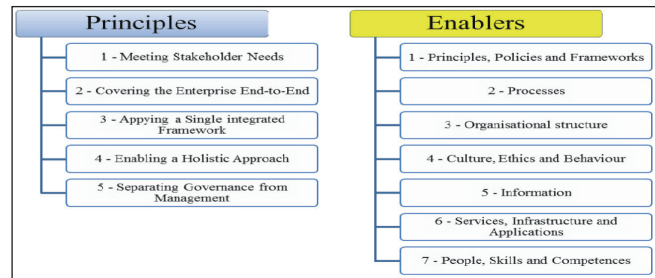


Figure 2. COBIT 5 principles and enablers (author)

COBIT5 *principles and enablers* are generalized and therefore applicable to all companies, regardless of size, types, and ownership. As such, COBIT5 recognizes 7 enablers, which in principle represent factors that individually or collectively influence organisational IT governance and management.

Also, COBIT5 contains 34 control objectives and 37 processes, the fulfilment of which allows the successful achievement of the objectives of functional information systems. These are grouped into five domains [9]:

- *Evaluate, Direct and Monitor* – EDM,
- *Align, Plan and Organise* – APO,
- *Deliver, Service and Support* – DSS,
- *Monitor, Evaluate and Assess* – MEA,
- *Build, Acquire and Implement* – BAI.

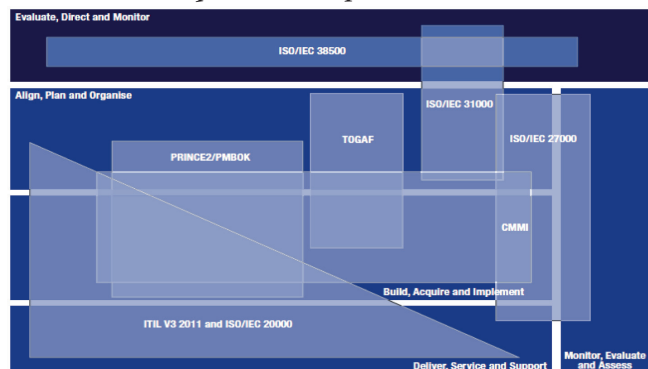


Figure 3. COBIT 5 covers issues from most of frameworks and standards (taken from [9] pg.61.)

As a standard, COBIT5 is useful for different types of users [13]:

- For **managers** – to assist understanding of the information system, to assist decision making on level of safety and control, to provide a basis for investment decisions, to increase efficiency in decision making, to assist in governance and definition of the strategic plan for the information system, to assist in improvement of IT architecture and purchase of necessary ICT technologies, to assist in follow-up and monitoring of system performance, etc.
- For **end-users/employees** – to assist understanding of the information system, to assist understanding of safety and control levels, to assist understanding of organisational strategies etc.
- For **auditors** – to assist understanding of the information system, to assist understanding of safety and control levels, to assist understanding of organisational strategies, to assist in identification of the IT controls and its infrastructure, to help traceability of information in the system, etc.

ITIL

ITIL (*IT Infrastructure Library*) presents a set of best practices for IT service management, both in the introduction and in the improvement. In its essence, ITIL advocates the need to harmonize IT services with needs of business and supports its core processes by providing guidance to the organization and individuals for the use of IT tools to facilitate business change, transformation and growth [2]. The author of ITIL methodology is British *Central Computer and Telecommunications Agency (CCTA)* that was reorganised from 2000 as *UK Office of Government Commerce (OGC)*. They created ITIL by the end of 1980s as a set of guidelines for the use of IT services. As such, it was an obligation for all institutions and bodies of the UK public administration. GITIM (*Government Information Technology Infrastructure Management*) was the first official version of ITIL, while the second version was published in 2001, and actual version 3 was introduced in 2007. The latest, third version, adopts the paradigm of management of IT services' life cycle with strong emphasis on business integration of IT [15]. The AXELOS company (<https://www.axelos.com>) took over ITIL in July 2013 as a joint venture of CAPITA (<http://www.capita.co.uk>) and the *Cabinet Office of British Government* (<http://www.gov.uk/cabinetoffice>), with

further authorities over licencing of use of ITIL's intellectual property rights [23].

ITIL as process and business-oriented, uses so-called *top-down approach*. The basis of ITIL consists of five main (5) processes described in 5 volumes of ITIL [1] [19]:

- **ITIL Service Strategy** - used for defining of strategic elements as initial phase of IT services life-cycle (who are consumers, what are their needs, which resources are needed for development etc.);
- **ITIL Service Design** - used to ensure effective design of new or improved services meeting customer needs, with the development of mechanisms for monitoring and evaluation of effectiveness and efficiency of processes;
- **ITIL Service Transition** - used to enable evaluation and testing of design from the previous phase and for transition from the service model to provision of service;
- **ITIL Service Operation** – used for provision of services including daily status monitoring, managing daily routines and users demands, etc.; and
- **ITIL Continual Service Improvement** – used to exploit measuring mechanisms and for improvement of the level of provided services, technologies, as well as for efficiency and effectiveness of the global system for services' management.

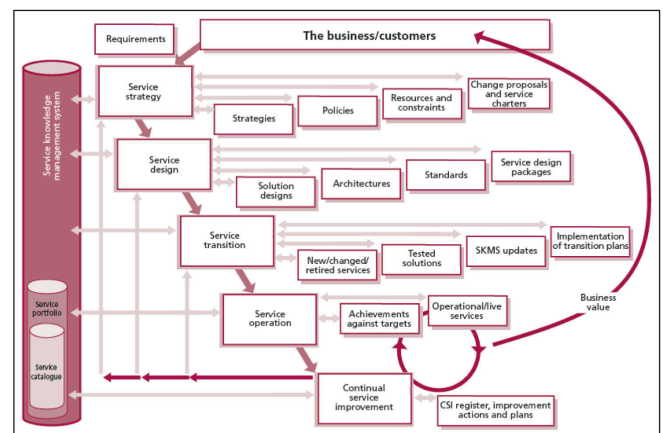


Figure 4. Integration across the service lifecycle (from [4] pg.9.)

There are at least three factors influencing success and acceptance of ITIL. The first one is that ITIL methodology is broadly available to all and that it is maintained by the governmental non-profit organisation. Second, ITIL is accepted by the largest global

organizations and the third factor is the existence of a large number of learning materials (websites and books) for achievements of ITIL goals [7].

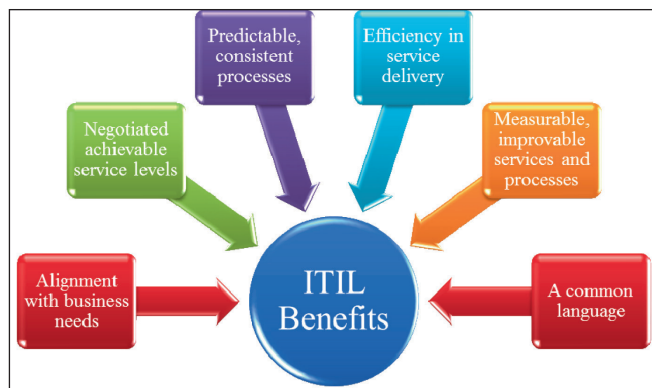


Figure 5. Benefits of implementing ITIL (adapted from [1])

ISO 27000 family of standards

The family of ISO/IEC 27000 standards deals mainly with setting up of a valid system for management with information security called *Information Security Management System – ISMS*. The definition and vocabulary of ISMS were given in ISO/IEC 27000:2014 (third version). More details on ISO/IEC 27000 family of standards are given in Table 1.

The standard ISO/IEC 27001:2013 provides precise requirements for setting up, implementation, maintenance and continuous improvement of ISMS

within the organizational context. It also incorporates requirements for evaluation and treatment of information security risks, tailored in accordance with the need of the organisation. The requests are more generic in order to be implemented in all organizations regardless of its type, size or nature. Conceptually, the standard is composed of seven chapters, as follows [11]:

1. Context of the organisation;
2. Leadership;
3. Planning;
4. Support;
5. Operation;
6. Performance evaluation;
7. Improvement; and
8. Annex A with a list of controls and their objectives.

