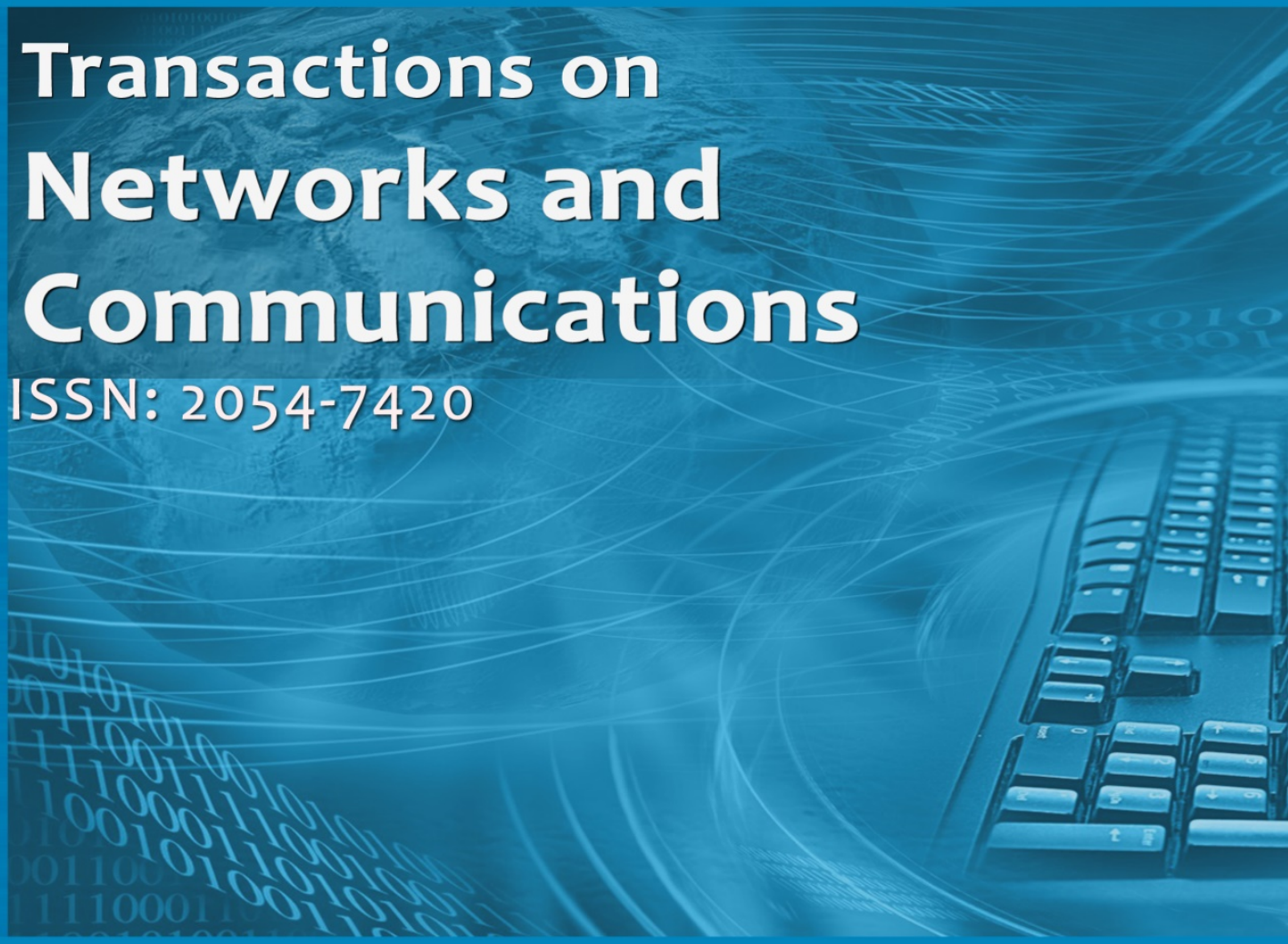
Volume 2. Issue 4 - August 2014

Transactions on Networks and Communications

ISSN: 2054-7420



Society for Sciences and Education - United Kingdom

TABLE OF CONTENTS

EDITORIAL ADVISORY BOARD

DISCLAIMER

All the contributions are published in good faith and intentions to promote and encourage research activities around the globe. The contributions are property of their respective authors/owners and the journal is not responsible for any content that hurts someone's views or feelings etc.

TNC Transactions on Networks and Communications
SOCIETY FOR SCIENCE AND EDUCATION UNITED KINGDOM
VOLUME 2, ISSUE 4
ISSN: 2054 - 7420

Binary Division Attack for Elliptic Curve Discrete Logarithm Problem

Boris S. Verkhovsky, Yuriy S. Polyakov
Department of Computer Science, New Jersey Institute of Technology, USA;
verb73@gmail.com, polyakov@njit.edu

ABSTRACT

Elliptic curve cryptography (ECC) is an approach to public key cryptography (PKC) that is based on algebraic operations with elliptic curves defined over finite fields. Security of elliptic curve cryptography is based on the hardness of the elliptic curve discrete logarithm problem (ECDLP). Although there is no theoretical proof that ECDLP is intractable, no general-purpose sub-exponential running time algorithm has been found for solving the ECDLP if the elliptic curve parameters are chosen properly. In this study, we develop a new security attack based on the binary division of elliptic curve points over prime fields that may be used to solve the ECDLP when the order q of elliptic curve satisfies the congruence $q = 2 \pmod 4$. To perform the binary division, we devise a novel algorithm of point halving on elliptic curves defined over prime fields that applies to the cases when $q = 1 \pmod 2$ and $q = 2 \pmod 4$. The binary division attack has exponential worst-case asymptotic time complexity but in certain practical cases can be used to solve the ECDLP in a relatively efficient way. We therefore make a recommendation to avoid the case of $q = 2 \pmod 4$ in elliptic curve cryptosystems.

Keywords: Elliptic Curve Cryptography, Discrete Logarithm Problem, Security Attack, Point Halving, Cryptoanalysis, Public-Key Cryptography.

1 Introduction

Elliptic curve cryptography (ECC) is an approach to public key cryptography (PKC) that is based on the algebra of elliptic curves defined over finite fields. ECC is more efficient than RSA and discrete logarithm (DL) systems: smaller keys in ECC can be used to achieve the same security level as in RSA and DL systems [1]. The ECC algorithms substantially outperform both RSA and DL systems when carrying out private-key operations, such as digital signature generation and decryption. The benefits of ECC are most pronounced when processing power, storage, bandwidth, or power consumption is constrained.

An elliptic curve E over a field K is defined by a Weierstrass equation [1]

DOI: 10.14738/tnc.24.293
Publication Date: 4th August 2014
URL: http://dx.doi.org/10.14738/tnc.24.293

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ , \tag{1}$$

where constants $a_1, a_2, a_3, a_4, a_6 \in K$ and discriminant $\Delta \neq 0$.

If the characteristic of *K* is not equal to 2 or 3, then Equation (1) can be simplified to

$$E: y^2 = x^3 + ax + b \ . \tag{2}$$

where coefficients $a, b \in K$. Here, the transformed coordinates *x* and *y* are obtained using the admissible change of variables

$$(x, y) \to \left(\frac{x - 3a_1^2 - 12a_2}{36}, \frac{y - 3a_1x}{216} - \frac{a_1^3 + 4a_1a_2 - 12a_3}{24} \right). \tag{3}$$

The discriminant of this curve is evaluated as $\Delta = -16\left(4a^3 + 27b^2\right)$.

The security of all ECC schemes is based on the hardness of the elliptic curve discrete logarithm problem (ECDLP) formulated as follows [1]: given an elliptic curve *E* defined over a finite field $\mathbb{F}_u$, a point $P \in E(\mathbb{F}_u)$ of order *n*, and a point $Q \in \langle P \rangle$, where $\langle P \rangle$ is the subgroup of *E* generated by *P*, find the integer $t \in [0, n-1]$ such that

$$Q = tP \ . \tag{4}$$

The integer *t* is called the discrete logarithm *Q* to the base of *P*, denoted $t = \log_P Q$.

The main attacks on the ECDLP include Pohlig-Hellman algorithm [1], Pollard's rho attacks and its modifications [1-5], and several isomorphism attacks that attempt to efficiently reduce ECDLP to the discrete logarithm problem (DLP) known to have sub-exponential algorithms [1]. The most efficient general-purpose attack on the ECDLP is a combination of the Pohlig-Hellman algorithm and Pollard's rho algorithm (or its modifications), which has a fully-exponential running time of $O\left(\sqrt{p}\right)$, where *p* is the largest prime divisor of *n*. Sub-exponential algorithms devised using isomorphism attacks are available only for special cases [1].

The special-purpose attacks, particularly those associated with polynomial-time and subexponential-time running times, are examined to devise countermeasures for verifying that a given elliptic curve is immune to these attacks. Currently, the following cryptographically weak special cases and corresponding countermeasures are known. (1) The Pohlig-Hellman algorithm reduces the computation of $t = \log_P Q$ to the computation of discrete logarithms in the prime order subgroups of $\langle P \rangle$ [1]. This implies the elliptic curve parameters should be selected to yield the order *n* of *P* that is divisible by a large prime. (2) For prime-anomalous elliptic curves ($\#E(\mathbb{F}_u) = p$) , ECDLP can be transformed to an equivalent DLP as part of the Araki-Satoh-Semaev-Smart attack [1]. It is simple to circumvent this attack by verifying that

$\#E(\mathbb{F}_u) \neq p$. (3) In the case when gcd(*n*,*u*) = 1, the Weil and Tate pairing attacks find an isomorphism between $\langle P \rangle$ and a subgroup of order *n* of the multiplicative group $\mathbb{F}_{u^k}^*$ of some extension field $\mathbb{F}_{u^k}$ [1]. To ensure that an elliptic curve *E* defined over $\mathbb{F}_u$ is not susceptible to the Weil and Tate attacks, it is sufficient to check that *n*, the order of the base point $P \in E(\mathbb{F}_u)$, does not divide $u^K - 1$ for all small *k* for which the DLP in $\mathbb{F}_{u^k}^*$ is tractable (for $n > 2^{160}$, the verification interval of *k* is [1,20]). (4) To protect against the Weil descent attack specifically designed for binary fields [1], it is suggested to avoid the use of elliptic curves $\mathbb{F}_{2^m}$, where *m* is composite.

The two kinds of elliptic curves recommended by the National Institute of Standards and Technology (NIST) for cryptographic protocols are elliptic curves over binary fields $\mathbb{F}_{2^m}$ (with the characteristic of 2) and elliptic curves over prime fields $\mathbb{F}_p$ (with the characteristic of *p*) [1, 6]. Ten specific elliptic curves over $\mathbb{F}_{2^m}$ and five elliptic curves $\mathbb{F}_p$ are recommended in the FIPS 186-2 standard for U.S. federal government use [6].

In this paper, we devise a "binary division" attack for elliptic curves defined over prime fields $\mathbb{F}_p$ that is based on the binary division of the integer $t = \log_P Q$. The binary division approach was previously examined for binary fields [7]. It was shown that this method has exponential complexity due to the fact that every point halving for the elliptic curves over binary fields yields two distinct points, which requires the consideration of two branches at each step where division is carried out.

2 Binary Division Algorithm

Consider an elliptic curve *E* defined over prime field $\mathbb{F}_p$ by Eq. (2). Let *P* be a generator point such that there is no point $A \in E(\mathbb{F}_p)$ that satisfies $P = 2A$. In other words, the point *P* is not divisible by 2. In this case, the sought integer *t* in Eq. (4) can be found using the following binary division algorithm:

Algorithm 1. Binary Division Algorithm for ECDLP

INPUT: $Q \in E(\mathbb{F}_p)$, $P \in E(\mathbb{F}_p)$, *P* is not divisible by 2

OUTPUT: $t_n t_{n-1} .. t_1 t_0$ (*t* in binary format)

1. Set $R \leftarrow Q$, $i \leftarrow 0$.
2. While ($R \neq O$ and $R \neq P$)
   - 2.1 If *R* is divisible by 2, then $t_i \leftarrow 0$.
   - 2.2 Else $t_i \leftarrow 1$, $R \leftarrow R - P$.
   - 2.3 $R \leftarrow R/2$.
   - 2.4 $i \leftarrow i + 1$.
3. If $R = P$ then $t_i \leftarrow 1$.

4. Else $t_i \leftarrow 0$.

Here, $t_i = 0$ denotes the case when point Q_i is divisible by 2, and $t_i = 1$ corresponds to the case when there is no such point $A \in E\left(\mathbb{F}_p\right)$ that satisfies $Q_i = 2A$.

To find the integer *t*, one needs to have both an efficient point divisibility criterion and an efficient point halving algorithm for elliptic curves over prime fields $\mathbb{F}_p$. There is an efficient point halving algorithm for binary fields [1, 5, 8, 9, 10] that is used to perform efficient scalar multiplication for elliptic curves over binary fields. However, there is no known point halving algorithm for elliptic curves defined over prime fields [11].

3 Point Halving Algorithm over Prime Fields

3.1 Formulation of the problem

The group law for elliptic curve *E* given by Eq. (2) over prime field $\mathbb{F}_p$ has the following rule for point doubling [1]:

Let $P = \left(x_1, y_1\right) \in E\left(\mathbb{F}_p\right)$, where $P \neq -P$. Then $2P = \left(x_2, y_2\right)$, where

$$x_2 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1,\ y_2 = \left(\frac{3x_1^2 + a}{2y_1}\right)\left(x_1 - x_2\right) - y_1. \tag{5}$$

To solve the inverse problem of finding a point $A \in E\left(\mathbb{F}_p\right)$ such that $P = 2A$, one needs to solve the system of nonlinear equations for x_1 and y_1 given the values of x_2 and y_2. To the best of our knowledge, there is no efficient general-purpose algorithm for solving system (5). The naïve approach of substituting every point $A \in \langle P \rangle$ into $\left(x_1, y_1\right)$ until a match is found (or no match if the system has no solution) requires the worst-case number of operations equal to the order of point *P*, which ultimately results in the exponential asymptotic complexity of same or higher order as the exhaustive search algorithm for ECDLP [1].

At the same time, efficient algorithms for some special cases can be devised. We separate the further discussion into the cases of odd and even elliptic curve orders.

3.2 Elliptic curve of odd order

Theorem 1: If the number *q* of points on elliptic curve $E\left(\mathbb{F}_p\right)$ given by Eq. (2) is odd, i.e., $\#E\left(\mathbb{F}_p\right) \bmod 2 = 1$, then for every point $P \in E\left(\mathbb{F}_p\right)$ there exists such a point $A \in E\left(\mathbb{F}_p\right)$ that

$$P = 2A \tag{6}$$

and

$$A=\left(\frac{q+1}{2}\right)P. \tag{7}$$

Proof: For every point $P\in E\left(\mathbb{F}_p\right)$

$$qP=O \tag{8}$$

because *q* is the order of elliptic curve *E*. Here, *O* is the point at infinity. We need to show that expression (7) implies (6). Indeed,

$$2A=\left(q+1\right)P=qP+P=O+P=P. \tag{9}$$

Corollary 1: Every point of $E\left(\mathbb{F}_p\right)$ with odd order *q* is divisible by two.

This suggests that the Binary Division Algorithm cannot solve ECDLP when the order of elliptic curve $E\left(\mathbb{F}_p\right)$ is odd (no generator point *P* that is indivisible by two can be selected), and thus any odd-order elliptic curve $E\left(\mathbb{F}_p\right)$ is immune to the Binary Division Attack developed in this study.

3.3 Elliptic curve of even order

3.3.1 Theorems and challenges

The order of $E\left(\mathbb{F}_p\right)$ can be even only if the curve contains at least one point with the *y*-coordinate of zero. Generally, for each *x*-coordinate such that $P=\left(x,y\right)\in E\left(\mathbb{F}_p\right)$, there is another point $Q=\left(x,p-y\right)\in E\left(\mathbb{F}_p\right)$, which follows from the square root operation performed when finding the value of *y*-coordinate for a given value of *x*-coordinate in Eq. (2). These two points coalesce into a single point when *y* = 0. Since the equation

$$x^3+ax+b\equiv 0\ \left(\mathrm{mod}\,p\right) \tag{10}$$

can practically have only 0, 1, or 3 roots (2 roots may occur only if the discriminant $\Delta=-16\left(4a^3+27b^2\right)=0$, which is not acceptable for ECC), the order of $E\left(\mathbb{F}_p\right)$ with at least one *y*-coordinate of 0 is the sum of 1 (for the O point) + the number of points with non-zero *y*-coordinate multiplied by 2 + 1 or 3 (depending on the number of roots to Eq. (10)). It is evident that this sum is always even.

Theorem 2: Let the number *q* of points on elliptic curve $E\left(\mathbb{F}_p\right)$ given by Eq. (2) be even, i.e., $\#E\left(\mathbb{F}_p\right)\mathrm{mod}2=0$. Let the points $P,A\in E\left(\mathbb{F}_p\right)$ such that $P=2A$ exist. If $q=2^m r$, where *r* is odd, $m\geq 0$, and

$$rP = O, \tag{11}$$

then

$$A = \left(\frac{r+1}{2}\right)P \ . \tag{12}$$

Proof: Indeed, Equations (11) and (12) imply that

$$2A = (r+1)P = rP + P = O + P = P \ . \tag{13}$$

It should be noted that Theorem 1 is a special case of Theorem 2 when $m = 0$.

Let us denote the points with the *y*-coordinate of 0 as Z_i, where integer $i \in \{1,3\}$. Let $\#(Z)$ denote the number of such points on a specific elliptic curve. The definition of point doubling given by Eq. (5) implies

$$2Z_i = O \ . \tag{14}$$

This suggests that expression (12) is not unique and the following values of A are also possible:

$$A = \left(\frac{r+1}{2}\right)P + V_i \ . \tag{15}$$

In order to apply the Binary Division Algorithm to the elliptic curve of even order, one also needs to find the divisibility criterion and determine if expressions (12) and (15) can be used to find the coordinates of point $A = P/2$ for all divisible points on even-order elliptic curves. This analysis is performed using numerical experiments.