Standard ISO/IEC 27002 started as ISO/IEC 17799 in 2000 and in 2005 was renamed and re-numbered into ISO/IEC 27002. It presents a codex for information security practices and is created for the use in organizations as a reference for selection of controls in process of ISMS implementation based on ISO/IEC 27001, or as guidelines for implementation of wide accepted controls related to the information security. Thus, ISO/IEC 27002 and ISO 27001 standards together are giving recommenda-

Table 1. The family of ISO/IEC 27000 standards (from[10])

ISO/IEC 27000	<i>Information security management systems — Overview and vocabulary</i>
ISO/IEC 27001	<i>Information security management systems — Requirements</i>
ISO/IEC 27002	<i>Code of practice for information security controls</i>
ISO/IEC 27003	<i>Information security management system implementation guidance</i>
ISO/IEC 27004	<i>Information security management — Measurement</i>
ISO/IEC 27005	<i>Information security risk management</i>
ISO/IEC 27006	<i>Requirements for bodies providing audit and certification of information security management systems</i>
ISO/IEC 27007	<i>Guidelines for information security management systems auditing</i>
ISO/IEC TR 27008	<i>Guidelines for auditors on information security controls</i>
ISO/IEC 27010	<i>Information security management for inter-sector and inter-organizational communications</i>
ISO/IEC 27011	<i>Information security management guidelines for telecommunications organizations based on ISO/IEC 27002</i>
ISO/IEC 27013	<i>Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1</i>
ISO/IEC 27014	<i>Governance of information security</i>
ISO/IEC TR 27015	<i>Information security management guidelines for financial services</i>
ISO/IEC TR 27016	<i>Information security management — Organizational economics</i>

tions or list of all controls needed for implementation of ISMS with the aim to decrease a level of risks dealing with security. These standards are very popular and widely used, while their implementation can contribute achievement of main objectives of internal controls of an information system (security aims, IT objectives, and business continuity). ISO/IEC 27002:2013 standard consists of 14 main chapters, as follows [12]:

1. Information security policies;
2. Organization of information security;
3. Human resource security;
4. Asset management;
5. Access control;
6. Cryptography;
7. Physical and environmental security;
8. Operation security;
9. Communication security;
10. System acquisition, development, and maintenance;
11. Supplier relationships;
12. Information security incident management;
13. Information security aspects of business continuity management; and
14. Compliance.

COSO

During 1985, accounting and financial associations in the USA gathered in an alliance named *Committee of Sponsoring Organizations of the Treadway Commission* – COSO (<http://www.coso.org>) with the main aim to finance public-private initiatives given by the *National Commission on Fraudulent Financial Reporting* [5].

COSO framework states that the internal control is composed of five interconnected elements, and for IT auditing purposes the most important is the fourth one [17]:

1. **Control environment** – senior management must set up a positive environment for control and lead employees with own example to respect and to perform their duties as best as they can;
2. **Risk assessment** – a strategy that supports mission and key objectives of the company must be adopted and it will decrease eventual

risks of implementation;

3. **Control activities** –in order to ensure proper functionality of internal controlling system, it is necessary to establish adequate controls that will be regularly monitored;
4. **Information and Communication** – all relevant information must be accessible to employees and to the public in order to have good and successful two-way communication system; and
5. **Monitoring activities** – refers to regular evaluation and monitoring of risks and controls, and if necessary to make improvements and corrections.

Other recommendations and standards

There is a significant number of other guidelines, recommendations, and standards which can be adequately combined with previous ones and with the aim to ensure better use of IT and information systems in daily business.

For example, for the banking sector, there are very important and widely accepted recommendations - **Basel II** (2004) and **Basel III** (2011) - sets of reform measures that are covering banks' information system control [20]. These recommendations underline the importance of information system safety in providing services to customers.

Sarbanes-Oxley law was created in 2002 as an initiative of two (same named) USA congressmen as the response to corporative fraud in the financial reporting. The articles of this law became an obligation for all companies present at any stock exchange in the USA. The aim of the law was to introduce a more efficient system of internal controls over the financial reporting process. This law prescribes that the executive managers are responsible for the implementation of the internal control system in operations enabling management to understand the flow of transactions, including their IT aspects, and with sufficient details in order to identify eventual points of fraud and misuse [21].

CONCLUSION

Modern business is not possible without computer-supported information systems and relevant tech-

nologies. These can provide a market advantage to the organization, if used properly. A significant question is on the adequacy of these systems and technologies as well as their security issues. Therefore, the auditing of an information system is becoming an unavoidable factor for modern business and organizations. This is even more important considering the fact that IT functions of the company are recognized as a central driver of the organisation, especially in electronic commerce.

IT auditors require special skills and a lot of IT knowledge needed for quality and safety aspects of information system auditing. Such complex educational qualifications require experienced professionals and these professionals are becoming high demand at the labour market. Moreover, the IT professionals are the one most profiting from the present accelerated development of IT and information system auditing.

The aim of this paper was to provide an overview of basic standards and guidelines for information sys-

tem auditing that are broadly accepted worldwide. A number of standards were intentionally left unexplained (due to the limited space for the paper) such as ISO/IEC 38500, ISO/IEC 50000, VAL-IT etc. However, their importance is significant for overall auditing process of information systems and they should be also taken into consideration when planning such venture.

BIOGRAPHY

Dalibor Drljača is a Ph.D. candidate at the Faculty of Information Technologies at the Pan-European University APEIRON Banja Luka and has MA in information technology and MA in technologies for the Development of European Projects. His main research interests are in e-Government, audit of information systems and e-Commerce. He is part-time engaged as a Senior teaching and research assistant at Pan-European University APEIRON Banja Luka.

Branko Latinović, Ph.D., is a full-time professor and Dean of the Faculty of Information Technologies at the Pan-European University APEIRON Banja Luka since its establishment. His research interests are in information systems, e-Commerce and e-Government.

REFERENCE

- [1] Arraj V(2013) ITIL®: The basics (White paper), The APM Group and The Stationery Office
- [2] Axelos What is ITIL® Best practices? <https://www.axelos.com/best-practice-solutions/itil/what-is-itil> (accessed on 1.8.2016.)
- [3] Cangemi MP(2000) Managing the Audit Function: A Corporate Audit Department Procedures Guide 3rd ed., John Wiley & Sons, New York, USA, pg.23.
- [4] Cartledge AS et al. (2012) An Introductory Overview of ITIL v3, itSMF Ltd, UK
- [5] COSO About us, <http://www.coso.org/aboutus.htm>, (accessed on 2.8.2016.)
- [6] Gartner Inc. IT Glossary, <http://www.gartner.com/it-glossary/it-governance/> (accessed on 14.8.2016.)
- [7] Infotrend Poslovni IT certifikati, <http://www.infotrend.hr/clanak/2012/2/poslovni-it-certifikati,187,894.html> (accessed on 14.8.2016.)
- [8] ISACA COBIT 20th Anniversary, <http://www.isaca.org/COBIT/Pages/COBIT-20th-Anniversary.aspx#years> (accessed on 5.8.2016.)
- [9] ISACA (2012) COBIT 5 - A Business Framework for the Governance and Management of Enterprise IT, Rolling Meadows, IL, USA
- [10] ISO/IEC (2014) International standard ISO/IEC 27000:2014 (3rd edition), International Organization for Standardization
- [11] ISO/IEC (2013) International standard ISO/IEC 27001:2013 (2nd edition), International Organization for Standardization
- [12] ISO/IEC (2013) International standard ISO/IEC 27002:2013 (2nd edition), International Organization for Standardization
- [13] IT revizija.ba COBIT, <http://itrevizija.ba/2011/11/cobit/> (accessed on 3.8.2016.)
- [14] IT revizija.ba Upravljanje IT (IT Governance), <http://itrevizija.ba/2010/08/upravljanje-it-it-governance/> (accessed on 4.8.2016.)
- [15] ITIL Central History of ITIL, <http://itsm.fwtk.org/History.htm> (accessed on 1.8.2016.)

- [16] Kaplan RS, Norton DP (1996) *The Balanced Scorecard: Translating Strategy Into Action*, Harvard University Press, USA
- [17] Monte Negro Ministry of Finance (2011) *Priručnik za finansijsko upravljanje i kontrole*, Podgorica (available at www.mf.gov.me/pretraga/107135/Prirucnik-za-finansijsko-upravljanje-i-kontrole.html, accessed on 2.8.2016.)
- [18] Spremić M. *Primjena IT u finansijskom izvještavanju Računovodstveni informacijski sustavi* (available at http://itre-vizija.ba/wp-content/materijal/prezentacije/EFSA_Master_Primjena_IT_u_financijskom_izvjestavanju.ppt and accessed on 4.8.2016.)
- [19] The Art of Service Pty Ltd (2009) *ITIL V3 Foundation Complete Certification Kit: 2009 Edition Study Guide*, Brisbane, Australia
- [20] The Bank for International Settlements, *Basel III: international regulatory framework for banks*, <http://www.bis.org/bcbs/basel3.htm> (accessed on 14.8.2016.)
- [21] U.S. Securities and Exchange Commission (2009) *Study of the Sarbanes-Oxley Act of 2002 Section 404 Internal Control over Financial Reporting Requirements*, Office of Economic Analysis, USA
- [22] Van Grembergen W (2002) *Introduction to the minitrack IT Governance and its Mechanisms*, Proceedings of the 35th Hawaii International Conference on System Sciences (HICSS)
- [23] Wikipedia ITIL <https://en.wikipedia.org/wiki/ITIL> (accessed on 1.8.2016.)

Submitted: September 24, 2016.

Accepted: December 7, 2016.

USING OPEN SOURCE SOFTWARE FOR WEB APPLICATION SECURITY TESTING

Ksenija Živković, Ivan Milenković, Dejan Simić

Faculty of Organizational Sciences, University of Belgrade, Belgrade, Republic of Serbia

ksenija.zivkovic@mmklab.org, ivan.milenkovic@fon.bg.ac.rs, dejan.simic@fon.bg.ac.rs

Case Study

DOI: 10.7251/JIT1602086Z

UDC: 004.738.5.056

Abstract: Web applications are a standard part of our everyday lives. Their purpose can vary significantly, from e-banking to social networks. However, one thing is similar - users have generally high expectations from different web applications. To assure such high expectations, proper web application testing is necessary. Non-functional testing is an important part of web application testing. As technology advances and requirements become more complex, the importance of non-functional application aspects becomes even greater. It is necessary to identify non-functional requirements of web applications which are important to users, implement those requirements and test them.

Keywords: non-functional testing, web applications, testing tools.

INTRODUCTION

Software errors in most cases can cause trivial problems that have no greater impact on business and can be easily solved. However, software errors in flight control or medical equipment can not be allowed, because consequences may be disastrous. For companies, software errors could bring grave financial damage. Below are examples of problems that errors caused in the past.

In 1998 NASA launched the Mars Climate Orbiter, a robotic space probe for studying climate, atmosphere and surface changes on Mars. Instead entering the Martian atmosphere, it was destroyed because a navigation error caused it to miss its target altitude. Main cause of this problem was a bad translation of English to metric units. This way a project worth 327 million dollars was destroyed [9].

In 2003, the Amazon UK web site had to be closed because of error in pocket computer prices, which were sold for 7 instead of 192 pounds. As a result, all orders had to be cancelled [12].

In 2014, Sony suffered an enormous attack where hackers erased data from the system, stole and published movies that were not yet published, private and sensitive data [10]. Before that, in 2011, hackers have accessed data of 77 million users of PlayStation network. Company has lost millions of dollars because website was not working for over a month [8].

In February this year, Volvo had to recall 59,000 cars over software fault that could cause temporary shutdown of an engine while the car is in motion. This error was reported by drivers of new Volvos, who experienced a brief absence of steering and braking. The error could have caused traffic accidents and could be life threatening for drivers, and at the same time negatively affect reputation and financial stability of a company [12].

National Institute of Standards and Technology (NIST) concluded a research study in 2002. The study concluded that software errors cost American economy 59 billion dollars per year, and that with

better testing there could be saved 22.2 billion dollars [9].

In order to avoid problems caused by software omission, errors should be identified and amended on time, before they even appear. Process of identifying errors is called software testing. Testing is an important activity in software development and it will be described in detail in the next chapters.

Section 2 of this paper describes the process of application testing. In section 3, two tools for non-functional application testing are described. Analysis of a case study where described tools are applied is given in section 4. Section 5 contains conclusions and suggestions for future improvements.

APPLICATION TESTING

Testing is a method for software quality control and an important activity in software development, and its purpose is identifying errors. It represents check if software is implemented according to user requirements. In a broader sense, testing is a process of quality control, during which, besides checking software, contains checking of its components and characteristics.

There are two basic types of testing: [11]:

- Functional testing and
- Non-functional testing.

Functional testing checks if application meets all necessary functional requirements. It checks if application does what is made for. This type of testing will not be further discussed in this paper.

Non-functional testing checks behavior and readiness of an application. Focus is on the aspects of software that refer to software quality, not functionality.

Quality aspects of software that are determined by non-functional testing are:

- Performance,
- System behavior under heavy load,
- Reliability,
- Security.

Despite big differences between functional and non-functional testing, there are common basic concepts, team roles and activities in testing teams.

Non-functional application testing

Types of non-functional testing are [1]:

- Load testing,
- Security testing,
- Configuration testing and
- User interface testing.

Load testing is performed in order to determine system's behavior under extreme conditions and discover its endurance limits [3]. Result of testing can be time, amount of used memory, etc. Types of load testing are:

- Performance testing and
- Stress testing.

Performance testing checks how the system functions under normal load [3]. Time for performing an action is analyzed. Factors that affect application performance are: platform, infrastructure, number of users, etc. Each of the above factors needs to be considered during testing and acceptable results need to be defined. Some of the tools for performance testing are: FireBug, JMeter, Grinder, etc.

Stress testing checks how system functions under extreme conditions [3]. Goal of stress testing is finding limits of application's endurance. It can be tested how the system behaves with greater amount of users or a large database.

Security testing is a type of software testing which purpose is detecting system's vulnerabilities. It checks whether the system data is protected from unauthorized access, during which data could be altered or deleted.

Areas to be considered during security testing are:

- Network security,
- Software security,
- Security on client's side,
- Security on server's side.

Main goal of security testing is assuring that application is safe and there are no exploitable weak-

nesses. It is performed in order to protect data and application functionality when system is attacked. Security testing includes confidentiality testing, integrity testing and authentication and authorization testing [2].

Success of application depends also on interaction between user and graphic interface. In the early stages of application development, these tests are used for accelerating its development and enhancing its quality. Testing can be performed manually or automated, by using tools for user interface testing. UI testing checks quality of interface and ease of use [3]. Interface quality refers to application appearance, and ease of use means that user has no difficulties while using the application and that there are no complicated actions. It is necessary to check whether application looks the same in the environment in which it will be used as in development environment. Application appearance needs to be concise regardless of device and web browser.

Tools for non-functional application testing OWASP Zed Attack Proxy

OWASP Zed Attack Proxy (ZAP) is one of the most popular free security testing tools and one of the most active OWASP projects, maintained by hundreds of international volunteers. Main goal of this project is ease of use, so everyone could benefit from it. It can help with automated finding security vulnerabilities in web applications during development and testing phase.

Main characteristics:

- Free, open source tool,
- Can be used on Linux, Windows and Mac operating systems,
- Easy to use,
- Completely documented,

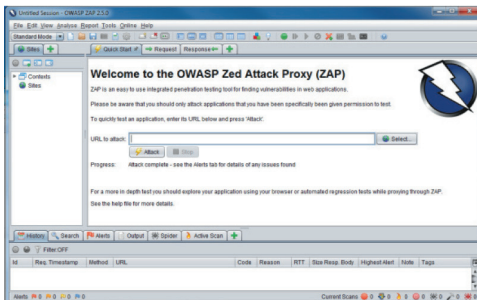


Figure 1. ZAP's interface

- Works well in combination with other software testing tools.

Some of the security problems are impossible to find with automated testing, but ZAP also has manual testing functionality.

Interface of ZAP contains:

- Menu,
- Toolbar which includes buttons for commonly used features,
- Window which displays the sites tree and the scripts tree,
- Workspace window,
- Information window,
- Footer, which displays a summary of the found alerts and their status.

Quick Start enables easy web application testing, which allows entering an URL that ZAP will attack. ZAP uses spider which crawls the application and passively scans all discovered pages. In the meantime, active scanner is used for attacking all found pages.

Spider is a tool which automatically finds links by examining the HTML in application responses. Using this tool it is possible to find hidden web application pages. List of found URLs depends on where spider starts with crawling.