3.3.2 Numerical experiments

Consider elliptic curve (2) defined over the prime field $\mathbb{F}_{23}$. According to Hasse's theorem [1],

$$p + 1 - 2\sqrt{p} \le \#E\left(\mathbb{F}_p\right) \le p + 1 + 2\sqrt{p} \ , \tag{16}$$

which implies that $15 \le \#E\left(\mathbb{F}_{23}\right) \le 33$. Our goal is to consider all even-order cases and both scenarios $\#(Z) = 1$ and $\#(Z) = 3$. A representative sample is listed in Table 1.

Table 1: Even-order cases of $E(F_{23})$

Curve #	*a*	*b*	#(*E*)	#(*Z*)
1	5	15	16	3
2	7	15	18	1
3	16	1	20	1
4	12	10	20	3
5	14	1	22	1
6	8	1	24	3
7	13	1	26	1
8	6	1	28	3
9	19	1	30	1
10	7	1	32	3

For each elliptic curve in Table 1, the following procedure was executed:

1. Count the order $\#E\left(\mathbb{F}_{23}\right)$ for each elliptic curve (including the at infinity point *O*).
2. Compute 2*A* for each point $A \in E\left(\mathbb{F}_{23}\right)$.
3. Compute the order of each point *A*, which is denoted as #(*A*).
4. Count $\#\left(Z\right)$.

To simplify the analysis, the following definitions are introduced:

- *Odd point*: An elliptic curve point that is not divisible by two;
- *Even point*: An elliptic curve point that is divisible by two.

The results of numerical experiments are listed in Tables 2 through 11. The even points are underlined. Only the points with $y<p/2$ are listed because points (x,y) and $(x, p-y)$ have the same order and divisibility property.

Table 2: Results for *E*: $y^2=x^3+5x+15$, #(*E*) = 16, #(*Z*) = 3

A	(5,2)	(6,10)	(7,5)	(12,3)	(13,0)	<u>(14,0)</u>	(18,7)	(19,0)	<u>(22,3)</u>
2A	(22,3)	(14,0)	(22,20)	(22,20)	O	<u>O</u>	(22,3)	O	(14,0)
#(*A*)	8	4	8	8	2	2	8	2	4

Table 3: Results for *E*: $y^2=x^3+7x+15$, #(*E*) = 18, #(*Z*) = 1

A	(1,0)	<u>(7,4)</u>	(8,10)	<u>(9,5)</u>	<u>(10,2)</u>	<u>(13,7)</u>	(18,4)	(20,6)	(21,4)
2A	<u>O</u>	(13,7)	(9,18)	(9,18)	(7,4)	(10,21)	(13,7)	(7,4)	(10,2)
#(*A*)	2	9	6	3	9	9	18	18	18

Table 4: Results for E: $y^2=x^3+16x+1$, #(E) = 20, #(Z) = 1

A	(0,1)	(1,8)	(2,8)	(9,0)	(11,6)	(12,9)	(14,5)	(16,11)	(18,7)	(20,8)
$2A$	(18,16)	(11,6)	(12,9)	O	(2,8)	(2,15)	(11,6)	(18,16)	(12,9)	(9,0)
#(A)	20	20	5	2	10	5	20	20	10	4

Table 5: Results for E: $y^2=x^3+12x+10$, #(E) = 20, #(Z) = 3

A	(1,0)	(3,2)	(7,0)	(10,7)	(11,1)	(14,1)	(15,0)	(18,3)	(19,6)	(20,4)	(21,1)
$2A$	O	(10,16)	O	(19,6)	(19,17)	(19,17)	O	(19,17)	(10,16)	(10,16)	(10,16)
#(A)	2	10	2	5	10	10	2	10	5	10	10

Table 6: Results for E: $y^2=x^3+14x+1$, #(E) = 22, #(Z) = 1

A	(0,1)	(1,4)	(3,1)	(4,11)	(5,9)	(6,5)	(8,2)	(17,0)	(18,6)	(20,1)	(22,3)
$2A$	(3,1)	(0,1)	(6,18)	(18,6)	(6,18)	(20,22)	(20,1)	O	(0,1)	(18,17)	(3,1)
#(A)	11	22	11	22	22	11	22	2	11	11	22

Table 7: Results for E: $y^2=x^3+8x+1$, #(E) = 24, #(Z) = 3

A	(0,1)	(2,5)	(3,11)	(6,9)	(7,3)	(8,5)	(10,0)	(12,10)	(13,5)	(15,0)	(16,4)	(17,6)	(21,0)
$2A$	(16,4)	(0,22)	(0,22)	(0,22)	(10,0)	(16,19)	O	(0,1)	(10,0)	O	(16,19)	(16,19)	O
#(A)	6	12	12	12	4	6	2	12	4	2	3	6	2

Table 8: Results for E: $y^2=x^3+13x+1$, #(E) = 26, #(Z) = 1

A	(0,1)	(2,9)	(4,5)	(10,2)	(11,7)	(14,11)	(15,11)	(16,2)	(17,11)	(18,8)	(19,0)	(20,2)	(21,6)
$2A$	(2,9)	(21,17)	(0,1)	(21,17)	(14,11)	(4,5)	(20,2)	(4,18)	(2,14)	(0,22)	O	(14,12)	(20,21)
#(A)	13	13	13	26	26	13	26	26	26	26	2	13	13

Table 9: Results for E: $y^2=x^3+6x+1$, #(E) = 28, #(Z) = 3

A	(0,1)	(1,10)	(3,0)	(5,8)	(6,0)	(7,8)	(8,3)	(9,5)	(10,7)	(11,8)	(14,0)	(15,4)	(17,5)	(20,5)	(21,2)
$2A$	(9,18)	(7,8)	O	(15,19)	O	(15,19)	(15,19)	(7,8)	(9,5)	(9,18)	O	(9,18)	(15,4)	(7,8)	(7,15)
#(A)	14	14	2	14	2	7	14	7	14	14	2	7	14	14	14

Table 10: Results for E: $y^2=x^3+19x+1$, #(E) = 30, #(Z) = 1

A	(0,1)	(2,1)	(3,4)	(4,7)	(6,3)	(9,2)	(10,8)	(11,0)	(12,5)	(15,2)	(16,10)	(17,4)	(20,3)	(21,1)	(22,2)
$2A$	(4,7)	(12,5)	(17,19)	(0,22)	(15,2)	(0,1)	(6,20)	O	(12,18)	(17,19)	(4,16)	(20,3)	(6,20)	(20,3)	(15,2)
#(A)	5	6	30	5	15	10	30	2	3	15	10	15	15	30	30

Table 11: Results for E: $y^2=x^3+7x+1$, #(E) = 32, #(Z) = 3

A	(0,1)	(1,3)	(2,0)	(3,7)	(4,1)	(5,0)	(6,11)	(7,5)	(10,6)	(11,11)	(13,9)	(15,10)	(16,0)	(18,5)	(19,1)	(21,5)	(22,4)
$2A$	(18,5)	(11,11)	O	(6,12)	(18,5)	O	(11,12)	(18,5)	(6,12)	(5,0)	(6,12)	(18,5)	O	(11,11)	(11,12)	(6,12)	(5,0)
#(A)	16	8	2	16	16	2	8	16	16	4	16	16	2	8	8	16	4

3.3.3 Observations

Tables 2-11 suggest that all even-order elliptic curves contain both odd and even points. This implies that the Binary Division Algorithm presented in Section 2 can generally be applied to any even-order elliptic curve.

Let $q = \#E(\mathbb{F}_{23})$. For all cases when $q \equiv 2 \pmod 4$, Equation (11) holds, which implies that expression (12) can be used to find the coordinates of point $A = P/2$ when $P = 2A$ exists. On the other hand, the tables corresponding to $q \equiv 0 \pmod 4$ contain a number of points with the order that is even and not divisible by the odd number *r*, which does not allow one to use Theorem 2 in this case.

It should be noted that $q \equiv 2 \pmod 4$ is equivalent to $q = 2r$, where *r* is odd, suggesting that expression (12) can be transformed to

$$A = \left(\frac{q+2}{4}\right) P \ . \tag{17}$$

Next we need to determine when a certain point $P \in E(\mathbb{F}_p)$ is divisible by two. Tables 3, 6, 8, and 10, corresponding to $q \equiv 2 \pmod 4$, show that for even points the order is *r* or a divisor of *r*. On the other hand, all odd points have even orders. This implies that the divisibility criterion for the case of $q \equiv 2 \pmod 4$ can be expressed as

If $q \equiv 2 \pmod 4$ and $(q/2)P = O$, then *P* is divisible by *two*. (18)

Our further analysis of the results of experimental data for this case suggests that when $(q/2)P = O$ does not hold, expression $(q/2)P = Z$ is valid, where *Z* is a point with the *y*-coordinate of zero, which can be restated as

If $q \equiv 2 \pmod 4$ and $(q/2)P = Z$, then *P* is not divisible by *two*. (19)

Expressions (18)-(19) can be considered as the Euler criterion for the elliptic curves over prime fields that correspond to the case of $q \equiv 2 \pmod 4$.

When the number of points with the *y*-coordinate of 0 is one or higher, point halving no longer has a unique solution, as shown by Eqs. (14) and (15). Table 1 suggests that in the case of $q \equiv 2 \pmod 4$, there is only one such point, denoted for simplicity as *Z* (the index *i* is dropped). This means that every point halving operation yields exactly two points in this scenario.

As an example, consider point (12,5) in Table 10. The first point found by Eq. (17) is (12,18). The second point found with Eq. (15) is (2,1). When each of this points is doubled, the result is the same: (12,5).

Combining expressions (15), (17)-(19), we can formulate the following conjecture:

Conjecture 1: Let the number q of points on elliptic curve $E\left(\mathbb{F}_p\right)$ given by Eq. (2) satisfy the congruence $q \equiv 2 \pmod 4$. Let a point $P \in E\left(\mathbb{F}_p\right)$ be given. If $(q/2)P = O$, then P is divisible by two and the two points $A \in E\left(\mathbb{F}_p\right)$ satisfying $P = 2A$ can be computed as

$$A = \left(\frac{q+2}{4}\right)P \text{ and } A = \left(\frac{q+2}{4}\right)P + Z, \tag{20}$$

where Z is the point with the y-coordinate of zero. If $(q/2)P = Z$, then P is not divisible by two.

This conjecture is valid for all of the experiments we ran, but it needs to be either formally proven or numerically (for a large number of elliptic curves with various prime characteristics) verified.

Tables 2, 5, 7, 9, 11 suggest that for the case of $q \equiv 0 \pmod 4$ and $\#(Z) = 3$, the divisibility criterion can be formulated as follows:

Conjecture 2: Let $q \equiv 0 \pmod 4$ and $\#(Z) = 3$. If $(q/4)X = O$, then X is divisible by two; if $(q/4)X = Z_i$, where Z_i is a point with the y-coordinate of zero, then X is not divisible by two.

In this case, Equation (12) cannot be used because its necessary condition (11) is rarely satisfied.

4 Counting Points on Elliptic Curves

Section 3 implies that the binary division attack can be applied only to even-order elliptic curves. Moreover, a non-brute-force point halving algorithm is available only for the case when the even order q of elliptic curve satisfies the congruence $q \equiv 2 \pmod 4$. In view of the above, the binary attack has to incorporate an algorithm for counting the number of points on elliptic curves (2) defined over prime fields.

Main practical algorithms for counting the order of elliptic curves over prime fields include Baby Step Giant Step (BSGS), Mestre's algorithm (improved BSGS), Schoof's algorithm, and Schoof-Elikes-Atkin (SEA) method [12]. They are implemented in standard number-theory software packages, such as Pari-GP and Sage.

The BSGS and Mestre's algorithms have the asymptotic computational complexity of $O\left(\sqrt[4]{p}\right)$; the most efficient variant has the space complexity of $O\left(n^2\right)$, where $n = \log p$. Schoof's algorithm has the computational complexity of $O\left(n^5\right)$ and space complexity of $O\left(n^3\right)$ - it was the first deterministic polynomial-time algorithm for counting points on elliptic curves. The SEA algorithm is probabilistic and has the asymptotic running time of $O\left(n^4\right)$ and space complexity between $O\left(n^3 \log n\right)$ and $O\left(n^4\right)$.

5 Examples

Section 3 suggests that the Binary Division Algorithm may practically be used only in the case of $q \equiv 2 \pmod 4$. When $q \equiv 1 \pmod 2$, every point is divisible by two, and thus the necessary condition for a generator point does not hold. When $q \equiv 0 \pmod 4$, no non-brute force point halving algorithm is known.

According to Eq. (20), each step in the loop of the Binary Division Algorithm for $q \equiv 2 \pmod 4$ should be run for two different values of R. This branching for each bit may theoretically run for all n bits of integer t, resulting in the exponential complexity of 2^n. Let us consider several examples to determine if certain branches can be truncated at early stages.

Example 1: Consider the problem of finding t in $(16,10) = t(21,1)$ for elliptic curve $E(\mathbb{F}_{23})$: $y^2=x^3+19x+1$ (the answer is 21). The recursive application of Algorithm 1 is illustrated in Fig. 1 as a binary tree. The root node has (16,10) as the initial value for R. As R is not divisible by 2, the bit t_0 is set to 1, and the new value of R is set to $R-(12,1)=(12,18)$. Then the breadth-first traversal (BFT) algorithm is used to visit both child nodes of the root node: (12,5) and (2,22). Figure 1 shows that $A=\left(\frac{q+2}{4}\right)P$ (left node) always yields an even point (bit: 0) and $A=\left(\frac{q+2}{4}\right)P+Z$ (right node) always gives an odd point. This follows from the fact that $q=2r$, where r is odd. It should be noted that some points are repeated, for example, point (12,18). This observation can be used to ignore certain "irrelevant" branches: If point R has previously been visited (traversed), then the current point R should not be traversed. The comparison of the current point with any points already visited can be implemented using a dynamic hash table.

The solution to Example 1 is retrieved as a bit sequence in the reverse order. In this case, it is "10101", which is 21. The number of binary divisions (scalar multiplications given by Eq. (17)) needed to find the solution is 7.

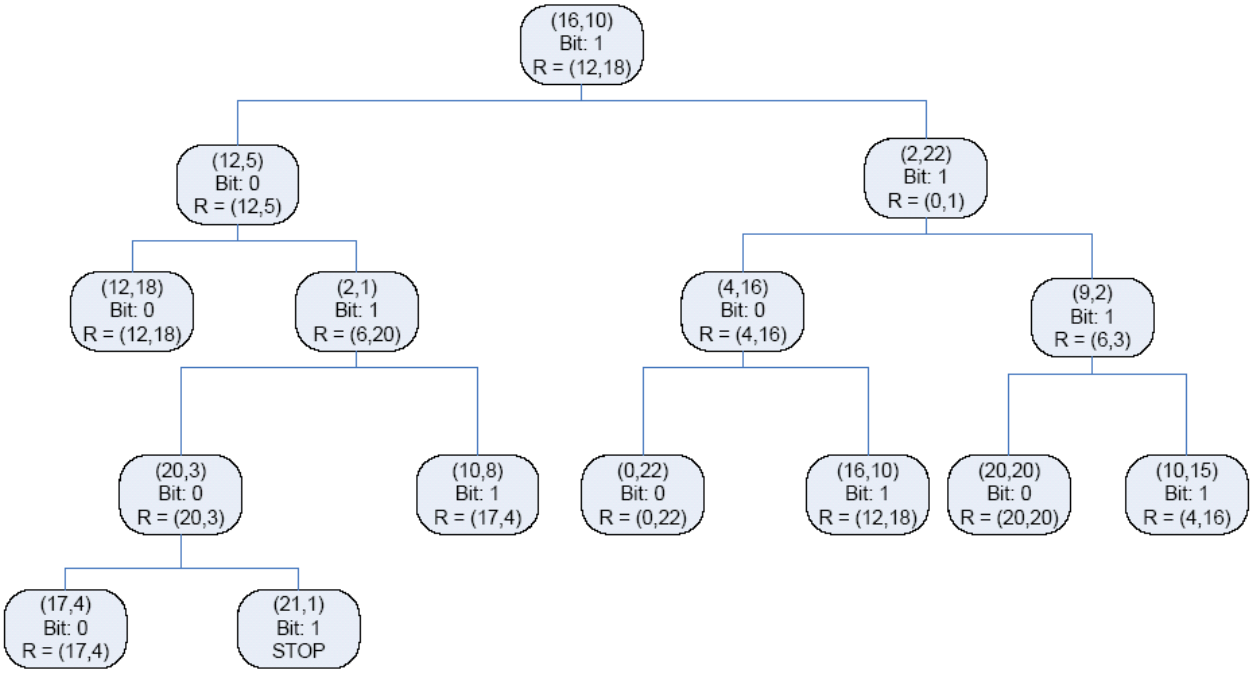


Figure 1: Tree Representation of the Solution for Example 1

Example 2: Consider the problem of finding t in $(10,15)=t(3,4)$ for elliptic curve $E(\mathbb{F}_{23})$: $y^2=x^3+19x+1$ (the answer is 19). In this case, the solution is "11001", which corresponds to 19. The number of binary divisions is 9.