The spider is very fast but not always effective when exploring AJAX applications. AJAX spider is more effective in this case, despite being slower, because it explores the application by invoking browsers which follow the links that have been generated.

Types of scanning ZAP does are:

- Passive and
- Active scanning.

Passive scanner identifies problems by analyzing requests and responses discovered via the spiders and it is safe to use on any web site or application, because it does not use attacks or changes the responses in any way.

Active scanning attempts to find vulnerabilities by using known attacks and it should be used only

on application where testers are allowed to perform such testing. With this kind of scanning it is not possible to identify logical errors, which means automated testing is not enough. Some of the rules of active scanning in ZAP are: Buffer Overflow, SQL Injection and Cross Site Scripting.

In order for active scanning to begin, URL should be listed in Starting point field. In Input Vectors tab target elements could be chosen, in Technology tab used technology should be listed and in Policy tab rules of active scanning could be modified.

Vulnerabilities that could not be detected by active scanners can be identified by using Fuzzer. Fuzzing is a black box software testing technique, which means that only inputs and outputs are tested. It involves providing invalid, unexpected or random data to the inputs of a web application, in order to identify implementation errors [9].

Forced browsing is an attack where the aim is to access resources that are not referenced in application. Attacker can use technique known as Brute Force in order to find sensitive data while searching through directory content.

ZAP generates reports including all found vulnerabilities of an application. Reports contain advices for avoiding these kinds of vulnerabilities and links to more information about security threats and methods to prevent them.

All of the potential vulnerabilities are shown in the Alerts tab. Alerts are connected with application requests and contain information about risks and solutions regarding those vulnerabilities. One request could have more than one alert. Types of alerts are shown on the next picture.






	High	
	Medium	
	Low	
	Informational	
	False Positive	

Figure 2. Types of alerts in ZAP

VEGA

Vega is a free open source scanner and security testing platform for web applications [4]. It is written in Java and runs on Linux, Windows and OS X operating systems. It is developed by Subgraph, company founded in Canada.

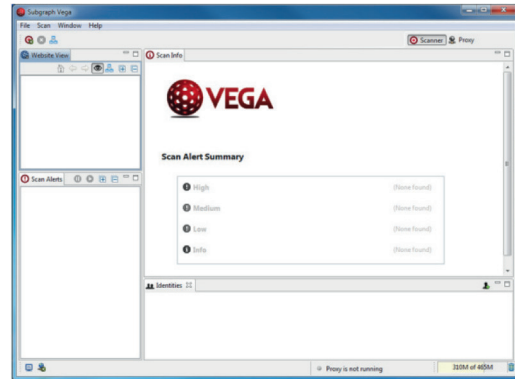


Figure 3. Vega's interface

Vega can be used as:

- Automated scanner or
- Intercepting proxy.

Automated scanner crawls the web application and analyzes pages content. It is capable of identifying system vulnerabilities such as XSS and SQL injection, unintended publishing of sensitive information and other vulnerabilities.

Vega as an intercepting proxy is used for tactical inspection. It is situated between the browser and the web server hosting the application which is tested. The proxy can read all requests that come from the browser and all responses that are returned from the server.

There is also an option to alter requests and responses before being passed on. In order to use this functionality, it is necessary to configure web browser.

High		(1 found)
Cleartext Password over HTTP	1	
Medium		(3 found)
HTTP Trace Support Detected	1	
Local Filesystem Paths Found	2	
Low		(5 found)
Directory Listing Detected	4	
Form Password Field with Autocomplete Enabled	1	
Info		(5 found)
Character Set Not Specified	4	
Possible AJAX code detected	1	

Figure 4. Types of alerts in Vega

During scanning, Vega identifies vulnerabilities and marks them with alerts. Types of alerts are shown in the picture below.

Scan Info contains data about URL where problem could occur and means of solving it.

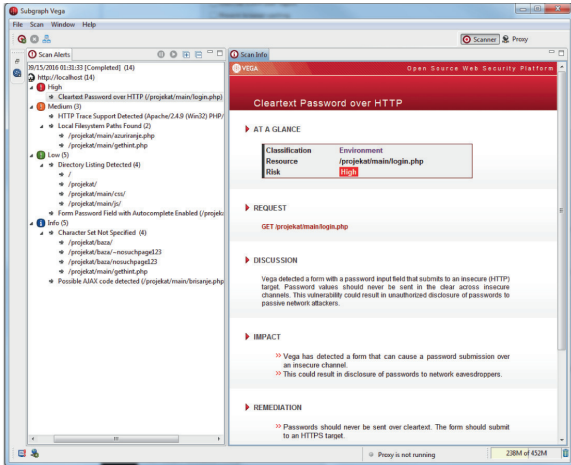


Figure 5. Scan Info in Vega

CASE STUDY

In order to demonstrate how these tools work, security of a web application will be tested. Application is written by using next technologies:

- HTML,
- CSS,
- PHP,
- Flight framework and
- MySQL database.

For initializing, an application on local server WampServer is used. Database is also created on MySQL WampServer. Flight framework was used for creating application paths.

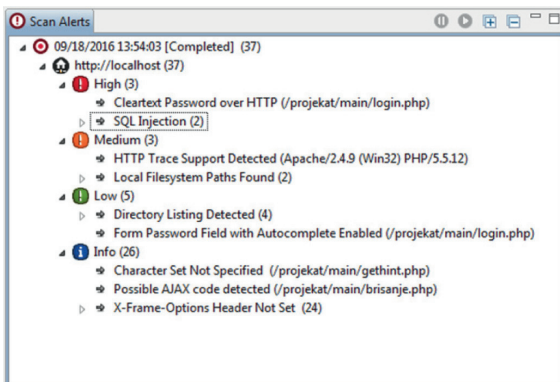


Figure 6. Testing results in Vega

Results of testing can be seen in the next two pictures:

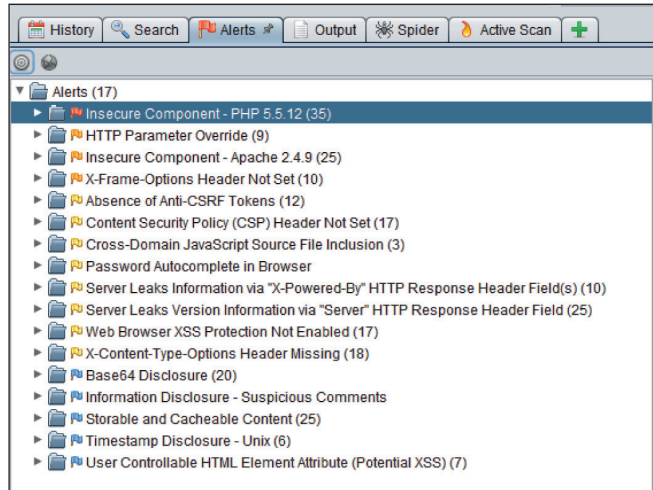


Figure 7. Testing results in ZAP

In Mozilla browser proxy was set to localhost on port 8888 which are default settings in Vega. This way proxy intercepting functionality was set so it could record all requests and responses from web application.

Alerts with highest level of risk are:

- Outdated version of PHP,
- Path traversal,
- Cleartext password over HTTP,
- SQL Injection.

During passive analysis, PHP version 5.5.12 was used, which is not supported anymore. Solution to this problem is using newer version, because web applications in older versions are susceptible to a higher number of security attacks [11].

Path traversal (dot-dot-slash, directory traversal) aims to access files and directories that are stored outside the web root folder. Attackers may manipulate variables that reference files with “dot-dot-slash” sequences and its variations to get to the files of interest [12]. One of the solutions to this problem is using white lists.

If a password is sent over HTTP, there is a danger it might be discovered by an attacker. Solution to this problem is using HTTPS instead of HTTP. That could be resolved by using SSL certificates.

SQL Injection is a technique of code injecting into web applications that are data driven. In this way attackers can get information even though they are not authorized. Web application was tested in order to test whether an attack during signing in is possible. Attack can be stopped by validating input. In case of working with database, it can be solved by preparing inputs for queries or escaping special characters.

Alerts with medium level of risk are:

- HTTP Trace Support detected,
- HTTP parameter override,
- ClickJacking attacks.

HTTP TRACE is a request method used for echoing back user inputs. If application is not secured from XSS attacks, this method can be used for getting confidential information or redirecting users to malicious sites.

On every page that contains a form possibility of overriding, HTTP parameters were detected. In order to stop this kind of attacks it is necessary to specify a name for form action, because if it does not, browser considers URL as an action name which means attackers can set values of parameters within URL, so user would not be redirected on the page it should be.

ClickJacking is an attack where attacker uses multiple transparent layers to trick the user into clicking on a page or button when they were intending to click on the other page. This way user can be redirected to a malicious page. X-Frame-Options header in HTTP responses must be set in order to prevent these attacks. This problem was reported on every page that contains a form.

Alerts with the lowest level of risk, that nevertheless should be considered are:

- Absence of Anti-CSRF token,
- Content Security policy header not set,
- Cross-Domain JavaScript source file inclusion,
- Web browser XSS protection not enabled,
- For password field with autocomplete enabled.

Other alerts are informational kind. In order to better estimate application security, manual tests

should be performed. Those alerts are:

- Character set not specified,
- AJAX code detected,
- Information disclosure – suspicious comments that could help attackers.

From the above stated, it can be concluded that application is not entirely secured and that attackers can get to information from a database and files that are on the server. In order to stop attacks and save data, it is necessary to apply all techniques, i.e. if a web application is for a financial organization, loss would be enormous if attacks occur.

CONCLUSIONS

With turbulent advancement of technology and even faster development of web applications, testing becomes a real challenge. Instead of evaluating software after process of development, testing should be a part of development cycle, in order to prevent errors that could lead to problems in production. Therefore, many organizations choose to use agile software development methodologies.

Security testing is predicted to have a significant growth of importance in future. Estimated market value equals 594.7 million of dollars in this year, and it is expected to rise to 1.724 million in 2021. The rise of web application testing is correlated with the increase of hacker attacks.

In order for web application to satisfy all non-functional requirements, it is necessary to apply all kind of tests during application development. Testing should be executed by qualified and experienced testing team. Which tools, methodologies and testing strategies should be used depends on company's necessities. For example, if application contains confidential data, testing should be done with extreme care, because unidentified problems can have serious financial, legal or reputation consequences for organization.

ACKNOWLEDGMENT

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

BIOGRAPHY

Ksenija Živković is a MSc candidate at University of Belgrade, Faculty of Organizational Sciences, Department for Information Technology. She currently works as Project Assistant at msgNetconomy, Belgrade. She published several research papers and her interests include software engineering, web security and biometrics.

Ivan Milenković is a PhD candidate at University of Belgrade, Faculty of Organizational Sciences, Department for Information Technology. He currently works as a researcher at Laboratory for multimedia communications in Belgrade, Ser-

bia. He published several research papers and participated in several research and commercial projects in Information Technology area. His interests include biometrics, computer security and mobile technologies.

Dr Dejan Simić is a full professor at University of Belgrade, Faculty of Organizational Sciences, Department for Information Technology. He is engaged as a researcher at Laboratory for multimedia communications in Belgrade, Serbia. He published many research papers and participated in several research projects in Information Technology area. His interests include biometrics, computer security and e-commerce.

REFERENCES

- [1] Chung L, and do Prado Leite J C S (2009) On non-functional requirements in software engineering. In *Conceptual modeling: Foundations and applications* (pp. 363-379), Springer, Berlin Heidelberg.
- [2] Mervi J, Joonas M (2015) Non-functional testing: security and performance testing, Bachelor's Thesis, JAMK University of Applied Sciences, Available:
- [3] http://www.theseus.fi/bitstream/handle/10024/110354/Joonas_Moilanen_Mervi_Jeskanen.pdf?sequence=1 [Accessed 5 August 2016].
- [4] Myers G et al (2011) *The art of software testing*, John Wiley & Sons, ISBN 978-1118031964
- [5] Official Vega software page, Available: <https://subgraph.com/vega/> [Accessed 6 August 2016]
- [6] OWASP - Definition of fuzzing, Available: <https://www.owasp.org/index.php/Fuzzing>, [Accessed 5 September 2016].
- [7] Path traversal attack description, Available: https://www.owasp.org/index.php/Path_Traversal [Accessed August 2016]
- [8] PHP supported version, Available: <http://php.net/supported-versions.php>, [Accessed 15 August 2016].
- [9] PlayStation Network hackers access data of 77 million users, Available:
- [10] <https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data> [Accessed 22 August 2016]
- [11] Popović J (2014) *Testiranje softvera u praksi*, ISBN 978-86-7991-363-0, CET, Beograd
- [12] Steinberg J (2014) *Massive Security Breach At Sony*, Available:
- [13] <http://www.forbes.com/sites/josephsteinberg/2014/12/11/massive-security-breach-at-sony-heres-what-you-need-to-know/#789e36ece9a5> [Accessed 22 August 2016]
- [14] Tomic B, Vlajic S (2008) Functional Testing for Students: a Practical Approach, *Inroads - ACM SIGCSE Bulletin*, Vol. 40, No. 4, pp. 58-62, ISSN 0097-8418, DOI 10.1145/1473195.1473221
- [15] Volvo recalls 59,000 cars over software fault, Available: <http://www.bbc.com/news/world-europe-35622753> [Accessed 18 August 2016]

Submitted: November 24, 2016.

Accepted: November 30, 2016.

THE IMPACT OF FELDER'S LEARNING STYLES INDEX ON MOTIVATION AND ADOPTION OF INFORMATION THROUGH E-LEARNING

Željko Pekić

Maritime Faculty Kotor, zeljko.pekic@ac.me

Srđan Jovanovski

Faculty of Information technology, srdjan.jovanovski@unimediteran.net

Nada Pekić

Centar za socijalni rad Kotor, nadjadjikanovic@hotmail.com

Case Study

DOI: 10.7251/JIT1602093P

UDC: 37.018.43:004.738.5

Abstract: In this paper, we examined the nature and distribution (direction and intensity) of motivation for using e-learning, focusing the connection between the independent variables on one side and the Felder's learning style on the other. The most relevant information that we wanted to examine and present is the individual ways of the respondents in adopting the same material. We were also interested in the ways to technically adjust the information delivery. The results confirm the statistical significance of the initial idea.

Keywords: e-Learning, motivation, learning style, placement of materials, adoption of information.

INTRODUCTION

In the forties of the twentieth century, the teams of engineers and psychologists were actively working on examining the relationship between the optimization in handling different types of machinery and efficient transmission and reception of information. It was found that the transmission and reception of information had limitations that were not of technological nature, but limitations of the cognitive system. Attention, selection and optimization of information transmission have become the focal problem of the research. In order to fully comprehend such problem, it is necessary to find a reasonable analogy between an abstract communication system and functioning of the nervous-sensory apparatus.

The mathematical formulation of information theory was given by Claude Shannon, but the basics of the approach were given by Andrei Kolmogorov [26]. They define the information as the probability of

events in a system, where the content of information is irrelevant. If the probability of event is lower than the quantity of information carried by this event is higher. This means that the amount of information carried by an event is inversely proportional to its probability.

Martin Dougiamas, working on his doctoral dissertation on the use of open source software to support education on the Internet, launched the idea of developing the Moodle platform. Dougiamas is the leading Moodle programmer of today [10].

LEARNING

It is important to emphasize that learning permeates almost every human activity. There is a large number of factors acting as indirect learning tasks. Firstly, it is the perception, as a general human mode of operation and a dose of idiosyncrasy. Stimulated by various stimuli, it presents its own value. Its latent importance

is in the perception of the previously seen, through experiences and connections with the new. Motivation also plays an important role in acquiring knowledge. Certainly, a man of certain age has defined certain motives, but additional motives can be excited by other people or specific relevant materials.

Today, in the 21st century we live in a computer world where production, processing and storage of knowledge are very important factor of a complete social progress. Education as one of the basic pedagogical category anticipates vocational training and life skills development through the acquisition of knowledge [20]. The basic elements of education are knowledge and competence, where knowledge is defined as a system of scientifically based facts that students gain and practically apply. The term information technology was first used by Jim Domsik in 1981 as a substitute for the term data processing, but the information technology anticipates the use, storage, production and exchange of information [19]. In the last decades, the development of information technology has recorded unprecedented growth and is further progressing. The essence of technological development comprises a complex range of information and communication technologies. The future development of information technology lies in the integration of the system, standardization of equipment, the Internet dispersal, higher speeds, but it also depends on new inventions, changing the world even more than expected [7].