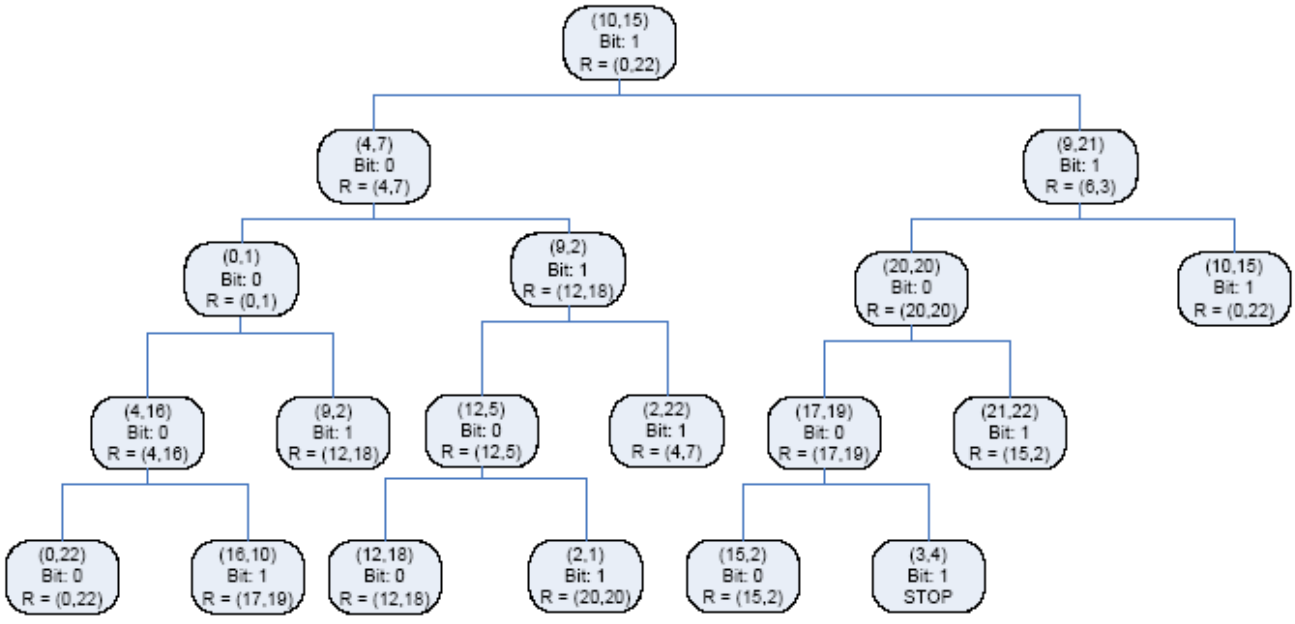


Figure 2: Tree Representation of the Solution for Example 2

Example 3: Consider the problem of finding t in $(11,16)=t(10,2)$ for elliptic curve $E(\mathbb{F}_{23})$: $y^2=x^3+13x+1$ (the answer is 17). In this case, the solution is "10001", which corresponds to 17. The number of binary divisions is 7.

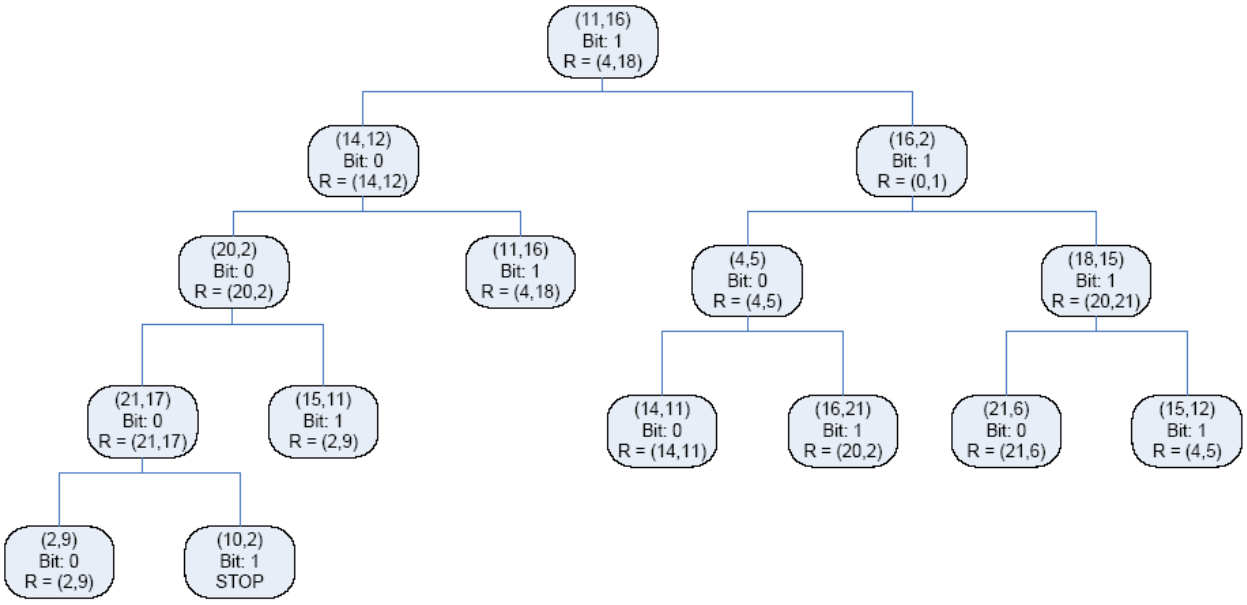


Figure 3: Tree Representation of the Solution for Example 3

6 Analysis

The most time-consuming operations in the binary tree implementation of Algorithm 1 for the case where $q \equiv 2 \pmod 4$ include (1) the counting of the number of points on elliptic curve, (2) the scalar multiplication involved in each point halving, and (3) the branching at each point halving leading to a binary tree traversal.

The first operation has to be executed only once and has a polynomial time complexity of $O(n^4)$, where $n=\log p$ (see Section 4 for details).

Equation (17) can be efficiently computed using one of the double-and-add methods, such as windowed, sliding-window, wNAF, or Montgomery ladder algorithm [1]. These algorithms generally require $O(k)$ iterations of point doubling and addition, where $k=\log q$.

The branching at each point results in at most $q/2$ binary divisions. Certain branches, as illustrated in the Examples, may be truncated at early stages. Still, the worst-case number of binary divisions is $O(q)=O(2^k)$, leading to the overall complexity of $O(k2^k)$. This implies that the binary division attack developed in this paper has exponential time complexity due to non-uniqueness of the point halving operation for elliptic curves defined over prime fields, which was also observed for the binary field case [7].

7 Conclusion

The binary division attack developed in this study can be used to solve the ECDLP when the order q of elliptic curve $E\left(\mathbb{F}_p\right)$ given by Eq. (2) satisfies the congruence $q \equiv 2 \pmod 4$. Although in the worst-case scenario the algorithm has an exponential asymptotic time complexity, in certain cases the number of visited branches in the binary tree representation of the algorithm (for example, see Fig. 1) may be relatively small making the solution of ECDLP practically feasible. Therefore, our recommendation is to avoid the case of $q \equiv 2 \pmod 4$ in practical ECC systems.

REFERENCES

[1]. D. Hankerson, A. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*, New York: Springer, 2004.

[2]. R. Gallant, R. Lambert, and S. Vanstone, "Improving the parallelized Pollard lambda search on binary anomalous curves", *Math. Comput.*, vol. 69, pp. 1699–1705, 1999.

[3]. P. van Oorschot and M. Wiener, "Parallel collision search with cryptanalytic applications", *J. Cryptol.*, vol. 12, pp. 1–28, 1999.

[4]. M. Wiener and R. Zuccherato, "Faster attacks on elliptic curve cryptosystems", in *Selected Areas in Cryptography'98*, Berlin: Springer-Verlag, LNCS 1556, 1998, pp. 190–200.

[5]. F. Zhang and P. Wang, "Speeding up elliptic curve discrete logarithm computations with point halving", *Des. Codes Cryptogr.*, vol. 67, pp. 197–208, 2013.

[6]. NIST, *Digital Signature Standard*, FIPS Publication 186-2, February 2000.

[7]. A. V. Bessalov, "A method of solution of the problem of taking the discrete logarithm on an elliptic curve by division of points by two", *Cybern. Syst. Anal.*, vol. 37, no. 6, pp. 820–823, 2001.

[8]. E. Knudsen, "Elliptic scalar multiplication using point halving", in *Advances in Cryptology-ASIACRYPT'99*, Lecture Notes in Computer Science 1716, 1999, pp. 135–149.

[9]. R. Schroeppel, "Elliptic curve point halving wins big", in *2nd Midwest Arithmetical Geometry in Cryptography Workshop*, Urbana, 2000.

[10]. D. Hankerson, K. Karabina, and A. Menezes, "Analyzing the Galbraith-Lin-Scott point multiplication method for elliptic curves over binary fields", *IEEE Trans. Comput.*, vol. 58, no. 10, pp. 1411-1420, 2009.

[11]. K. Wong et al., "Fast elliptic scalar multiplication using new double-base chain and point halving", *Appl. Math. Comput,*, vol. 183, pp. 1000–1007, 2006.

[12]. R. Schoof, "Counting points on elliptic curves over finite fields", *Journal de Theorie des Nombres de Bordeaux*, vol. 7, pp. 219-254, 1995.

TNC Transactions on Networks and Communications
SOCIETY FOR SCIENCE AND EDUCATION UNITED KINGDOM
VOLUME 2, ISSUE 4
ISSN: 2054 - 7420

Gain Matrix Distributed Computing Technique for Power System State Estimation

[1]H. Nagaraja Udupa, [2]H. Ravishankar Kamath
[1]Mewar University, District Mewar, Chittograh, Rajasthan, India
[2]Malwa Institute of Technology, RGPV University, Indore, India
[1] hnudupa@gmail.com; [2] rskamath272@gmail.com

ABSTRACT

The Electric Power System State Estimation problem involves large sparse matrices. The Jacobian matrix is highly sparse in nature and the computational efforts can be enhanced by avoiding arithmetic operations resulting in 'zero'. The researchers have introduced sparse matrix techniques so as to store only non-zero elements of the matrix and thereby reducing the huge dynamic memory requirements, which intern reduce the computational time. A few such techniques [2],[3], [4] are listed in the reference. The primary focuses of these sparse techniques are on the memory/storage space reduction.

This paper elaborates a different technique to obtain the "effective operation" with the focus on the computational time and the storage space reduction. The "effective operation" can be achieved without applying conventional compact storage techniques to find the Jacobian product. A different style for multiplication of two large sparse Jacobian matrices is adopted to obtain this novel approach. As a result, computational time is reduced and also Jacobian array size is reduced form two dimensional array to single dimensional array. The solution gives scope for distributed/parallel computing without disturbing the network structure [6].

Key Words: SE - State Estimation, WLS – Weighted Least Square, NR – Newton Rapson, ISE – Integrated State estimation, 'A' gain matrix, , NA – Node Area- A node along with its connected Node is referred as Node Area, H1 to H12 are the sub set of Jacobian metrics 'J'.

1 Introduction

The state of power system is to be known for healthy planning, operation and energy management for both online and off-line system. The complex non-linear equations along with large sparse matrix involved in the power system makes it complicated and difficult for fast computation of state variables. Many researchers have presented different technique to overcome this problem. A few such papers [5], [7] & [8] are given in reference. Interestingly, there is a one to one relation between the network incident matrix and the Jacobian matrix for

DOI: 10.14738/tnc.24.311
Publication Date: 4th August 2014
URL: http://dx.doi.org/10.14738/tnc.24.311

non-zero elements. Using this intelligence it is possible to focus all the computations only for non-zero elements and thereby minimize the computational time with minimum dynamic storage space. It is essential to modify the NR solution steps to achieve the same. An insight of the procedural steps involved in the existing NR method is given below for better understanding of the modification detailed out in the later session.

1.1 State Estimation:- Newton-Raphson technique

By applying the tylor series to the nonlinear equations of power system following equations is derived [1].

$(J^T W J)\,\Delta x = J^T W\,\Delta z$

$A = (J^T WJ)$ & $b = J^T W\,\Delta z$

$A\,\Delta x = b$ (1)

$\mathbf{x_i}$– No of state variables :- = (2*n-1)

n – No.of network nodes : - = 1,2,…n.

m– Total no of measurements

J – Jacobian matrix, size is : - m*(2n-1)

W - Diagonal weigh matrix of the order of (m*m)

A – Gain matrix of the order of (2n-1)*(2n-1)

$[x]^T = [\delta_1, \delta_2, ...\delta_{n-1}; v_1, v_2, ...v_n,]$; of the order of *x* is (2n-1)*1.

$[z^{measured}]^T$ = [P_i ,Q_i ,p_{ij} ,q_{ij}, V_i ,δ_i]; of the order of (m*1); These measurements may include one or all quantities.

Pi ,Qi = Real & Imaginary part of injected power respectively.

pij ,qij = Real & imaginary part of line follows respectively

$\Delta z = z^{measured} - z^{calculated}$, size is: - m*1;

$b = J_0^T W\,\Delta z$ of the order of (2n-1)*1;

$$\overbrace{\begin{bmatrix}\Delta P_i\\ \Delta Q_i\\ \Delta p_{ij}\\ \Delta q_{ij}\\ \Delta v_i\\ \Delta \partial_i\end{bmatrix}}^{[\Delta z_i]} \Longrightarrow \overbrace{\begin{bmatrix}|H_1||H_2|\\ |H_3||H_4|\\ |H_5||H_6|\\ |H_7||H_8|\\ |0||1|\\ |1||0|\end{bmatrix}}^{[J]} \overbrace{\begin{bmatrix}\Delta \partial_i\\ \Delta v_i\end{bmatrix}}^{\Delta x_i} \qquad (2)$$

This is a set of linear equations, if higher order terms of the taylor expansion of f(x) were really negligible, the solution yield the correct 'x'. The state variable vector x is obtained by solving the equation $A*\Delta x = b$ iteratively. The vector x should therefore be changed accordingly after every iteration till the convergence is obtained.

$x^{c+1} = x^c + \Delta x^c$; 'c'-iteration count. Elements of Jacobean are derived from injected power, and line flow equations.

1.2 Conventional Computing Steps

Step 1: - Read input data

Step 2: - From system parameters find Y_{bus}

Step 3: - Initialize $[v_i]^T = 1$; and $[\partial_i]^T=0$;

Step 4: - Find $[z]^{cal}$ and $[\Delta z]= [z]^{measured} -[z]^{cal}$

Step 5: - Find all rows of [J] and $[\Delta z]$

Step 6: - Find $[J]^T*[W]*[J] =[A]$ and $[J]^T*[W]*[\Delta z] = [b]$

Step 7: - Find $[\Delta x_i] = [A]^{-1}*[b]$;

Step 8: - check for $[\Delta x_i]$

if $[\Delta x_i]$<<€;

if No - Update [xi]; $[xi]^{new} = [x_i]^{old} +[\Delta x_i]^{old}$; then repeat from step 4.

if yes – Stop

2 Distributed Technique: - New Method

The dimension/size of the matrices involved in equation (1) depends on the number of network nodes. The conventional algorithm can be divided into two parts,

i. up to the formation of matrix 'A' and 'b'
ii. obtaining the solution for $[\Delta xi] = [A]^{-1}*[b]$

It is difficult to allot multiple processors to solve the problem in its present form. A new novel distributed computing technique is discussed to address the issue.

2.1 Matrix Multiplication – Alternate Technique

Let us consider the conventional way of multiplication of two matrices.

$$[C]*[D] = [A]; \quad a_{\substack{ij \\ i=1,2,....n \\ j=1,2,...r}} = \sum_{k=1}^{m} (c_{ik} * d_{kj}) \tag{3}$$

Order of 'C' is : – (n*m), Order of 'D' is : – (m*r) and Order of 'A' is – (n*r)

From the (3), the resultant matrix can be rearranged as shown below

$$A = \sum_{k=1}^{m} \left\{ \left((c_{i1} * d_{1j}) \right)_{\substack{k=1 \\ k=p \\ i=1,2,....n; \\ j=1,2,...r}} \left((c_{im} * d_{mj}) \right)_{\substack{k=m \\ i=1,2,....n; \\ j=1,2,...r}} \right\} \tag{4}$$

Each sub-matrices of 'A' can be obtained by taking a Coolum of 'C' and corresponding row of

'D', for example Am is obtained by multiplying the mth column of 'C' and mth row of 'D', which is as follows

$$[A_m] = \begin{bmatrix} c_{1m} \\ c_{2m} \\ . \\ . \\ c_{nm} \end{bmatrix} \begin{bmatrix} d_{m1} & d_{m2} & \dots d_{mr} \end{bmatrix}; \tag{5}$$

.

$$[A] = [A_1]_{k=1} + [A_2]_{k=2} + \dots\dots + [A_m]_{k=m} = \sum_{k=1}^{m} A_m \tag{6}$$

2.2 Distributed Approach

From the above relationship, the components of 'A' can be computed by considering a Column of 'C' and corresponding row of 'D'. By applying the above relationship to $[J]^T*[W]*[J] =[A]$ and $[J]^T*[W]*[\Delta z] = [b]$, yields, ('W' assumed unity diagonal)

$$A = \sum_{k=1}^{m} \left\{ \underset{k=1}{\left(J_{i1}^T * J_{1j} \right)_{\substack{i=1,2,\dots 2n-1; \\ j=1,2,\dots 2n-1}}} \left(J_{im}^T * J_{mj} \right)_{\substack{\overset{k=m}{} \\ i=1,2,\dots 2n-1; \\ j=1,2,\dots 2n-1;}} \right\}$$

$$b = \sum_{k=1}^{m} \left\{ \underset{k=1}{\left(J_{i1}^T * \Delta z_1 \right)_{i=1,2..(2n-1)}} \left(J_{im}^T * \Delta z_m \right)_{\substack{\overset{k=m}{} \\ i=1,2..(2n-1)}} \right\}$$

$$[A_m] = \begin{bmatrix} J_{m1} \\ J_{m2} \\ . \\ . \\ J_{m(2n-1)} \end{bmatrix} \begin{bmatrix} J_{m1} & J_{m2} & \dots J_{m(2n-1)} \end{bmatrix}$$

$$[\mathrm{b_m}] = \begin{bmatrix} J_{m1} \\ J_{m2} \\ . \\ . \\ J_{m(2n-1)} \end{bmatrix} [\Delta \mathrm{z_m}]$$

$$[A] = [A_1]_{k=1} + [A_2]_{k=2} + ... + [A_m]_{k=m} \quad (6)$$

$$\text{and } [b] = [b_1]_{k=1} + [b_2]_{k=2} + ... + [b_m]_{k=m} \quad (7)$$

It is evident from the above relationship that after obtaining the each row of Jacobin with respect to a measurement, corresponding sub-matrices of resultant matrix (A and b) can be obtained. Hence it is not necessary to form the complete Jacobian matrix before multiplication of $[J]^T$ *W*[J] =[A] and $[J]^T$*W*[Δz] = [b]. It reduces the Dynamic size of 'J' matrix from m*(2n-1) to 1*(2n-1). Also A_1, A_2.. A_m and b_1, b_2… b_m can be formed independently. The equations (6) and (7) can be re-written by grouping the measurements as node wise clusters, which is shown below.