MOODLE PLATFORM

Electronic learning (e-Learning) is a type of education based on the use of modern technologies for creating, presenting of educational content, as well as the adoption of material. Suppose we have a forum where a student has the opportunity to download some material, but also to ask questions to a professor[1]. Asking questions does not guarantee a response within a specified time period, the professor will answer questions when available and "online". The disadvantages of this approach have been avoided by the use of synchronous technologies such as web and video conferencing, IP telephony. Attending lectures and discussions in real time provide added value to distance education, so that group work leads to generating more ideas.

This form of communication has been experienced more responsibly by students than professors. They are 2-3 times more likely to send messages and much more responsive to those received [21].

Educational platforms are complex tools that enable controlled distribution of multimedia and text lessons to all or selected users enrolled in a course, either through conventional or distance education. That way we can track approaches to a text, note changes and add comments. To testing the student on computers, you can use many free and simple programs that can easily fit into classes, so it is very easy to test students who are not physically present in the classroom [28].

The market offers specific tools that enable easy content creation, setting presentations, forums, all with the aim to enable users to focus on the content itself, not on the techniques of presentation [6].

Moodle is a free, open source platform for e-Learning. This very popular platform has more than 57 million users. According to many surveys published on the Internet, moodle is one of the best accepted platforms in its segment [22].

Moodle is a Course Management System (CMS), also known as a Learning Management System (LMS), or a Virtual Learning Environment (VLE). It is a free web application that educators can use for creating efficient online learning sites. There are also many additional ways to use it [2].

The focus of the Moodle project is to provide teachers with the best tools to manage and promote learning. Built-in functionality allows exactly the same procedures in the work whether it has a couple of users, or dozens, hundreds of thousands of active users. Due to its scalability, it has been applied both to private users that provide courses for a small number of users, and to huge systems having over 50 thousand users [24].

Moodle characteristics are as follows [25]:

- Built-in support for the evaluation and monitoring of student activities,
- Roles system can be adjusted to the level of activity
- Supports collaboration through forums, chat, wiki's and other modules,
- Supports the development of tests with different types of tasks,

- Supports imports of standardized packages for learning objects,
- A number of free plug-ins are available on the Internet
- Moodle has been localized in 78 languages.

MOTIVATION

Motives are movers, tendency to achieve and adopt the goal and psychological processes supporting us in our efforts. The psychological motives comprise learning incentives (means of motivation) such as: grades, praise, critics, competition etc. [27].

It is important to understand the difference between traditional learning and modern active teaching. The emphasis is not on technology, but on a higher involvement of students, their encouraged motivation, resulting in knowledge. In the traditional teaching we had a simple system, the professor teaches, the students listen (regardless of the attention, motivation and desire). In more contemporary form of teaching, students do not feel such a drastic hierarchical distinction between themselves and lecturers. This way they are equally involved, important, and can provide innovative contributions to this kind of teaching. The important finding is that learning has stimulating effect on the involvement of two sensory modalities (hearing and vision), unlike traditional style, solely listening. But active teaching is just one step that binds innovation in teaching and online learning. It brings a series of new ways and knowledge sharing and acquiring.

In particular, strict requirements regarding attendance for lessons and exercises and limited number of examination terms are absolutely incompatible with the needs of active seafarers, who spend few months, half a year, or longer onboard ships, but who would like to, or need to improve their knowledge in order to keep their jobs and/or get a career advancement [4].

The material adopted by students through these classes needs to be related to earlier contents, preferably through experience, through a positive transfer [15]. Furthermore, the student should have a personal way of adopting materials, adjusted to the most suitable strategy of idiosyncratic personality and di-

versity of opinion. Interpretation is also a free alternative upon each individual. It is also an opportunity for expressing a personal touch of each participant.

There are two types of motivation [13]:

Extrinsic (external) motivation:

- focused on fulfillment of obligations in the subject
- is strongly influenced by incentives or pressures coming from outside;
- leads toward superficial approach to learning and the fear from failure;
- outcomes are not flexible and cannot be easily transferred to various application contexts (knowledge is "rigid").

Intrinsic (internal) motivation:

- reflects a personal goal;
- results from the interest in the field of study;
- depends on personal engagement in tasks that can be selected;
- depends on the feeling of their own competence and self-confidence;
- leads to a deep approach to learning and understanding of concepts;
- outcomes are flexible and can be easily transferred to various application contexts.

FELDER'S LEARNING STYLES

Learning styles can be defined as a method through which an individual focuses on new and complex information, process them, reform them into knowledge, persisting and using the acquired knowledge. "The style of learning is an established and dominant way of receiving, processing and use of stimulus / information in the learning process, and the most recognizable in the course of organized learning in the classroom; it's a way of dominating the mental representation and processing of the learning content" [5].

Learning can be defined as a complex process acknowledging the influence on students, teachers, motivation, interaction and cohesion of these factors [9]. The earlier learning process has changed. The basics have remain the same. The principle transfer - adopt knowledge - is still the main driver of the process. Everything that comes along is additional learn-

ing motivators, positively correlated by their intensity. The technical revolution has brought a number of innovations with their advantages and disadvantages.

Felder-Silverman model examines three issues [18]:

- a) a distinctive learning style with an alternative way to process information and its significance for engineering education;
- b) learning style most preferred by students and teaching style most favored by teachers and
- c) strategies undertaken by students, which are not equivalent to standard methods of engineering education.

Learning in a structured educational system has two important steps:

- a) reception of external information through senses;
- b) the inside information, to be processed by a specific method or simply ignored.

A further process may include short-term or long-term memory, through repetition or detailed analysis. Felder-Silverman model classifies students into one of the four learning styles:

- a) Sensory students (specifically, practically oriented towards facts and procedures) or intuitive students (conceptual, innovative, oriented theories and very important);
- b) Visual learners (preferring visual presentations of the material - images, diagrams) and verbal learners (preferring written and spoken explanations);
- c) Active students (through interaction and continuous work) or reflective students (working and thinking by themselves);
- d) Sequential learners (neat, learn in small steps, upon a detailed scheme and work division) or global learners (holistic, systematic thinkers, learning in big steps forward) [11].

The model emphasizes the importance of adapting the teaching process to one of the styles or at least one of the two style dimensions, e.g. visual or intuitive style of teaching, and stimulating environment for such strategic type.

The first dimension - sensory / intuitive, is one of the four dimensions of the Jung's theory of psycho-

logical types, and the third dimension - active / reflective, is a component of the Kolb's learning style. The second dimension - visual / verbal, is analogous to the visual-auditory-kinesthetic modality of the theory formulation and rooted by the cognitive study of information processing. The fourth dimension - sequential / global, has been developed eclectically.

For sensual students to remember and understand information, it is best to enable them sense the way it relates to the real world. If they are in a class where the most of material is of an abstract and theoretic type, they will be prone to have difficulties. Instructors for specific examples of suitable concept examples will know which model should be applied in practice. If the instructors do not provide sufficient specifics, stimuli and motivation, it will not produce a positive effect.

In the Felder's model, visual dimension refers to internal processing (such as visualization) rather than a sensory stimulus. There are evidences from studies on brain hemispheres and clinical observations showing that global learners are more likely to use visual processors, a sequential learners are more likely to use verbal processors [11]. Felder made two significant changes to his model in 1987. The first change was the deletion of inductive / deductive dimension due to the misunderstandings of the instructors in the distribution of materials for inductive or deductive methods of teaching. The second change was the renaming of category visual learners / spectators into visual / verbal. Felder made this change to allow both spoken and written word to be included in the verbal category [12].

Kolb says that learning involves the provision of abstract concepts that can be flexibly applied in various situations. In the Kolb's theory, a stimulus for the development of new concepts provides new experiences [17].

AIM AND OBJECTIVES OF THE RESEARCH

The initial aim of research is to assess the nature and distribution (direction and intensity) of motivation in e-learning, as an independent variables on one side and the Felder's learning styles, as a dependent one on the other.

Research Objectives

The research has a two-fold objective:

a) **Scientific objective**- aiming to determine the type and nature of relationship between e-Learning motivation and learning styles, also wishing to use the obtained results for further research on this and similar fields.

b) **Practical objective** – aiming to use the data obtained for contributing to more efficient and practical work of educational institutions in the country and encourage effective engagement of individuals (students and teachers) who would readily act towards enhancing the educational system of Montenegro.