All possible measurements at n^{th} node cluster is

$$\left[\Delta z^n\right] = [\Delta P_n, \Delta Q_n, \Delta p_{nk}, \Delta q_{nk}, \Delta v_n, \Delta \delta_n]; \quad (8)$$

$$\left[\mathrm{A_n^P}\right] = \left\{[J_n^P]^T * [W_{Pn}] * [J_n^P]\right\}; \quad \left[\mathrm{A_{nk}^q}\right] = \sum_{\mathrm{k}}^{\mathrm{cb}} \left\{[J_n^q]^T * [W_{qn}] * [J_n^q]\right\} \quad (9)$$

$$\left[\mathrm{b_n^P}\right] = \left\{[J_n^P]^T * [W_{Pn}] * [\Delta P_n]\right\}; \quad \left[\mathrm{b_{nk}^q}\right] = \sum_{\mathrm{k}}^{\mathrm{cb}} \left\{[J_n^P]^T * [W_{Pn}] * [\Delta q_{nk}]\right\}, \quad (10)$$

similarly for other measurements.

where 'cb' number of connected nodes of 'n^{th}' bus; 'k' varies up to 'cb'.

$$[^n A] = [A_n^P + A_n^Q + A_{nk}^p + A_{nk}^q + A_n^v + A_n^\delta] \quad (11)$$

$$[^n b] = [b_n^P + b_n^Q + b_{nk}^p + b_{nk}^q + b_n^v + b_n^\delta] \quad (12)$$

$$[\mathrm{A}] = \sum_{\mathrm{i=1}}^{\mathrm{n}} \mathrm{A^i} \text{ and } [\mathrm{b}] = \sum_{\mathrm{i=1}}^{\mathrm{n}} \mathrm{b^i} \quad (13)$$

Note: - $A^{\mathrm{P/Q/p/q/v/}\delta}$ - stands for type of measurements

n - stands for node

The equation (13) or (6) and (7) can be used to compute Matrices 'A' and 'b'

2.3 Jacobian Distributed Computing:

Step 1: - Read Input data

Step 2: - From system parameters find Ybus.

Step 3: - Initialize $[vi]^T = 1$; and $[\partial i]^T=0$;

For(r = 1 to m)

{ Step 4.: - Find z_r^{cal}

Step 5: - Find J_r : - Jacobian row corresponding 'z_r ' and $\Delta z_r = z_r^{mes} - z_r^{cal}$

Step 6: - Find $J_r^T*W_{rr}*J_r = [A] + [A_r]$ and $J_r^T*W_{rr}*\Delta z_r = [b] + [b_r]$ **}**

Step 7: - Find $[\Delta x_i] = [A]^{-1}*[b]$;

Step 8: - check for $[\Delta x_i]$

if $[\Delta x_i] << €$;

if No - Update [xi]; $[xi]^{new} = [x_i]^{old} + [\Delta x_i]^{old}$; then repeat from step 6.

if yes – Stop

2.4 Advantages: - From the above facts it is clear that

i. The task from Step 1 to step 4 can be distributed to 'n' processors.
ii. Dynamic size of Jacobian is (1 * 2n-1) but in conventional method 'J' size is (m * 2n-1)
iii. Dynamic size of Δz is just a simple variable. In conventional method 'Δz' size is (m*1).
iv. No need to store the z^{cal} in file/array variables.
v. Local indexing for 'Jacobian' elements is easier
vi. Multiplication of $J_r^T*W_{rr}*J_r = [A] + [A_r]$ and $J_r^T*W_{rr}*\Delta z_r = [b] + [b_r]$ can be done easily for non zero elements using local indexing.
vii. It is observed that the multiplication time required by the new method is much lesser than the conventional method.

2.5 Sparse Technique

The following C++ program demonstrates the use of new logic, taking line flow measurement example. Let the global variable sij[][] and h[] structure is

- sij[i][1] na; sij[i][2]- node from (i); sij[i][3]- node to (j)
- sij[i][4] = pij measured & sij[i][5] = qij measured
- sij[i][6] = y/2 half line charging between i & j
- sij[i][7] = Gij & sij[i][8] = Bij
- h[] = Jacobian row variables

find_jaco_lf(int r,int n): - is the sub-program to find the elements of A and b corresponding to a measured line flow values using this new technique. In the following program all the computations are focused only for non-zero elements.

```
void find_jaco_lf(int r,int n)
 {
  int i,j,q,p,kl,g,k,l,x1,x2,x3,x4; // (x1 to x4) non-zero location of Jacobian row
  long double delz,a1,b1,deg,yij,tea, smp,smq;
  for(q=0;q<=2*n;q++)
      h[q].x = 0.0;
  for(g=1;g<=kl;g++) // kl - number of line flow measurements
     {
            i = (sij[g][2].x); // node 1 is taken as reference
            j = (sij[g][3].x);

            x1=i-1;
            x2=j-1;
            x3=n+i-1;
            x4=n+j-1;
            z[1].x=x1;
            z[2].x=x2;
            z[3].x=x3;
            z[4].x=x4;
                        a1 = sij[g][7].x;
                        b1 = sij[g][8].x;
                        yij = sqrt((a1*a1)+(b1*b1));
                        tea= atan(b1/a1);
                        if(a1==0.0)
                        tea=-(11./7.);
                        deg = (del[i].x - del[j].x - tea);
           smp=yij*(v[i].x*v[i].x*cos(tea)-(v[i].x*v[j].x*cos(deg)));
           smq=yij*(v[i].x*v[i].x*sin(-tea)- v[i].x*v[j].x*sin(deg)) -  (sij[p][6].x* v[i].x * v[i].x);
/*----To find  Jr- for line flow "pij. For the sake of simplicity 'Wii' is assumed to be unity*/
           h[x1].x = v[i].x*v[j].x*yij*sin(deg);                                  /*h5i*/
           h[x2].x= -v[i].x*v[j].x*yij*sin(deg);                                  /*h5j*/
           h[x3].x=yij*(2*v[i].x*cos(tea)-v[j].x*cos(deg));/*h6i*/
           h[x4].x = -v[i].x*yij*cos(deg);                                        /*h6j*/
/*----A = A + Jr^T*Jr and b = b+ Jr^T*Δzr---- (for line flow "pij")*/
 delz = (sij[g][4].x-smp);
           for(p=1;p<=4;p++)
                    {
            k=z[p].x;
            b[k].x = (b[k].x + h[k].x*delz);
            for(q=1;q<=4;q++)
                    {
                     l=z[q].x;
                     a[k][l].x = (a[k][l].x + h[k].x*h[l].x);
                                        } }
/*----To find  Jr- for line flow "qij".....*/
          h[x1].x = -v[i].x*v[j].x*yij*cos(deg);                                  /*h7i*/
          h[x2].x =  v[i].x*v[j].x*yij*cos(deg);                          /*h7j*/
          h[x3].x = (2*v[i].x*sin(-tea)-v[j].x*sin(deg))*yij;                     /*h8i*/
          h[x4].x = -v[i].x*yij*sin(deg);                                         /*h8j*/
```

```
/*----A = A + Jr^T*Jr-and b = b+ Jr^T*Δzr---- (for line flow "qij")*/
        delz = (sij[g][5].x-smq);
        for(p=1;p<=4;p++)
                {
         k=z[p].x;
         b[k].x = b[k].x + h[k].x*delz;
         for(q=1;q<=4;q++)
                {
          l=z[q].x;
          a[k][l].x = a[k][l].x + h[k].x*h[l].x;
                } } } }
```

2.6 Computational Efforts

A matrix is said to be sparse if a given finite discrete ample space Ω and a non-empty set of sample S is such that the cardinality |S| of S is small compared to the cardinality | Ω | of Ω i.e. |S| << | Ω |. As discussed L.P.Singh [2],

2.6.1 Effort for Conventional technique

- Let p= |S| and Q = | Ω |.
- 't_i' is the time taken to perform operation by elements 'i' of 'S'
- 'r_i' is the additional time taken to retrieve an element of elements 'S' in a compact storage scheme.
- 's_i' is the additional time taken to store an element of elements 'S' in a compact storage scheme.

The total processing time without compact storage is = $\sum_{i=1}^{Q} t_i$

The total processing time with compact storage is = $\sum_{i=1}^{p} t_i + r_i + s_i$

For sparse matrix $\sum_{i=1}^{p} t_i + r_i + s_i < \sum_{i=1}^{Q} t_i$

2.6.2 Effort for New technique: -

As seen earlier no special storing and retrieving scheme is required for Jacobian in this new technique,

The total processing time for new scheme = $\sum_{i=1}^{p} t_i$

Normally J^T*Wi*J is carried out by taking the row of J^T into column of J. In conventional method, the identification of non-zero elements of each column of J takes more time than row wise non-zero elements identification of J. This is because of the fact that the non-zero elements in each row of Jacobian have direct relation with the corresponding row of network incident matrix.

The time 'r_i' in the new technique will be very small as compared to the old scheme because of local dynamic indexing. The time 'S_i' in the new technique is considered zero without compact storage for the resultant matrix 'A'. When the measurements are grouped node-wise the resultant matrix 'A' for the given node will be dense matrix.

3 Example & Results

A simple four bus example has been considered. First 'A' is calculated using conventional method, where A= (J^T*W*J). Next 'A' is computed using new method, where A= $\sum_{j=1}^{m}(J_j^T * W_{jj} * J_j)$; 'm' is the total number of measurements taken.

The new method (Distributed technique) results are also processed with single processor.

3.1: Circuit & Input tables

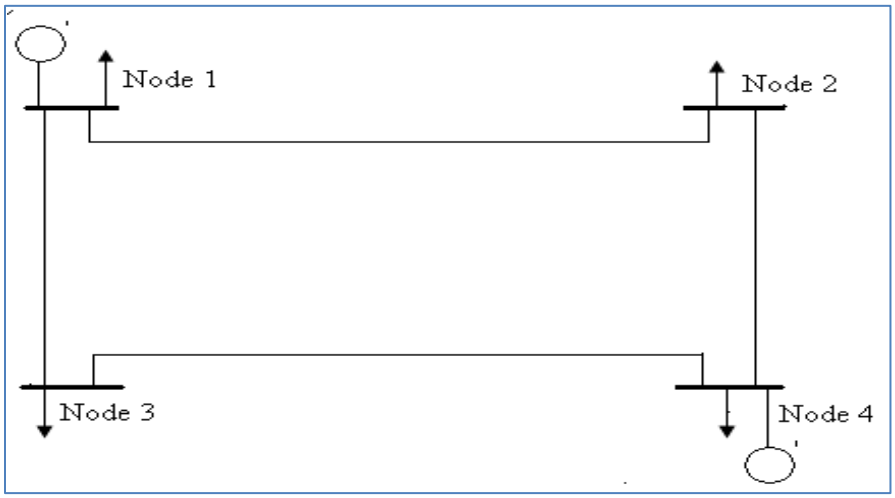


Fig-1: - Circuit diagram

Table 1: Line data

I - j	R	X	G	B	Y/2
1--2	0.01008	0.0504	3.815629	-19.0781	0.05125
1--3	0.00744	0.0372	5.169561	-25.8478	0.03875
2--4	0.00744	0.0372	5.169561	-25.8478	0.03875
3--4	0.01272	0.0636	3.023705	-15.1185	0.06375

Table 2: Injected power, Voltage & Phase measurements

P_i	Q_i	V_i	∂_i
1.3718	0.8431	1	0
-1.6945	-1.0735	0.982	-0.0171
-1.9914	-1.2416	0.969	-0.032
2.3809	1.3299	1.02	0.026

Table 3 Line flow measurements

na	i	j	P_{ij}^{mes}	Q_{ij}^{mes}
1	1	2	0.3877	0.2825
1	1	3	0.9792	0.6514
2	2	1	-0.3852	-0.2809
2	2	4	-1.3138	-0.715
3	3	1	-0.969	-0.5999
3	3	4	-1.0266	-0.5446
4	4	2	1.3311	0.8013
4	4	3	1.0266	0.6361

3.2 Results:

The results are divided into two parts.

Part-I: - Tables R1 to R6 shows the resultant matrix 'A' by either method for first iteration.

(Note: - In the below tables "the smallest value is represented by 'E-06')

Table-R1: - $[A]=[J^T * W * J]$ size of 'A' is $=[(2n-1)\ x(2n-1)]$ and size of 'J' is $=[m\ x\ (2n-1)]$						
5320.17	919.265	-3698.6	1.56322	-3.68118	E-06	1.71871
919.265	4544	-1763.67	2.11791	E-06	-2.72392	1.00527
-3698.6	-1763.67	4544.01	E-06	2.11791	1.00527	-2.72398
1.56322	2.11791	E-06	5304.04	-2532.97	-3688.65	919.265
-3.68118	E-06	2.11791	-2532.97	5304.04	919.265	-3688.65
E-06	-2.72392	1.00527	-3688.65	919.265	4527.25	-1757.47
1.71871	1.00527	-2.72398	919.265	-3688.65	-1757.47	4527.25
Table-R2: - $[A]=\sum_{i=1}^{n}[{}^{i}A]$ size of 'A' is $=[(2n-1)\ x(2n-1)]$ and size of 'J_r' is $=[1\ x\ (2n-1)]$						
5320.17	919.265	-3698.6	1.56321	-3.6811	E-06	1.71868
919.265	4544.01	-1763.67	2.11794	E-06	-2.72402	1.0053
-3698.6	-1763.67	4544.01	E-06	2.11794	1.0053	-2.72402
1.56321	2.11794	E-06	5304.04	-2532.97	-3688.65	919.265
-3.6811	E-06	2.11794	-2532.97	5304.04	919.265	-3688.65
-E-06	-2.72402	1.0053	-3688.65	919.265	4527.25	-1757.47
1.71868	1.0053	-2.72402	919.265	-3688.65	-1757.47	4527.25
Table-R3: - $[{}^{1}A]=[A_1^P + A_1^Q + A_{1k}^p + A_{1k}^q + A_1^v + A_1^\delta]$						
757.068	512.853	**0**	1.56323	E-06	E-06	**0**
512.853	1389.67	**0**	2.11793	E-06	E-06	**0**
0	**0**	**0**	**0**	**0**	**0**	**0**
1.56323	2.11793	**0**	3157.3	-1266.49	-1897.87	**0**
E-06	E-06	**0**	-1266.49	757.068	512.853	**0**
E-06	E-06	**0**	-1897.87	512.853	1389.67	**0**
0	**0**	**0**	**0**	**0**	**0**	**0**

Table-R4: - $[{}^2A] = [A_2^P + A_2^Q + A_{2k}^p + A_{2k}^q + A_2^v + A_2^\delta]$						
3173.44	**0**	-1902.52	E-06	-3.6811	**0**	E-06
0	**0**	**0**	**0**	**0**	**0**	**0**
-1902.52	**0**	1389.67	E-06	2.11793	**0**	E-06
E-06	**0**	E-06	757.068	-1266.49	**0**	512.853
-3.6811	**0**	2.11793	-1266.49	3157.3	**0**	-1897.87
0	**0**	**0**	**0**	**0**	**0**	**0**
E-06	**0**	E-06	512.853	-1897.87	**0**	1389.67

Table-R5: - $[{}^3A] = [A_3^P + A_3^Q + A_{3k}^p + A_{3k}^q + A_3^v + A_3^\delta]$						
0	**0**	**0**	**0**	**0**	**0**	**0**
0	2678.92	-881.837	E-06	**0**	-2.72402	E-06
0	-881.837	475.425	E-06	**0**	1.00529	E-06
0	E-06	E-06	1389.67	**0**	-1790.78	406.412
0	**0**	**0**	**0**	**0**	**0**	**0**
0	-2.72402	1.00529	-1790.78	**0**	2662.16	-878.737
0	E-06	E-06	406.412	**0**	-878.737	475.425

Table-R6: - $[{}^4A] = [A_4^P + A_4^Q + A_{4k}^p + A_{4k}^q + A_4^v + A_4^\delta]$						
1389.67	406.412	-1796.08	**0**	E-06	E-06	1.71871
406.412	475.424	-881.836	**0**	E-06	E-06	1.00529
-1796.08	-881.836	2678.92	**0**	E-06	E-06	-2.72402
0	**0**	**0**	**0**	**0**	**0**	**0**
E-06	E-06	E-06	**0**	1389.67	406.412	-1790.78
E-06	E-06	E-06	**0**	406.412	475.424	-878.737
1.71871	1.00529	-2.72402	**0**	-1790.78	-878.737	2662.16

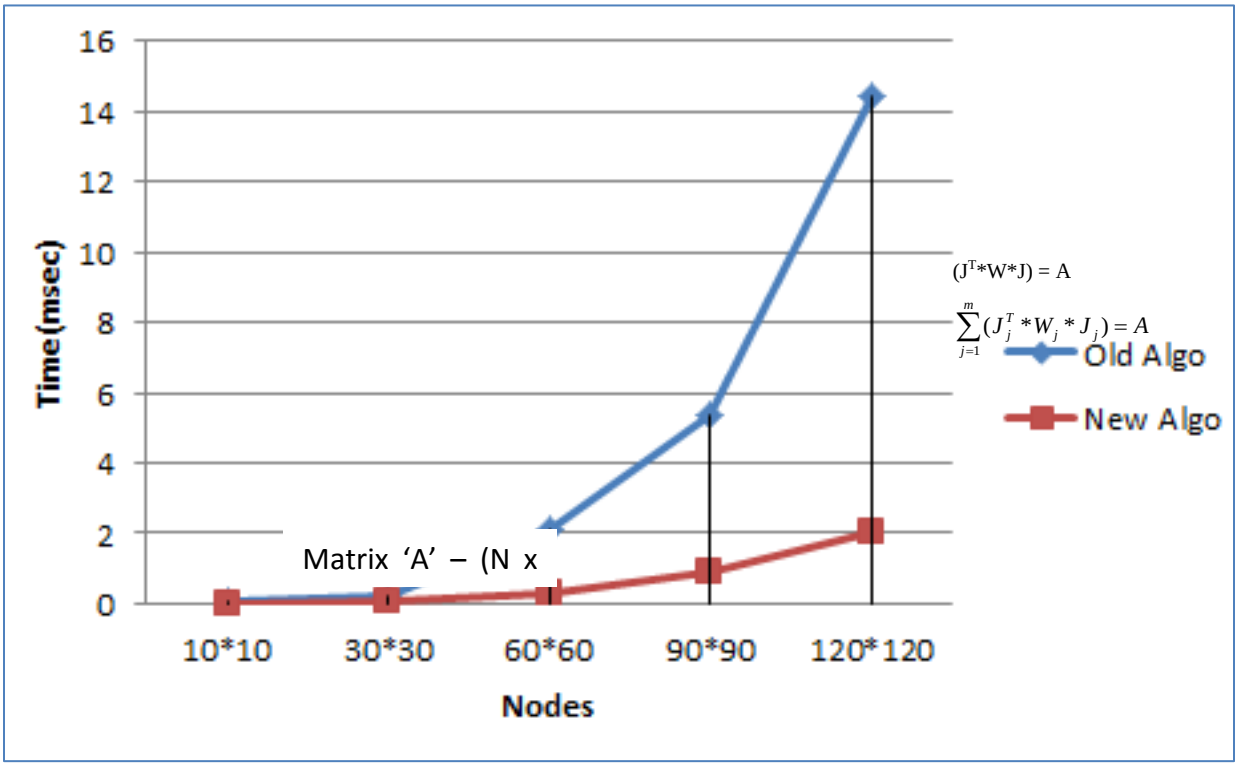
Part-II: -

The graph in figure 2 shows the computing time for 'A' by either method.