Variables in the research:

a) Considering the dependent variable, we have been examining students' motivation for e-Learning at the Maritime Faculty of Kotor. The motivation scale has 5 items and has been designed by the author. The Krombah's alpha coefficient is 0,67;

b) As intervening variables, we examined the impact of the Felder's learning styles to knowledge acquisition. The testing scale for the Felder's learning styles, with 44 items and of the Likert's type, was designed by Richard M. Felder and Linda Silverman. It had been originally designed by Felder and Solomon, with subsequent modification.

c) The independent variables were student experiences with e-Learning.

RESEARCH METHODOLOGY

The Sample

The survey was conducted on a sample of 100 respondents. It consists exclusively of the students of the Maritime Faculty in Kotor. The sample has elements of intentional.

While processing of data, the following statistical procedures were applied:

- a) the frequencies and percentages;
- b) differentiation measures for the segments of crossed variables (Pearson Chi-square);
- c) measures that indicate the rate of correlation among the variables (C - Contingency coefficient).

Research Results

Table 1. Results of the dependent variable (motivation for using e-Learning)

No.	Items	A.S.
1.	This kind of learning is an innovation leading the educational process into progress.	3.90
2.	Learning this way is efficient both for students and teachers.	3.74
3.	I gladly give suggestions for possible changes in the work of electronic forms of teaching process.	3.66
4.	Aquisition of knowledge by this method of learning is easy.	3.51
5.	E-Learning is a motivating method of teaching/learning.	3.04

The arithmetic mean - the average is the most commonly used measure of central tendency. Its definition is simple: sum of data values divided by the number of data.

Table 1 shows the order of items that are had the highest to the lowest value of the arithmetic mean. Item No. 1 is the claim with the mean value perceived by students as the most positive one. And so on for all five. They are very minor differences in the values of all items, which implies that students are generally strongly motivated for the use of this type of learning.

Table 2. Display items independent variables (general experience of e-Learning)

VARIABLE	FREQUENCY	PERCENTAGE
<i>I like the e-Learning method</i>		
YES	89	89%
NO	11	11%
<i>This kind of learning I evaluate as</i>		
BAD	9	9%
GOOD AND EXCELLENT	91%	91%

Table 2 shows the percentage of student motivation and satisfaction with e-Learning. In a large percentage (89%), students like this kind of work and evaluated it as good or excellent (91%). This means that this kind of teaching generally suits the respondents, with the modification of individual segments, i.e. while adapting the learning styles.

Table 3. Frequency percent of the Felder’s learning styles

LEARNING STYLE	FREQUENCY	PERCENT
Active / reflective	19	19%
Visual / verbal	41	41%
Sensory / intuitive	22	22%
Sequential / global	18	18%

Table 3 shows the frequency percent of the Felder’s learning styles. What is the most striking is that more than 40% of the respondents preferred the visual-verbal learning style, while other styles are quite balanced.

Table 4. Correlations between dependent and independent variables (motivation and learning styles)

1. Motivation for the use of e-learning and the active-reflective subjects			
$\chi^2 = 2.888$	df = 4	c = 0.179	p = 0.875
2. Motivation for the use of e-learning and visual-verbal			
$\chi^2 = 11.007$	df = 4	c = 0.157	p = 0.050
3. Motivation for the use of e-learning and sensory-intuitive			
$\chi^2 = 4,355$	df = 4	c = 0.156	p = 0.512
4. Motivation for the use of e-learning and sequential-global			
$\chi^2 = 5.677$	df = 4	c = 0.197	p = 0.617

Differentiation measures for the segments of crossed variables (Pearson Chi-square).

Pearson’s correlation coefficient (r) is used in cases where the variables of observed model show a linear correlation and continuous normal distribution. The value of the Pearson correlation coefficient ranges from +1 (a perfect positive correlation) to -1 (perfect negative correlation). The “+” or “-“indicates the direction of correlation - whether positive or negative, but it does not refer to the strength of correlation.

The **p** value indicates the statistical significance that exists or does not exist. If there is one, then its value ranges from **0,000** to **0,050**.

Table 4 clearly shows the correlation between the motivation for the use of e-Learning and the Felder’s learning styles. Out of the four learning styles, only the visual / verbal style is positively correlated with

motivation. This is indicated by the value **p = 0.050**, which is the statistical significance at the level 0.05 and Hi square value of 11. This means that students with greatest interest in this kind of learning belong to the visual-verbal learning style.

$$r = \sqrt{r^2} = \frac{SD_{xy}}{SD_x SD_y} E [-1, +1]$$

$$t = \frac{r\sqrt{n-2}}{\sqrt{1-r^2}}, df = n - 2$$

The measures show the degree of correlation between the variables (**C - Contingency coefficient**), a measure of association between statistical variables which have quantitative categories of unequal magnitude or at least one of which can be classified only qualitatively.

$$C = \sqrt{\frac{\chi^2}{N + \chi^2}}$$

Df is the number of degrees of freedom, i.e. the number of values in the final statistical calculation, which is free to vary.

χ^2 (Chi-squared)

$$\chi^2 = \sum \frac{(f_o - f_t)}{f_t}$$

f_o - required frequency

f_t - expected frequency

Σ - sum

CLOSING REMARKS

At the beginning of the paper we were engaged in theoretical part and hypotheses about impact on the adoption of information among the respondents. In particular, we focused on the dependent variable, i.e. the Index of the Felder’s styles of learning that have proved to be a relevant variable in this study. Through operational defining of the variables we obtained the results that the visual-verbal learning style is the most dominantly present among the respondents and the only one having a positive correlation with the independent variable.

Visual learners are best in remembering the contents they can see, whether that is schemes, diagrams, graphs, demonstrations. The verbal respondents were

better in remembering by using sensory materials, meaning that they are prone to acquire information with sound but with no images. These are audio recordings, oral texts, verbal presentations, etc. [16].

It should be noted that many studies showed that the majority of the visual-verbal respondents belong to the visual type. This percentage reaches up to 70% [11].

CONCLUSION

The existing technologies enable and provide the basis for the existence of universal society i.e. information society. No one is to be excluded from the education society, as guaranteed by the Law. Knowledge is a public property accessible to everyone. The technological progress i.e. the emergence and development of technological innovation allow for the development of creativity and further innovation, or generation of new ideas.

Regardless of the student motivation and satisfaction with the teaching forms of today, it is necessary to introduce continuous innovation also at the level of individual. As this and other studies show, students and teachers are still not enough aware of the possibilities to make their jobs easier and practical with an appropriate form of providing information.

The research results show the following:

- 89% of the respondents are satisfied with e-Learning;
- 91% of the respondents who are satisfied with e-learning believe that this form of learning is good or excellent;
- As for the Felder's learning styles, more than 40% of the respondents preferred the visual-verbal learning style, while other styles are quite balanced and
- In examining the correlation between dependent and independent variables, the found statistical significance was at the level 0.05, with the satisfaction in e-Learning and visual-verbal type of acquiring knowledge.

As shown by the research results, it is necessary to note that the subjects/respondents mostly have an emphasized visual intelligence. Individuals who have a high coefficient in this kind of capabilities have a personal style of adopting information. When such an individual at-

tempts to extract information from the long-term memory, (s)he uses the visualization mnemonics and creating of images in her/his mind. This ability is a good predictor of geometry jobs, jobs with the spatial orientation, but in the adaptation to a new environment.

They find it easier to interpret images, layouts, diagrams, charts, numbers, etc. They like to assemble three-dimensional objects. And as their future occupations they usually choose engineering, architecture, sculpture, mechanics and visual arts.

These data leave place for further research in the same and similar fields. They also confirm the fact that e-Learning is a specific and attractive form of education, and, as such, it modifies the human awareness, simplifying the process of teaching/learning and adapting it to the needs of its users.

BIOGRAPHY

Zeljko Pekic, Spec.Sci. Zeljko Pekic was born in Bar, Montenegro, in 1984. He received the Spec.Sci. degree in Computer Engineering at the University of Montenegro, Podgorica, in 2009. Currently a postgraduate student of computer science in Podgorica. Since 2011, he is employed at the University of Montenegro – Faculty of Maritime Studies, at the post of computer laboratory system engineer. His area of interest includes computer engineering, networks, advanced forms of e-Learning, learning styles, etc.