In the graph the New Algorithm and Old Algorithm represents the computational time for the new and old method respectively. The above relation is obtained under following assumption.

- The number of measurements is assumed to be equal to the number of state variables.
- Approximately 15% of the Jacobian elements are assumed to be non-zero; this fact is based on the practical system.

The profiling is conducted on Core2-Duo X-86 2GB RAM machine with Operating System Windows 7, we were able to fetch the above results. The result may vary with the different hardware configuration but the ratio of the Old Vs New Algorithm remains almost constant no matter what hardware configuration has been adapted.



(Note: - Both the above results are obtained using single processor.)

Figure 2: Computation time

4 Conclusions

The results show that the resultant matrixes 'A' computed by both methods are same. In Old Algorithm (Algo) the time was exponentially increasing with the number of network nodes, whereas in the new Algo the exponential growth has been reduced to almost linear growth. Using new algorithm, the time can be reduced further by employing more number of processors. Even though both the methods are mathematically same, new method results in drastic reduction in computational time. In the new method up to Jacobian product can be computed by parallel processing using the equations (6) and (7). By grouping the measurements in the form of node clusters [equations (8), (9) & (10)] it is possible to divide the Matrix 'A' (& b) as node cluster wise gain matrix [nA] and [nb]. The size of [^{n}A] and [^{n}b] is directly related to the size of node cluster state variables. For example, at node cluster No. 2, [refer table-R4] state variables are (∂2, ∂4,v1, v2,v4) taking node-1 as angle reference node. Hence the size of [^{2}A] is (5x5) and not (7x7) similarly, the size of [^{2}b] is (5x1) & [^{2}Δx] is (5x1). It is not necessary to have separate reference node at each node cluster. Hence, solution for [Δxi] can also be divided into 'n' independent sub tasks which will further reduces the computational time, which will be presented in further papers.

ACKNOWLEDGEMENT

The authors would like to thank Mr. Antriksha Somani, Assit. Prof., Dept. Cs, MIT, Indore, MP, for his help in programming and profiling.

REFERENCES

[1]. H.N. Udupa, Dr. H.R.. Kamath et al., Modified electric power system state estimation – Multi- processing technique, IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET) ISSN 2321-8843 Vol. 1, Issue 5, Oct 2013, 47-56

[2] L.P. Singh, third edition 1992, *"Advanced Power System Analysis & Dynamic,"* New Age International Publishers. P.No. 254 – 287.

[3] L.P Singh and H.C Srivastava. 'Sparsity and Optimal ordering'. Journal of The Institute of Engineers (India), vol.57,pt EL6, June 1977, p274

[4] K.K.Goyal and L.P Singh. 'Optimal Elimination of Sparse System Using Dynamic Programming Technique'. Proceeding CS 9-81, March 1-4,1981, New Delhi.

[5] EPRI, "Exploring applications of Digital parallel Processing to Power System Problems," Seminar proceedings, Oct 4- 7, 1979.

[6] Y. Wallach, E. Handschin, C.Bongers, "An Efficient Parallel Processing Method for Power system State Estimation," Trans. IEEE, Vol. PAS-100, Nov.1981, pp.4402 – 6.

[7] M.Y.Patel, A.A.Girgis,, "Two-Level State Estimation for Multi-Area Power system", 1-4244-1298/$25.00 @2007IEEE

[8] Patel M. Y., Girgis A. A., "Two-Level State Estimation for Multi-Area Power System",1-4244-1298-6/07/$25.00 ©2007 IEEE.

BIOGRAPHIES

First Author was born in south Indian Village, Udupi District in 1963. He received the B.E in Electrical Engineering from National Institute of Technology (formerly known as "Regional Engineering College"), Silchar, Gwhati University of India, in 1988 and M.Tech honors degree, in Power System from IIT Roorkee (formerly known as "University of Roorkee"), Utarakhand, India, in 1995. The Author is the Ph.D scholar of Mewar University, Rajastan, India. From 1990 to 1999, he was a faculty at Manipal Institute of Technology, Manipal, India. From 2000 to 2009 he has been an Associate Professor with Sikkim-Manipal University.

Dr. H Ravishankar Kamath, completed his Bachelor of Engineering from Mysore University in the year 1989 and Master of Technology from National Institute of Technology Surathkal Karnataka in the year 1996 in power and energy system. He has done PhD from Manipal University in the year 2008.He has subject specification in soft computing and its various application in the field of power system and Nonconventional energy systems

TNC Transactions on Networks and Communications
SOCIETY FOR SCIENCE AND EDUCATION UNITED KINGDOM
VOLUME 2, ISSUE 4
ISSN: 2054 - 7420

A High-Resolution Laser Beam Collimator System with a High-NA Lens for a High-Density Ternary Barcode Detection System

Hiroo Wakaumi

Division of Electronics and Information Engineering, Tokyo Metropolitan College of Industrial Technology, Japan

wakaumi@s.metro-cit.ac.jp

ABSTRACT

A laser beam collimator system with a high numerical aperture lens and a 1.2 mm aperture masked collimator is proposed to realize a miniature high-resolution ternary barcode detection system in which high-density ternary barcodes can be detected. It was clarified that a 1.2 mm aperture mask combined with a 0.5 NA lens is suitable for maintaining the laser beam width at less than 150 µm over a wide range of more than 4.5 cm. The laser head with this collimator system was applied to a ternary barcode detection system. It was confirmed that the detection system could detect the ternary barcode with a minimum bar width of 0.2 mm over a practical detection range greater than 5 cm (which conventional detection systems could not detect) by optimizing the clamp bias voltage in the clamping circuit to -0.8 V, and the gray bar concentration to 58 %. Barcode detection results also showed that an optimized mask aperture for achieving a maximum detection range for the barcode with a 0.2 mm minimum bar width was 1.2 mm. This collimator system has potential applications in high-speed, high-resolution ternary or binary barcode detection systems.

Keywords: Optical detection system; Laser diode; Barcode; Ternary; Collimator.

1 Introduction

Real-time identification of barcodes is needed for applications such as goods management on production lines where high-speed detection is required. Though identification systems for mono or color two-dimensional binary barcodes using a CCD camera have been considered, its scanning speed is limited to nearly 50 scans/sec because of the complicated image processing and the need for focus adjustment [1,2]. This makes the high-speed sorting of goods problematic. In addition, an auxiliary light must be provided.

The authors have developed ternary barcode detection systems (BCDSs) using laser diode

DOI: 10.14738/tnc.24.318
Publication Date: 4th August 2014
URL: http://dx.doi.org/10.14738/tnc.24.318

(LD) scanning to resolve the above problems of low-speed scanning, focus adjustment and auxiliary lighting requirements [3-5]. In particular, the ternary BCDS using the dual-bias differential method could detect a 0.25 mm wide ternary barcode within a 7.4 cm detection range. This performance has also been achieved with long detection distances of around 35 cm [5]. However, the detection of a minimum 0.2 mm wide ternary barcode equivalent to conventional binary barcodes has not yet been achieved. In conventional ternary BCDSs, a low numerical aperture (NA=0.26) non-spherical lens with a relatively wide aperture (2.5–3 mm) optical masked collimator (consisting of a thin vinyl chloride sheet mask with a central hole), has been considered for achieving a narrow laser beam over a wide range for realizing as high a detection resolution as possible [6]. This is because a slightly wider aperture mask fabricated with high accuracy can be easily used because of an intrinsically wide depth of focus of the lens itself. However, it resulted in an insufficient beam width for detection distances over 35 cm while it could achieve a uniform beam over a wide range. Because of this inadequate performance of the optical collimator system in collimating the LD light, the detection resolution for the ternary BCDS is limited to 0.25 mm. Therefore, the development of a high-resolution optical collimator system that provides a narrower laser beam over a wide range, is required to increase the detection resolution. As an approach to increasing the detection resolution, the use of a combination of a non-spherical lens and beam expander was considered. While the beam expander is useful for extending the width of the laser light beam before condensing it with the focusing non-spherical lens to achieve a narrow beam [7,8], this approach results in a large and expensive system. Because a miniature BCDS is desirable for practical applications, it is also essential to fabricate the system compactly.

In this study, a high-resolution laser beam collimator system consisting of a high NA non-spherical lens providing high resolution and a narrow aperture masked collimator operating as a narrow optical stop for a laser light beam [9], is proposed. This is to provide a high quality laser beam and a wide depth of focus for short detection distances, resulting in the achievement of a small high-density ternary BCDS.

2 High Resolution Collimator

The conventional collimator system, using a low NA (NA=0.26) non-spherical lens with an intrinsic focal length of 14.5 mm, is required to adjust a masked collimator aperture size for a scanning distance of over 35 cm when it is desirable to achieve a uniform laser beam over a wide range. When a masked collimator with a hole diameter (aperture) Φ of 2.5 mm was attached after adjusting the focal distance of the lens to near 35 cm, the laser beam widths became 175–185 μm for a scanning range of 5 cm as shown in Fig. 1 [6]. These laser beam widths were not narrow enough to detect the 0.2 mm wide high-density ternary barcode and so limited the barcode detection resolution to 0.25 mm.

Resolution of lens δ is given by K/NA [10]. Here, K is constant. Considering this fact, the

increase of NA of the lens is needed to increase the detection resolution. Narrowing a mask aperture of masked collimator is also needed to achieve more uniform beam over a wide range. Such a high resolution collimator system can keep a narrow beam within a wide range as shown in Fig. 2. Based on such ideas, the proposed collimator system uses a high resolution non-spherical lens with an NA of 0.5 and a narrow-aperture masked collimator, to realize a short focus laser head corresponding to short distance scanning. The position of the high 0.5 NA non-spherical lens with an intrinsic focal length of 4 mm was designed to provide a focal distance of 15 cm. The masked collimator with an aperture of Φ=1.2–1.5 mm was attached to the laser head to retain a uniform laser beam over a wide range of nearly 5 cm.

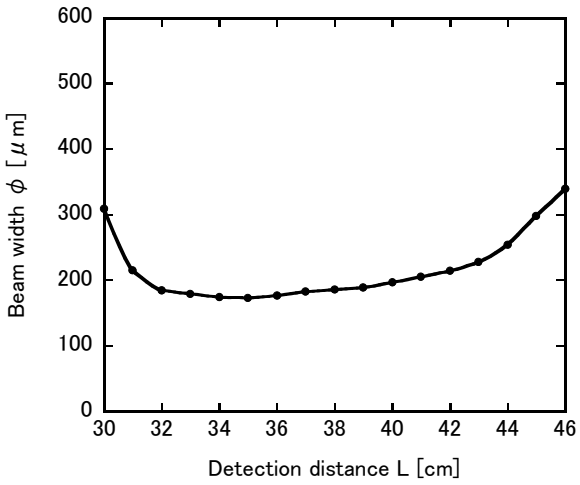


Figure 1: Beam width versus detection distance in a conventional collimator laser head. Φ=2.5 mm

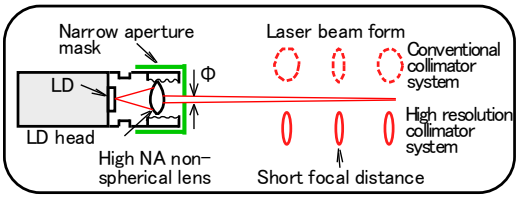


Figure 2: Laser beam forms for conventional collimator and high-resolution collimator systems

3 Experimental Results

3.1 Laser Beam Width

The laser head using the conventional low-NA non-spherical lens cannot simply shorten its focal distance. As described above, because the beam width of the laser light emitted from the laser head was 175–185 μm around a focal distance of nearly 35 cm, it was impossible to apply it to high density ternary BCDSs. Even if its focal distance was shortened to 15 cm by adjusting the position of a lens attached in front of the laser equivalent to a small scanner, the scanning range of a laser head with a masked collimator of Φ=1.2 mm producing light beams narrower than 150 μm was below 2 cm, which was extremely narrow (Fig. 3). This was near the limitation of the laser beam width required for detecting 0.2 mm wide ternary barcodes.

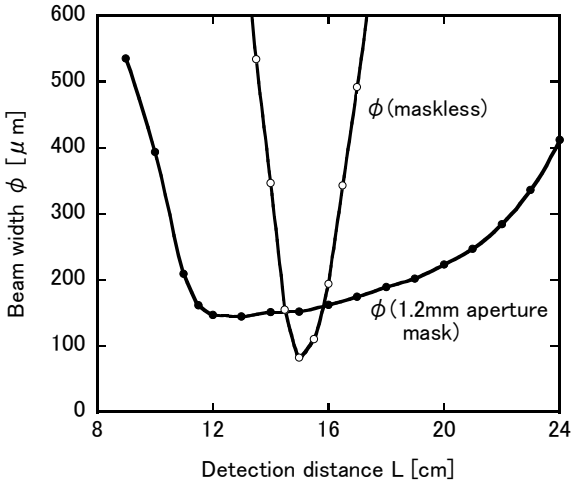


Figure 3: Beam width versus detection distance when the focal distance is adjusted to 15 cm using a conventional laser head

The laser head using the proposed collimator system consisted of a semiconductor laser of DL3149-057 (lasing wavelength λ=670 nm) with a non-spherical lens of NA=0.5 and an intrinsic focal length of 4 mm as described above. The beam width versus detection distance characteristics with masked collimators of Φ=1.2 mm and 1.5 mm (including that without a masked collimator) are shown in Fig. 4. Although, without a masked collimator, the beam width at a detection distance L=15 cm decreased to 70 μm resulting from the increase in NA, the scanning range ΔL producing light beams narrower than 150 μm was 2 cm, which was still too narrow. Conversely, when a laser head using masked collimators with apertures of 1.2 mm and 1.5 mm was used, the scanning range extended to 4.5 cm and 4.4 cm, respectively. Thus, it was decided that a high-resolution laser beam collimator system consisting of a high NA non-spherical lens with a 1.2 mm wide masked collimator was the most useful for realizing miniature BCDSs with wide scanning ranges.

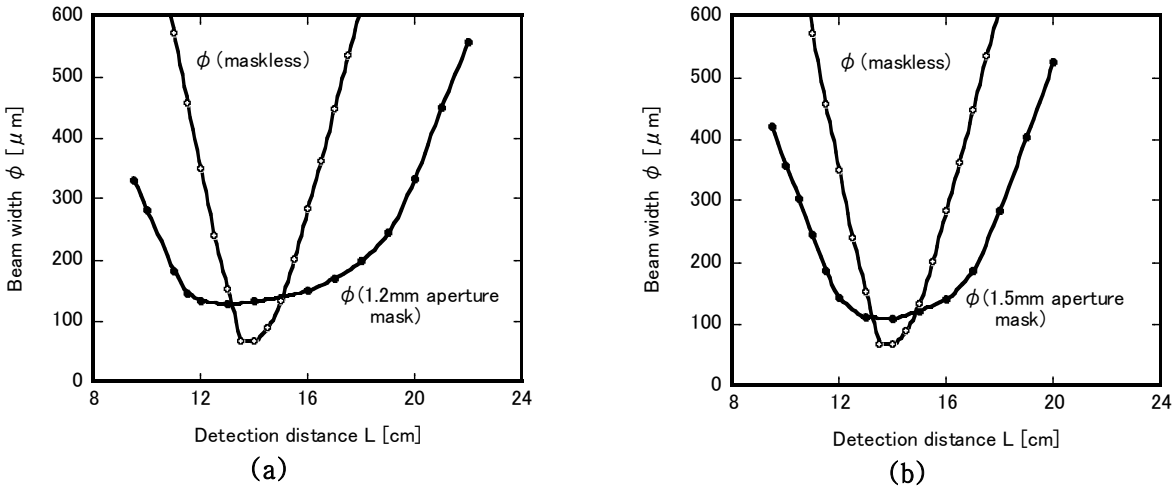


Figure 4: Beam width versus detection distance when the masked collimator aperture is 1.2 mm (a) and 1.5 mm (b) in the proposed high NA system

3.2 Application to Ternary BCDS

The laser head combined a high NA lens with a masked collimator of Φ=1.2 mm. This was expected to realize the widest scanning range, and was applied to a ternary BCDS including a four-character ternary barcode (consisting of nine elements per character except for start and stop codes) as shown in Fig. 5. The detection characteristics were measured. The distance between the polygonal rotating mirror and the laser head was 7 cm. The scanning distance indicating the distance between the laser head and the surface of the barcode was nearly 15 cm on average. In this system, the detection range was controlled by adjusting the average level of gray signals using a clamp bias voltage in the clamping circuit [11]. It was expected that the average level of the gray signals changed depending on barcode pattern density and gray bar concentration. Figure 6 shows detection signal processing waveforms depending on a gray bar concentration. Actually, it is seen that gray signals in a clamped average signal increase as the gray bar concentration increases from 52 % to 58 %. This fact indicates the need of optimization of the clamp bias voltage because differential signals change depending on an average level of the clamped average signal. Figure 7 shows a change of the occurrence of code errors depending on the clamp bias voltage. Strong saturation in differential signals was seen without a clamp bias, causing code errors in a decodable signal. However, when the clamp bias voltage of -0.8 V was applied, differential signals came not to saturate strongly. This weak saturation caused correct codes in the decodable signal. Consequently, applying some clamp bias voltages seems desirable.