Srdan Jovanovski, D.Sc. Srdan Jovanovski was born on August 30 1982 in Bar, Montenegro, where he finished elementary and high school. For great results during education he was rewarded twice with the diploma "LUČA". He entered Faculty of Electrical Engineering of University of Montenegro in Podgorica in 2001/02.

On September 13, 2004, he received degree Bachelor of Science (BSC) in Electrical Engineering, and his diploma is the first one of that type at the University.

On June 18, 2005, he received his second degree in Electrical Engineering "Hardware systems for time-frequency signal analysis", Department of Electrical Engineering, the University of Montenegro, supervised by prof. dr Veselin Ivanović.

On November 4, 2006, he received his MS degree in Electrical Engineering "Design of the systems for time-frequency signal analysis based on the S-method realization using short time Fourier Transform" M.S. thesis, Department of Electrical Engineering, the University of Montenegro, supervised by prof. dr Veselin Ivanović.

On May 13, 2010, he received his PhD degree "Specialized multyclock-cycle signal adaptive architectures for highly nonstationary single dimensional and multidimensional signals analysis and time varying filtering", PhD dissertation, Department of Electrical Engineering, the University of Montenegro, supervised by prof. dr Veselin Ivanović.

Current areas of interest:

- Time-frequency signal analysis
- Time-varying filtering
- Design of special purpose hardware for signal analysis
- Hardware/software codesign
- Architectures and design of computers
- Design of microcontrollers

Active member of the Young Researchers Centre of Montenegrin Academy of Arts and Sciences

Nadja Pekić, Spec. Sci. Nadja Pekić was born in Nikšić, Montenegro, in 1983. She received the Spec. Sci degree in Psychology at the University of Montenegro, Nikšić, in 2012 as a student of generation. Since 2013, she works at the Center for social work, Kotor, at the position of psychologist. In 2016, she acquired the degree of Professional transactional analysis practitioner at the Institute Psihopolis in Belgrade, which she continues to attend while training to be a psychotherapist. Her area of interest includes: counseling psychological research, e-Learning, emotional intelligence, defense mechanisms, etc.

LITERATURE

- [1] Aničić, O., Barlovač, B. (2010). Učenje na daljinu – e-obrazovanje. U: Tehnika i inforamtika u obrazovanju, 3. Internacionalna Konferencija, Čačak, Tehnički fakultet
- [2] Bauk S., Dlabač T., Pekić Ž., “Implementing E-learning modes to the students and seafarers education: Faculty of maritime studies of Kotor case study”, IMSC 2012., June 16 th -17th, Split 2012. (Zbornik radova, pp 247-254)
- [3] Bauk S., Kopp M., Avramović Z., A Case Study on Introducing E-learning into Seafarers’ Education, JITA - Journal of Information Technology and Applications (ISSN:2232-9625), Volume 3, Issue 1, June 2013, Page(s) 34-43
- [4] Bjekić, D., Dunjić-Mandić, K. (2007). Stilovi učenja i profesionalne preferencije maturanata gimnazije, Preuzeto 26.02.2010. iz Pedagogija LXII 1/07, 48-59. sa veb stranice: <http://scindeks-clanci.nb.rs/data/pdf/0031-3807/2007/0031-38070701048B.pdf>
- [5] Bjekić, D. (2008). Psihologija e-učenja i e-nastave 6, 1-17
- [6] Bishop M., (2004). Introduction to Computer Security, Chapter 18: Evaluating Systems Wesley and Sons, November 1
- [7] Bransford, J. (2000). How people learn: Brain, mind, experience, and school. Washington, D. C.: National Academy Press.
- [8] Cooper, C. (1975) .Theories of Group Process, London: John Wiley. T.A. Litzinger, S.H. Lee, J.C. Wise, and R.M.
- [9] Dougiamas, M. and Taylor, P.C. (2003) Moodle: Using Learning Communities to Create an Open Source Course Management System. Proceedings of the EDMEDIA 2003 Conference, Honolulu, Hawaii.
- [10] Felder, R.M. and Silverman, L. K. (1988). Learning and Teaching Styles in Engineering Education, Foreign Language Annals, 28 (1), 21–31 (1995)
- [11] Felder, R.M. and Silverman, L.K. (1987) “Learning Styles and Teaching Styles in Engineering Education, ” Presented at the 1987 Annual Meeting of the American Institute of Chemical Engineers, New York.
- [12] Goleman, D. (1995). *Emotional intelligence*. New York: Bantam.
- [13] He, K. (2004). Blending learning and the development of educational technology theory. Educational Technology of China.
- [14] Heiskanen, E., Pantzar, M.: Toward Sustainable Consumption: New Perspectives, Journal of Consumer Policy, No. 20, 1997.
- [15] Honey, P & Mumford, A., (1983). Using Your Learning Styles. Maidenhead, UK, Peter Honey Publications
- [16] Kolb. D. A. & Fry, R. (1975). Toward an applied theory of experiential learning.
- [17] Litzinger, S.H. Lee, J.C. Wise, and R.M. Felder, “A Psychometric Study of the Index of Learning Styles.” *J. Engr.Education*, 96(4),309-319(2007).Reliability, factor structure, and construct validity of the *Index of Learning Styles*
- [18] Milosavljević M., Grubor G., Osnovi bezbednosti i zaštite informacionih sistema, Univerzitet Singidunum, 2006.
- [19] Pekić Ž., Đikanović N., “Stav o e-Learningu i stilovi učenja”, Informacione tehnologije IT 2013., Februar 26 th – March 1th, Žabljak 2013.
- [20] Pekić Ž., Pekić N., Kordić S., Kovač D., Dlabač T., “Analiza online komunikacije i interakcije kroz e-Learning”, Informacione tehnologije IT 2014, Žabljak 2014.
- [21] Pekić Ž., Pekić N., Kovač D., Dlabač T., “HOW LEARNING STYLES AFFECT THE EXPERIENCE OF E-LEARNING”, IMSC 2014., April 28 th -29th, Solin 2014.
- [22] Pekić, Ž., Pekić, N., Kovač, D., “Influence motivational factors and learning styles on efficiency e-learning”, 8th International Conference on Ports and Waterways, POWA 2013
- [23] Sasikumar, M. (2008). *Moodle Your Way to Elearning*. Copyright CDAC Mumbai
- [24] Shannon, C. E. (1948). “A Mathematical Theory of Communication”. Bell System Technical Journal. 27
- [25] Stevanović, B. (1984): „Pedagoška psihologija“. Zavod za udžbenike i nastavna sredstva, Beograd.
- [26] <http://slidehot.com/resources/integracija-moodle-sms-master-rad-biljana-djukanovic-fon.832511/>

Submitted: November 1, 2016.

Accepted: November 29, 2016.

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 Lincoln 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 Lincoln 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

EDITORS

Gordana Radić, PhD, Editor-in-Chief (B&H)

Zoran Ž. Avramović, PhD, (B&H)

Dušan Starčević, PhD, (B&H)

EDITORIAL BOARD

Zdenka Babić, PhD, (B&H)

Leonid Avramović Baranov, PhD, (Russia)

Patricio Bulić, PhD, (Slovenia)

Valery Timofeevič Domansky, PhD, (Ukraine)

Hristo Hristov, PhD, (Bulgaria)

Emil Jovanov, PhD, (USA)

Petar Marić, PhD, (B&H)

Vojislav Mišić, PhD, (Canada)

Igor Esaulenko, PhD (Russia)

Valery Popov, PhD (Russia)

Boško Nikolić, PhD, (Serbia)

Dragica Radosav, PhD, (Serbia)

Gjorgji Jovanchevski, PhD, (Macedonia)

Branko Latinović, PhD (B&H)

Vladimir Nikolajevič Mališ, PhD (Russia)

Goran Đukanović, PhD (B&H)

Yidong Li, PhD (China)

EDITORIAL COUNCIL

Siniša Aleksić, APEIRON University, Director

Esad Jakupović, APEIRON University, Rector

TECHNICAL STAFF

Stojanka Radić, Lector

EDITOR ASSISTANTS

Sretko Bojić, APEIRON University

Gordan Ružić, ETF University of Belgrade

ISSN 2232-9625



9 772232 962005