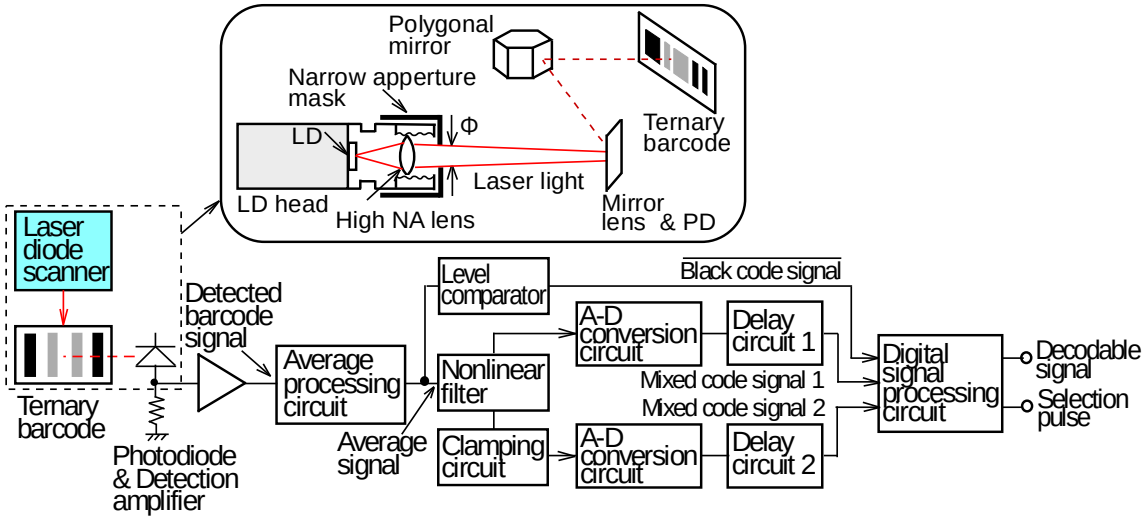


Figure 5: A ternary barcode detection system configuration

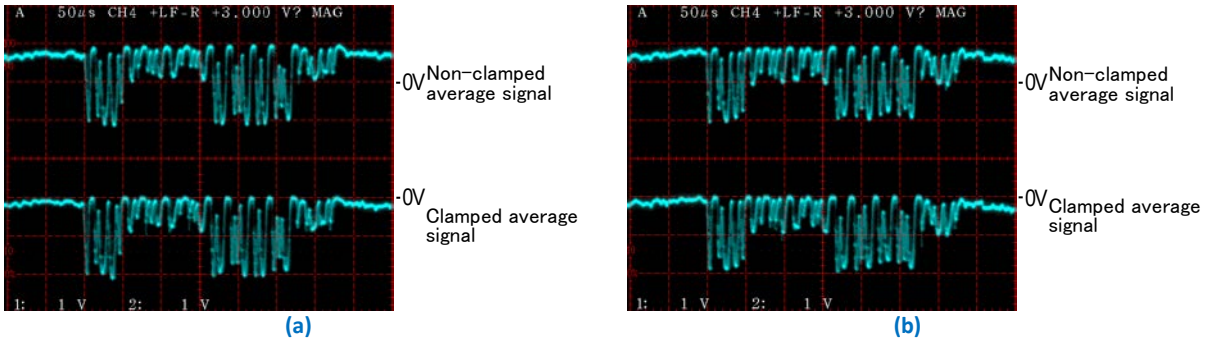


Figure 6: Detection signal processing waveforms depending on a gray bar concentration of 52 % (a) and 58 % (b)

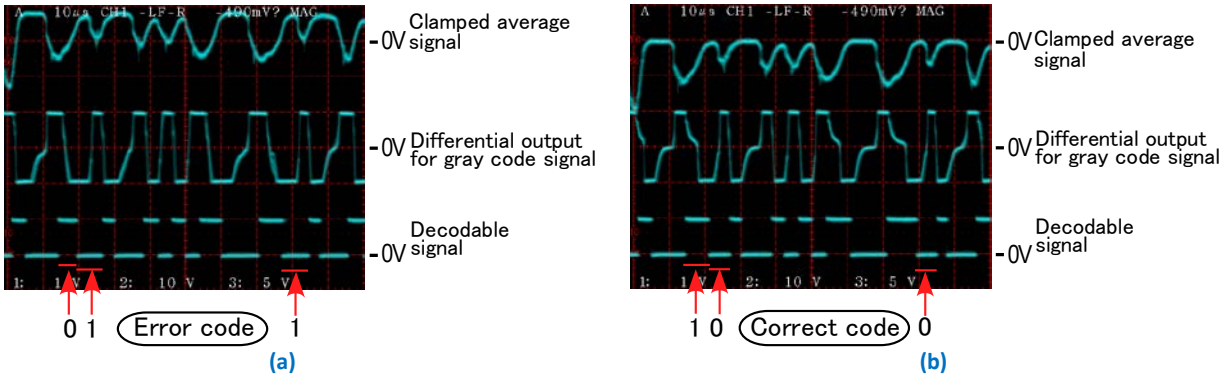
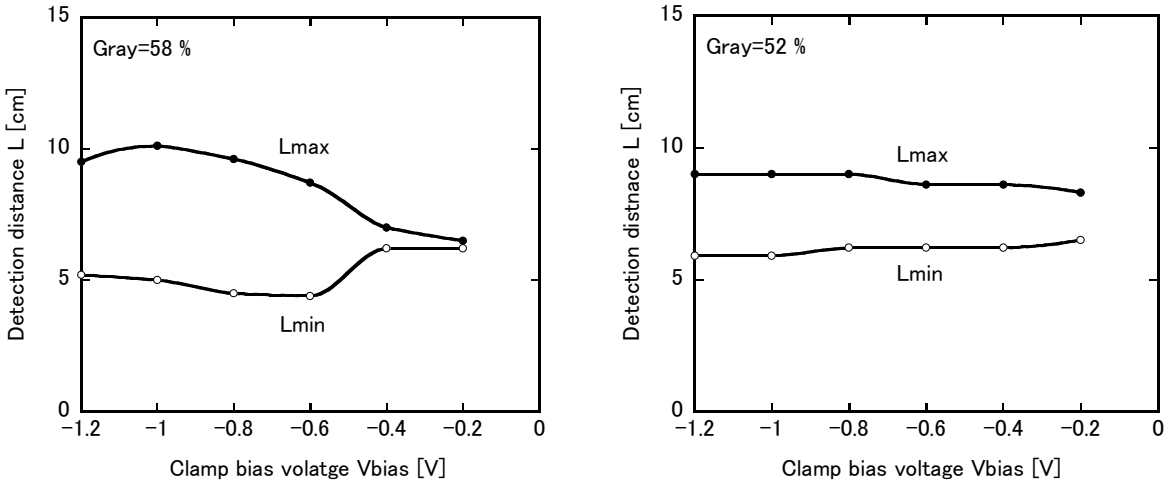


Figure 7: Detection signal processing waveforms depending on a clamped bias voltage V_{bias} of 0 V (a) and -0.8 V (b)

Thus, based on these facts, the detection characteristics for the clamp bias voltage with respect to different gray bar concentrations when using the barcode with a minimum bar width of W=0.2 mm, were compared (Fig. 8(a) and (b)). It is apparent that when the gray bar concentration is increased from the conventional value of 52 % to 58 %, compared with that of the white bar, the detection range is greatly extended for a clamp bias voltage V_{bias} of near -0.8 V. Although the gray signals corresponding to narrow gray bars specifically diminish for a narrow ternary barcode of nearly 0.2 mm, the increase in the detection range is thought to be because these gray signals increase (resulting in a wide detection range) when increasing the gray bar concentration. When this gray bar concentration is increased further, the detection range decreased at the same clamp bias voltage.



(a) (b)

Figure 8: Detection distance versus clamp bias voltage with a gray bar concentration of 58 % (a) and 52 % (b). W=0.2 mm. Scanning speed fs=333 scans/sec. Light output power of the LD measured through the masked collimator of Φ=1.2 mm: P_o=0.6 mW

This decrease in the detection range is also thought to be because gray signals resulting from a further increase in the gray bar concentration caused the system to exceed the comparator level of the black signals. At the optimum clamp bias voltage mentioned above, the detection distance versus minimum bar width is shown in Fig. 9. We can see that though the detection range for the barcode with a W of over 0.25 mm is not quite dependent on the gray bar concentration, a high gray bar concentration is effective in extending the detection range for a narrow barcode of W=0.2 mm. In this regard, when the gray bar concentration was increased by 6 % to 58 %, a practical detection range greater than 5 cm was obtained even for a high density barcode of W=0.2 mm. This could not be achieved in the conventional BCDS with a scanning distance of nearly 35 cm.

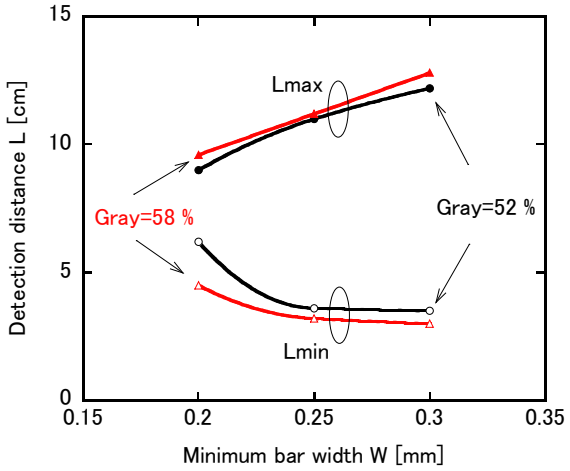


Figure 9: Detection distance versus minimum bar width depending on the gray bar concentration. fs=333 scans/sec. V_{bias}=−0.8 V. Φ=1.2 mm. P_o=0.6 mW

Though a 1.2 mm aperture mask was chosen in section 3 from the high possibility of achievement of narrow beam width within a wide range, barcode detection characteristics were actually tested to confirm the optimum masked collimator aperture size. Figure 10 shows detection distance versus masked collimator aperture. It is apparently seen that a 1.2 mm mask aperture is most desirable for a wide detection range. When this mask was used, the detection range became maximum.

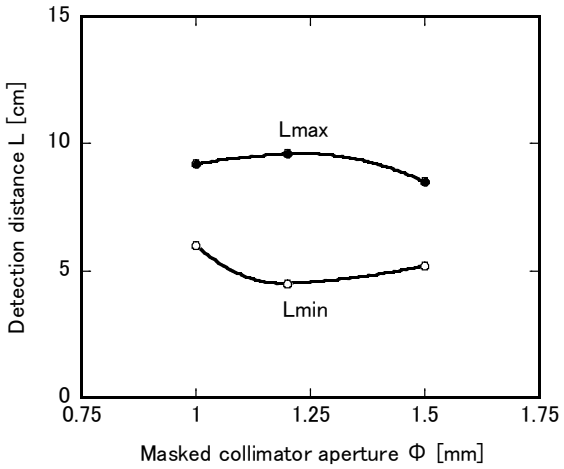


Figure 10: Detection distance versus masked collimator aperture. V_{bias}=-0.8 V

Thus, it was established that by applying a high 0.5 NA non-spherical lens with a narrow 1.2 mm aperture masked collimator, and optimizing the gray bar concentration and clamp bias voltage, a miniature ternary BCDS able to detect narrow 0.2 mm wide ternary barcodes, equivalent to conventional binary barcodes, could be achieved.

4 Conclusions

A high-resolution laser beam collimator system with a high numerical aperture non-spherical lens and a 1.2 mm aperture masked collimator has been proposed to realize a miniature ternary barcode detection system which can detect high density ternary barcodes. It was clarified that a 1.2 mm aperture mask combined with a 0.5 NA lens is suitable for maintaining the laser beam width at less than 150 um over a wide range of more than 4.5 cm. The laser head with this collimator system was applied to a ternary barcode detection system. As a result, it was confirmed that the detection system with the high-resolution collimator system could detect a ternary barcode with a minimum bar width of 0.2 mm for a practical wide detection range greater than 5 cm, by optimizing the clamp bias voltage to -0.8 V and the gray bar concentration to 58 %. Under this condition, an optimized mask aperture was 1.2 mm for achieving a maximum detection range for the barcode with a 0.2 mm minimum bar width. This collimator system has potential applications in high-speed, high-resolution ternary or binary barcode detection systems.

REFERENCES

[1]. J. Hiramoto, *Knowledge of Barcode and Two-Dimensional Code*, 5th Edition 2001, Tokyo: Japan Industrial Publishing (Japan).

[2]. T. Nagaya, T. Yamazaki, M. Hara, and T. Nojiri, *Two-Dimensional Code for High-Speed Reading*, in *Proc. of the 52th Information Processing Society of Japan (IPSJ) General Conference*, 1996, pp. 253-254.

[3]. H. Wakaumi, *An Envelope-Differential Composite Method for a High-Density Ternary Barcode Detection System*, The IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences (Japanese Edition), 2011, Vol. J94-A, No. 2, pp. 142-144.

[4]. H. Wakaumi, *A High-Density Ternary Barcode Detection System Employing a Stable Fixed-Period Delay Method*, Optical Review, 2011, Vol. 18, No. 5, pp. 408-413.

[5]. H. Wakaumi, *A Ternary Barcode Detection System Employing a Dual-Bias Differential Method*, in the 13th Mechatronics Forum International Conference-Mechatronics 2012, 2012, pp. 399-403.

[6]. H. Wakaumi and C. Nagasawa, *High detection resolution for two-dimensional bar-code detection system using masked collimators*, Sensors and Actuators A: Physical, 2004, Vol. 110, pp. 177-181.

[7]. B. Grahame and T. Tsunehisa, *Laser Diode Collimator System*, Japan Patent Application number : 2003-018131, Jan. 28, 2003.

[8]. T. Ohsawa and T. Obokata, *Lasermetrics*, 1st Edition 1994, Tokyo: Shokabo (Japan).

[9]. H. Wakaumi, *A High-Resolution Laser Beam Collimator System for a High-Density Ternary Barcode Detection System*, in the 13th International Conference on Control, Automation and Systems (ICCAS2013), 2013, pp. 1384-1387.

[10]. M. H. Freeman, *Optics*, 10th Edition 1997, Oxford: Butterworth Heinemann (United Kingdom).

[11]. H. Wakaumi, *A High-Density Ternary Barcode Detection System with a Dual-Bias Differential Method*, Journal of Sensor Technology, 2013, Vol. 3, No. 1, pp. 6-12.

TNC Transactions on Networks and Communications
SOCIETY FOR SCIENCE AND EDUCATION UNITED KINGDOM
VOLUME 2, ISSUE 4
ISSN: 2054 - 7420

CPW-Fed KOCH SNOWFLAKE Fractal Antenna for UWB Wireless Applications

Abdelati Reha[1*], Abdelkebir El Amri[1], Othmane Benhmammouch[3], Ahmed Oulad Said[4]**
[1]*RITM Laboratory, EST CASABLANCA, Hassan II University, Casablanca, Morocco*
[2]*Mundiapolis University, Nouaceur, Casablanca, Morocco*
[3]*Royal Air Academy, Marrakech, Morocco*
* reha.abdelati@gmail.com, ** elamri_abdelkebir@yahoo.fr,
[3]othmane.benhmammouch@gmail.com, [4]a_ouladsaid@hotmail.com

ABSTRACT

Four iterations of a Coplanar Waveguide (CPW)-Fed KOCH SNOWFLAKE fractal antenna are studied. Increasing the number of iterations allow us obtaining a simple and miniaturized antenna with good performances, operating for Ultra Wide Band (UWB) applications.

The proposed antennas are a good solution for the 3.7-4.2GHZ C-Band, the 5.15-5.82 Wireless Local Area Network (WLAN), and for the 5GHZ Worldwide Interoperability for Microwave Access system (WIMAX) applications. The simulation was performed in FEKO 6.3.

Keywords: Fractal antennas, KOCH SNOWFLAKE, Multi-Band, Ultra Wide-Band, UWB, Antenna design.

1 Introduction

With the proliferation and miniaturization of telecommunications systems and their integration in restricted environments, such as Smart-phones, tablets, cars, airplanes, and other embedded systems. The design of compact multi-bands and Ultra Wide Band (UWB) antennas becomes a necessity.

For designing this kind of antennas, two techniques are used:

1. Designing multi-band antennas operating in several frequencies bands. Several studies have been made to design this kind of antennas by using fractal geometries or adding slots to the radiating elements [1-4].
2. Designing UWB antennas operating in the frequencies bands exceeding 500MHZ or having a fractional bandwidth of at least 0.20, UWB wireless communication occupies a bandwidth from 3.1 to 10.6 GHz (based on the FCC "Federal Communication

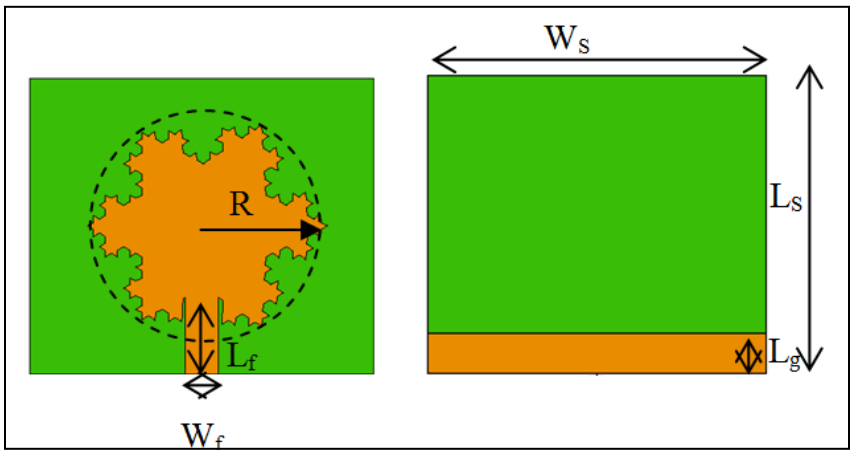
DOI: 10.14738/tnc.24.337
Publication Date: 24th August 2014
URL: http://dx.doi.org/10.14738/tnc.24.337

Commission") [5-12][15]. One of the interesting techniques used is the fractal geometry, because it's a simple technique based on the auto-similarity, the most known techniques used are: Minkowski Island, Koch loop, Pascal's triangle and Sierpinski gaskets… [13-16].

In this paper, we propose a CPW-fed KOCH SNOWFLAKE Fractal slot antenna. The simulation is done by FEKO 6.3 based on the Method of the Moment (MoM) [17].

2 Antenna Design

As shown in figure 1, the proposed antenna is printed on a FR4 dielectric substrate of relative permittivity εr = 4.4, thickness H=1.6mm and fed by a CPW transmission line. Several studies have used this mode of feeding because it's one of the ways to increase the Bandwidth of the antenna [4][7][14][19].



(a) the front face (b) the back face

Figure1: The geometry of the CPW-Fed KOCH SNOWFLAKE Fractal Antenna

The characteristic impedance of a microstrip line (Zm) is given by the formula (1) [15][18]

$$Z_m = \frac{120.\pi}{\sqrt{\varepsilon_e}}\left[\frac{w_f}{H} + 1.393 + 0.667\ln\left(\frac{W_f}{H} + 1.444\right)\right]^{-1} \quad (1)$$

And $$\varepsilon_e = \frac{1}{2}(\varepsilon_r + 1) + \frac{1}{2}(\varepsilon_r - 1)\left(1 + 12\frac{H}{W_f}\right)^{-\frac{1}{2}} \quad (2)$$

With

ε_e: The effective permittivity

ε_r: The relative permittivity of the substrate

H: The thickness of the substrate

W_f: the width of the microstrip line

To adjust Z_m=50Ω, the value of Wf should be 3.35mm.

The other parameters are as follow:mW_s= 35mm, L_s=30mm, L_f=8mm, and L_g=4mm

The generation of the KOCH SNOWFLAKE iterations is based on the triangle initiator and on the generator shown in the figure 2.

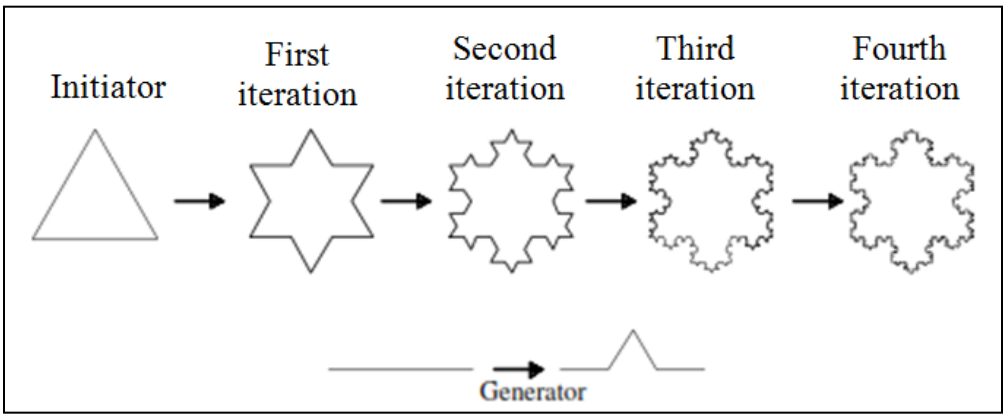


Figure2: The Four iterations of the KOCH SNOWFLAKE Fractal Antenna [20]

We observe that the radius of the fractal antenna (R) is the same for all the iterations as shown in the figure3.

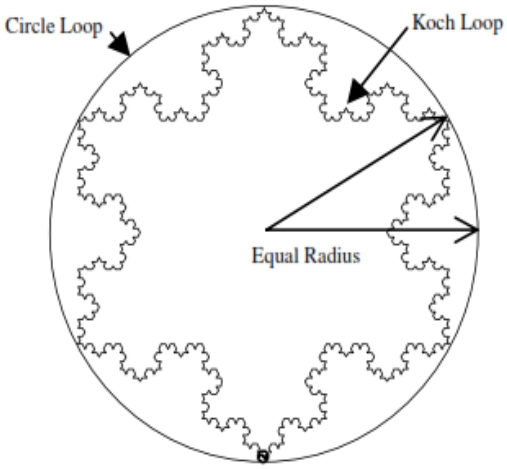


Figure 3: Circular and Koch loops of equal radii [21]

A parametric study is based on the variation of the parameters R.

3 Results and Discussions

3.1 The initiator (iteration 0)

For the initiator (figure 4), the variation of the simulated S_{11} parameter versus the frequency for some values of R is shown in the figure 5.

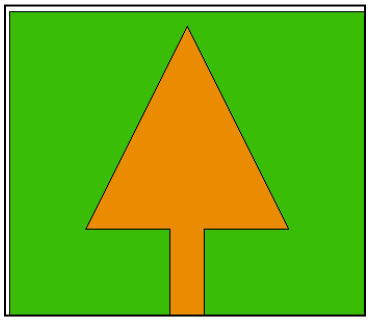


Figure 4: the front face of the antenna (the initiator)

We observe that, for R=13mm, the antenna has 2 resonant frequencies f_{r1} = 4.1GHz with S_{11}=-16.6dB and f_{r2}= 5GHz with S_{11}=-15.45dB. The bandwidth (-10dB) of the antenna is 1.76GHz (3.5 - 5.26 GHz).

For the R=14mm, the antenna has 1 resonant frequency f_{r1}=4.4GHz with S_{11}= -29.8dB. The bandwidth (-10dB) of the antenna is 1.5GHz (3.5 - 5 GHz).

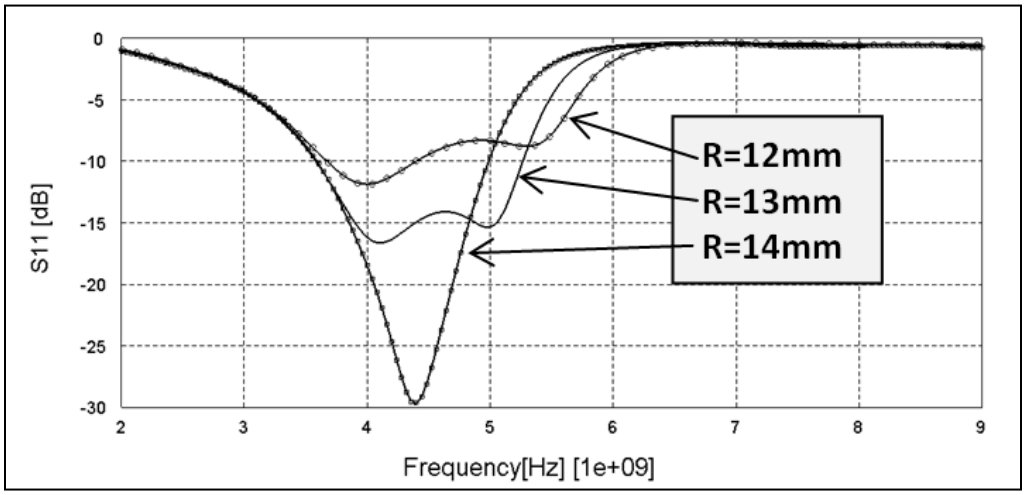


Figure5: Simulated S_{11} versus frequency graph of the antenna (iteration0)

The figure 6 shows the evolution of the total maximum gain of the antenna versus the frequency for some values of the radius R. we observe that the gain increases when the frequency increases. The figure 7 shows an example for the 3D total gain pattern of the antenna for R=14mm and for the two frequencies 3.5GHZ and 5GHZ. We observe that the shape of this pattern is nearly similar for the two frequencies.

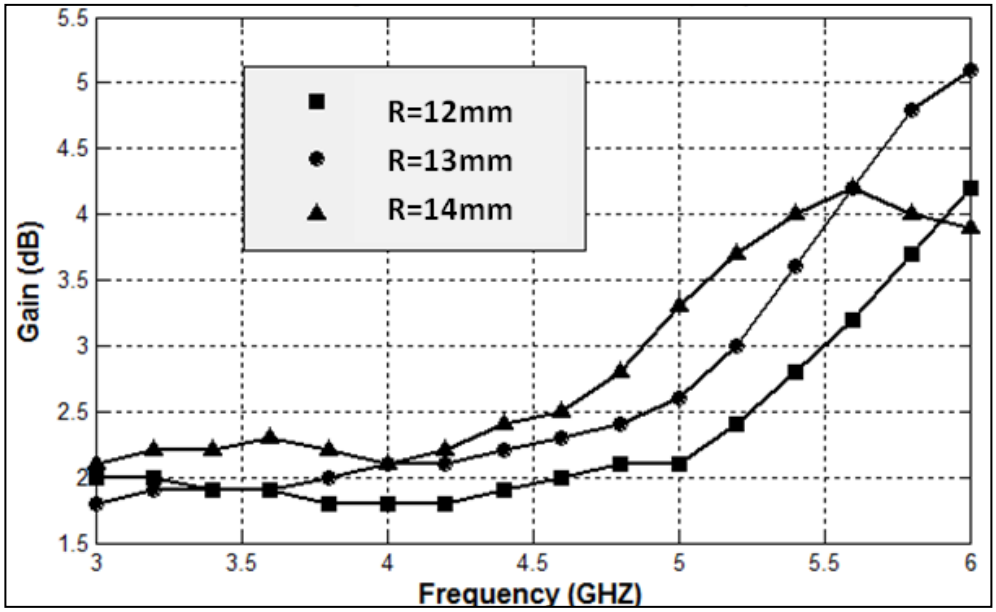
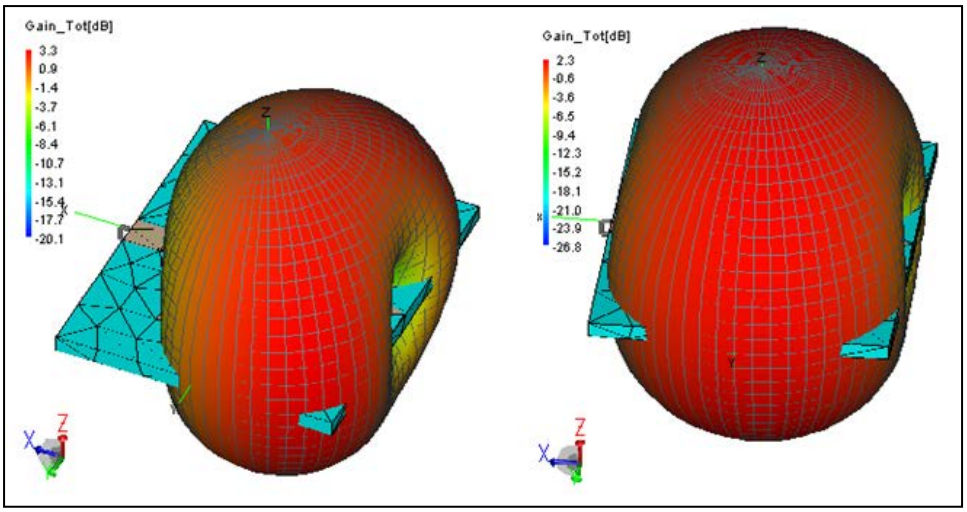


Figure6: Simulated Maximum Gain versus frequency graph of the antenna (iteration 0)



a)F=5GHZ **(b)F=3.5GHZ**

Figure7: the 3D total gain of the antenna for R=14mm

The table 1 summarizes the resonant frequencies, the bandwidths and the gains of the antenna in the Bandwidth.

Table 1: the bandwidths and the gains for the antenna (iteration 0)

R (mm)	Resonant frequencies (GHz)	Bandwidth(-10dB)	S_{11}* (dB)	Gain (dB)**
12	4	750MHz (3.65 – 4.4)	-11.9	1.8 to 1.9
13	4.1 and 5	1.76GHz (3.5 – 5.26)	-16.6 and 15.45	1.9 to 3.3
14	4.4	1.5GHz (3.5 – 5)	-29.8	2.3 to 3.3

(*) the S_{11} are given in the resonant frequencies
(**) the Gains are given in the bandwidth (-10dB)

3.2 The First iteration

For the first iteration (figure 8), the variation of the simulated S_{11} parameter versus the frequency for some values of R is shown in the figure 9.

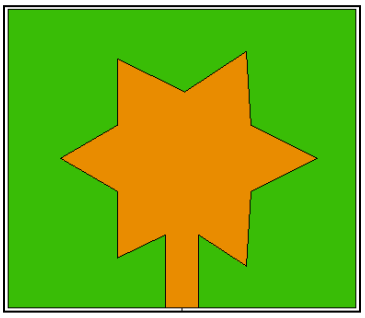


Figure 8: the front face of the antenna (First iteration)

We observe that, for R=13mm, the antenna has 3 resonant frequencies f_{r1} = 4.11GHz with S_{11} = -42dB, f_{r2}= 5.4GHz with S_{11}=-16.4dB and f_{r3} = 6.7GHz with S_{11} = -16.16dB. The largest bandwidth of the antenna is 2.21GHz (3.56 - 5.77 GHz).

For the R=14mm, the antenna has 3 resonant frequencies f_{r1}=4.04GHz with S_{11}= -15.7dB, f_{r2}= 5.4GHZ with S_{11}= -39.25dB and f_{r3} = 6.4GHZ with S_{11} = -17.58dB. The largest bandwidth of the antenna is 2.2GHz (3.6 – 5.8 GHz).

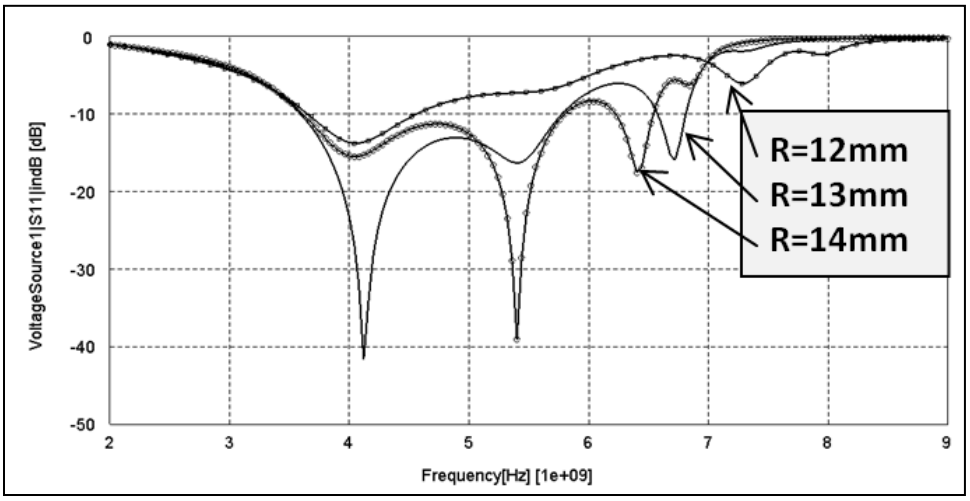


Figure9: Simulated S_{11} versus frequency graph of the antenna (First iteration)

The figure 10 shows the evolution of the maximum total gain of the antenna versus the frequency for some values of the radius R. we observe that the gain increases when the frequency increases. We observe also that the gain increases when the R increase. The figure 10 shows an example for the 3D total gain pattern of the antenna for R=14mm and for the two frequencies 4GHZ and 5.4GHZ. We observe that the shape of this pattern is nearly similar for the two frequencies.

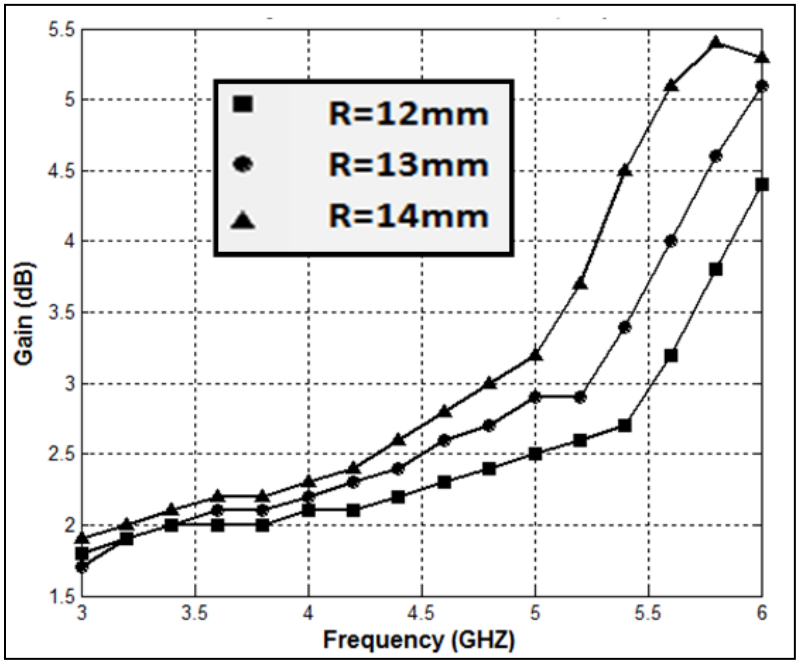
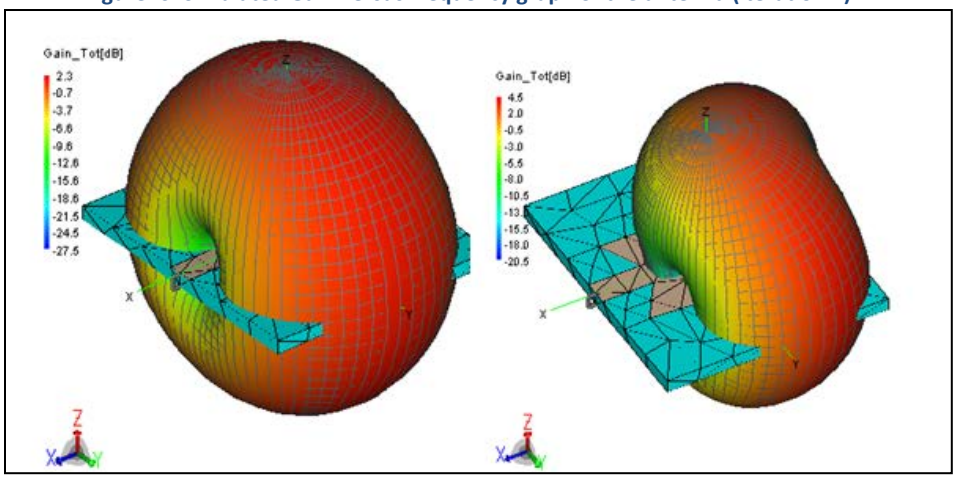


Figure10: Simulated Gain versus frequency graph of the antenna (iteration 1)



(a)F=4GHz **(b)F=5.4GHz**

Figure11: the 3D total gain of the antenna for R=14mm

The table 2 summarizes the resonant frequencies, the bandwidths and the gains of the antenna in the Bandwidth.

R(mm)	Resonant frequencies (GHz)	Bandwidth (-10dB)	S_{11}* (dB)	Gain (dB)**
12	4.05	930MHz (3.64 – 4.57)	-13.84	2 to 2.3
13	4.11 and 5.4 and 6.7	2.21GHz (3.56 - 5.77) And 210MHz (6.59 – 6.8)	-42 and -16.4 and -16.16	2.1 to 4.5 And 5.5 to 5.7
14	4.04 and 5.4 and 6.4	2.2GHz (3.6 – 5.8) And 310MHz (6.21 – 6.52)	-15.7 and -39.25 and -17.58	2.2 to 5.4 And 5.4 to 5.6

Table 2: the bandwidths and the gains for the antenna (First iteration)

(*) the S_{11} are given in the resonant frequencies
(**) the Gains are given in the bandwidth

3.3 The Second iteration

For the second iteration (figure 12), the variation of the simulated S_{11} parameter versus the frequency for some values of R is shown in the figure 13.

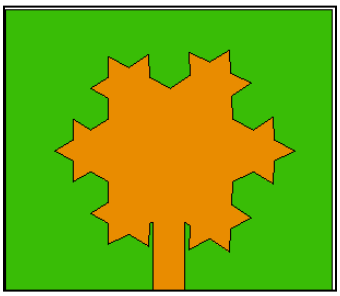


Figure 12: the front face of the antenna (Second iteration)

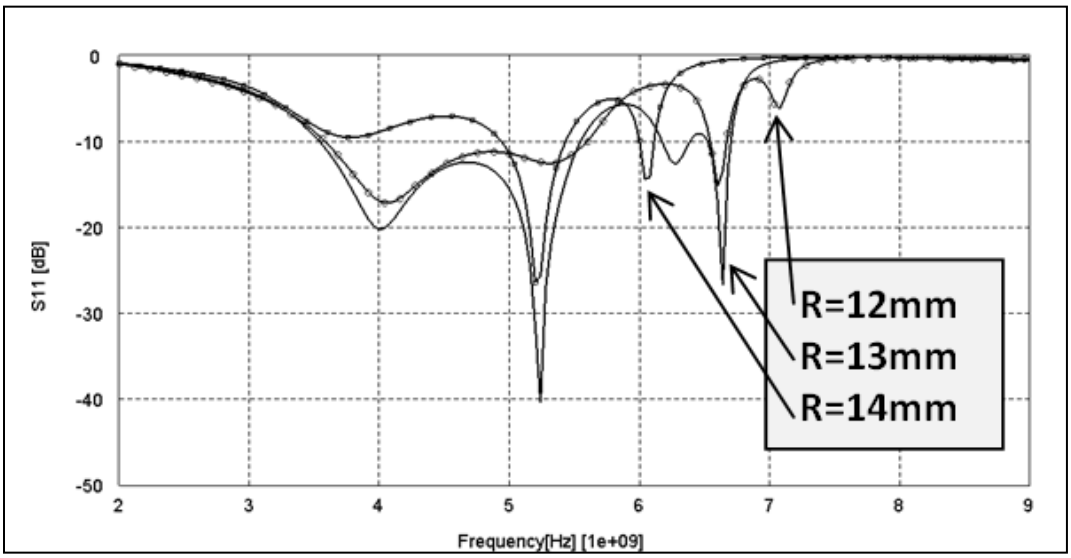


Figure13: Simulated S_{11} versus frequency graph of the antenna (Second iteration)

We observe that, for R=13mm, the antenna has 4 resonant frequencies f_{r1} = 4GHz with S_{11} = -20.4dB, f_{r2}= 5.23GHz with S_{11}=-40.3dB, f_{r3} = 6.27GHz with S_{11} = -12.55dB, and f_{r4} = 6.64GHz with S_{11} = -27dB. The largest bandwidth of the antenna is 2.02GHZ (3.53 - 5.55GHz).

For the R=12mm, the antenna has 3 resonant frequencies f_{r1}=4.07GHz with S_{11}= -17.24dB, f_{r2}= 5.32GHz with S_{11}= -12.64, and f_{r3}= 6.6GHz with S_{11}= -15.3dB. The largest bandwidth of the antenna is 2.02GHz (3.57 – 5.59 GHz).

For the R=14mm, the antenna has 2 resonant frequencies f_{r1}=5.2GHz with S_{11}= -26.55dB, and f_{r2}= 6.07GHz with S_{11}= -14.3dB, and fr3= 6.6GHz with S_{11}= -15.3dB. The largest bandwidth of the antenna is 460MHz (4.95-5.41 GHz).

The figure 14 shows the evolution of the gain of the antenna versus the frequency for some values of the radius R. we observe that the gain increases when the frequency increases. We observe also that in general, the gain increases when the R increases. The figure 15 shows an example for the 3D total gain pattern of the antenna for R=13mm and for the two frequencies 4GHz and 5.2GHz. We observe that the shape of this pattern is nearly similar for the two frequencies.

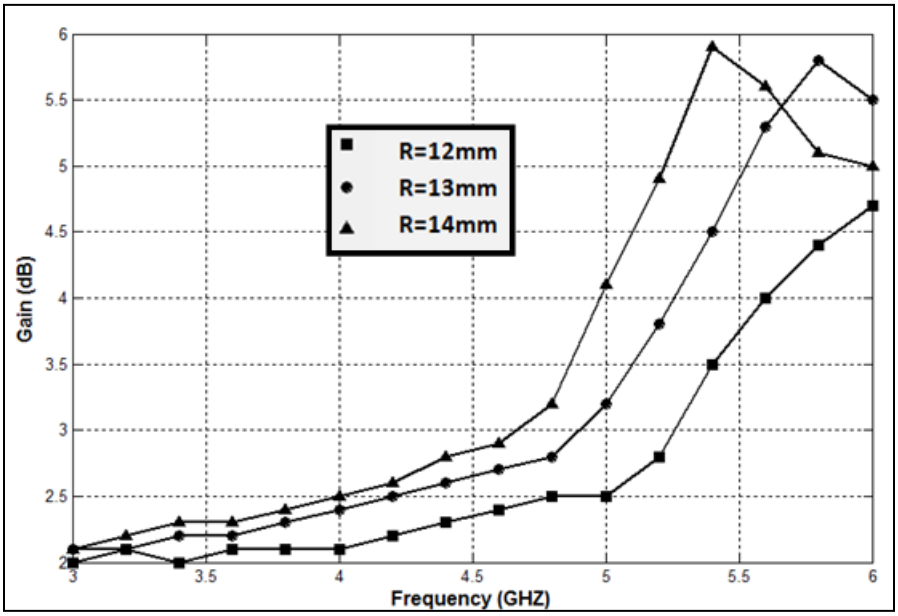
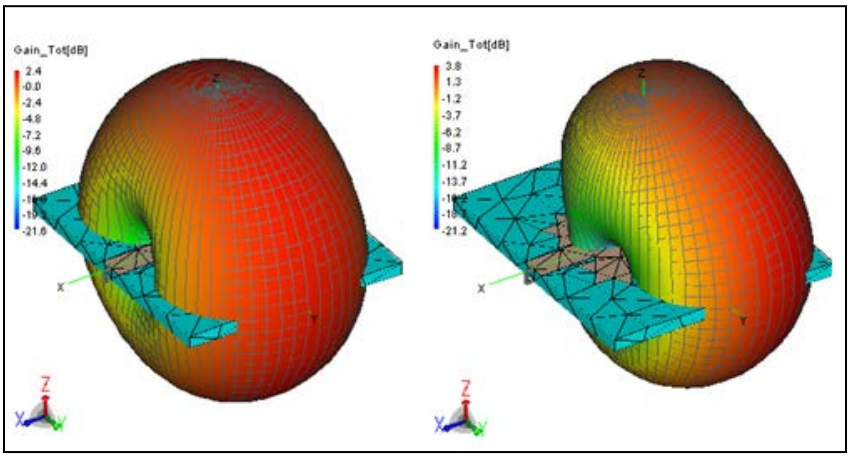


Figure14: Simulated Gain versus frequency graph of the antenna (iteration 2)



(a)F=4GHZ (b)F=5.2GHZ

Figure15: the 3D total gain of the antenna for R=13mm

The table 3 summarizes the resonant frequencies, the bandwidths and the gains of the antenna in the Bandwidth.

Table 3: the bandwidths and the gains for the antenna (First iteration)

R(mm)	Resonant frequencies (GHZ)	Bandwidth (-10dB)	S_{11}* (dB)	Gain (dB)**
12	4.07 and 5.32 and 6.6	2.02GHZ (3.57 – 5.59)	-17.24 and -12.64and -15.3	2.1 to 4 And 5.3 to 4.9
13	4 and 5.23 and 6.27 and 6.64	2.02GHZ (3.53 - 5.55) And 240MHZ (6.16 – 6.4) And 180MHZ (6.52-6.7)	-20.4 and -40.3 and -12.55 and -27	2.2 to 5.1 And 4.9 to 4.1 And 4.7 to 5.1
14	5.2 and 6.07	460MHZ (4.95 – 5.41) And 120MHZ (5.99 – 6.11)	-26.55 and -14.3	3.9 to 5.6 And 4.2 to 5

(*) the S_{11} are given in the resonant frequencies
(**) the Gains are given in the bandwidth

3.4 The Third iteration

For the third iteration (figure 16), the variation of the simulated S_{11} parameter versus the frequency for some values of R is shown in the figure 17.

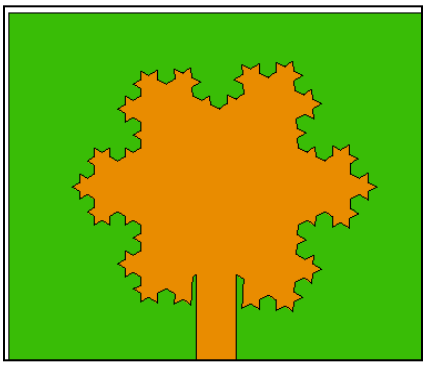


Figure 16: the front face of the antenna (Third iteration)

We observe that, for R=13mm, the antenna has 3 resonant frequencies f_{r1} = 3.9GHz with S_{11} =-17.67dB, f_{r2}= 5.08GHz with S_{11}=-21.45dB, and f_{r3} = 5.92GHz with S_{11} = -13.31. The largest bandwidth of the antenna is 1.89GHz (3.46 - 5.35GHz).

For the R=12mm, the antenna has 3 resonant frequencies f_{r1}=4GHz with S_{11}= -19dB, f_{r2}= 5.2GHz with S_{11}= -16.4, and f_{r3}= 7GHz with S_{11}= -18.5. The largest bandwidth of the antenna is 2GHz (3.49 – 5.49 GHz).

For the R=14mm, the antenna has 2 resonant frequencies fr1=5.03GHz with S_{11}= -35.8dB, and fr2= 5.73GHz with S_{11}= -23.7dB. The largest bandwidth of the antenna is 460MHz (4.74-5.2 GHz).

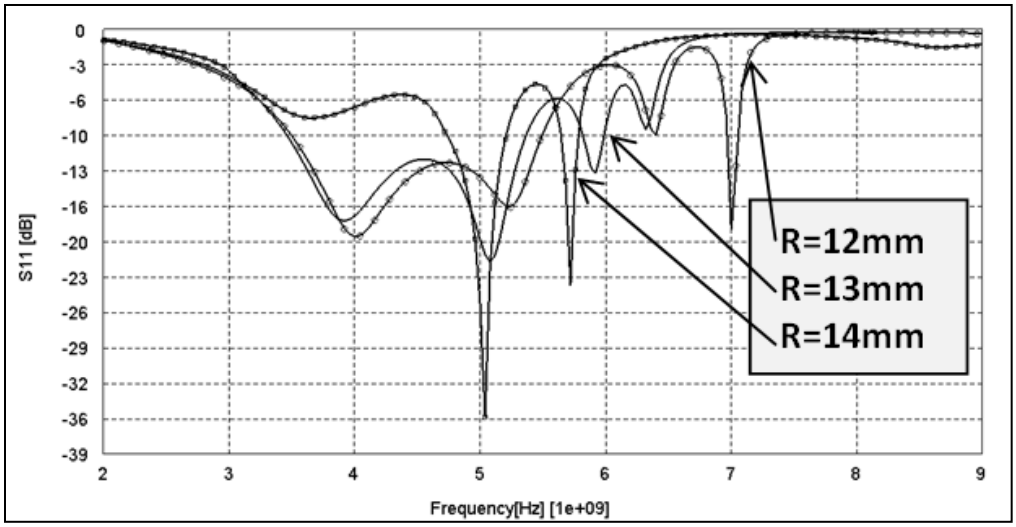


Figure17: Simulated S_{11} versus frequency graph of the antenna (Third iteration)

The figure 18 shows the evolution of the gain of the antenna versus the frequency for some values of the radius R. we observe in general, that the gain increases when the frequency increases. We observe also that in general, the gain increases when the R increases. The figure 19 shows an example for the 3D total gain pattern of the antenna for R=13mm and for the two frequencies 4GHz and 5GHz.

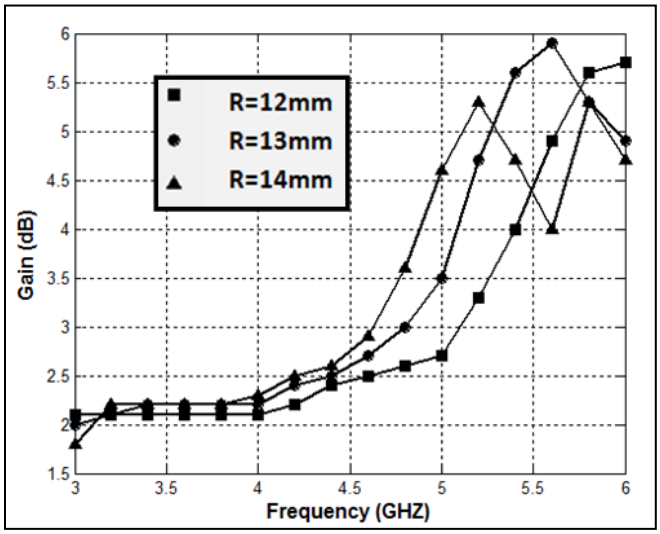
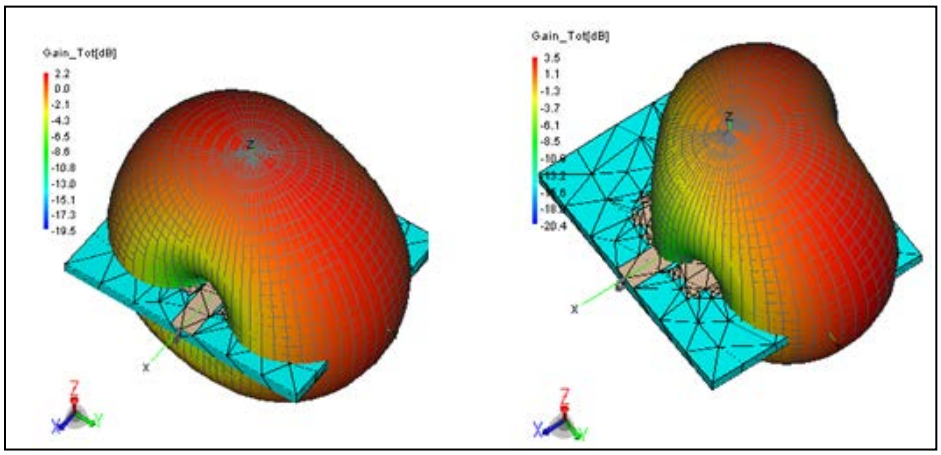


Figure 18 : Simulated Gain versus frequency graph of the antenna (iteration 3)



(a)F=4GHZ **(b)F=5GHZ**

Figure19: the 3D total gain of the antenna for R=13mm

The table 4 summarizes the resonant frequencies, the bandwidths and the gains of the antenna in the Bandwidth.

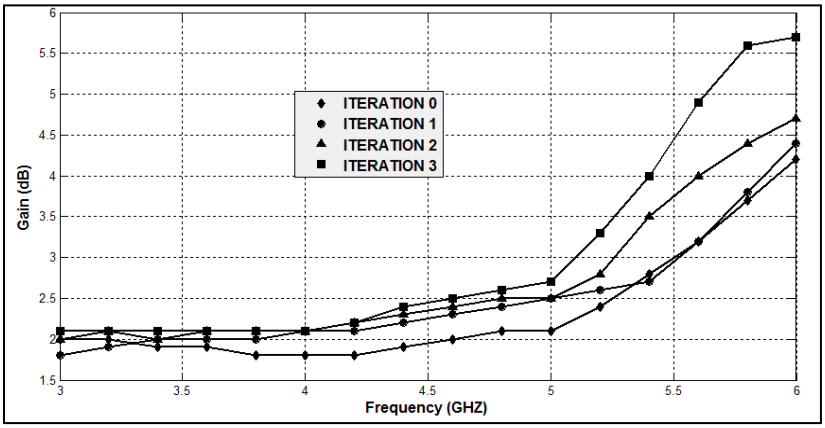
Table 4: the bandwidths and the gains for the antenna (First iteration)

R(mm)	Resonant frequencies (GHz)	Bandwidth (-10dB)	S_{11}* (dB)	Gain (dB)**
12	4 and 5.2 and 7	2GHz (3.49 – 5.49) And 90MHZ (6.96-7.05)	-19 and -16.4 and -18.5	2.1 to 4.4 And 6.4 to 6.2
13	3.9 and 5.08 and 5.92	1.89GHz (3.46 - 5.35) And 190MHz (5.8 – 5.99)	-17.67 and -21.45 and -13.31	2.2 to 5.5 And 5.3 to 4.9
14	5.03 and 5.73	460MHz (4.74 – 5.2) And 200MHz (5.6 – 5.8)	-35.8 and -23.4	3.2 to 5.3 And 4 to 5.3

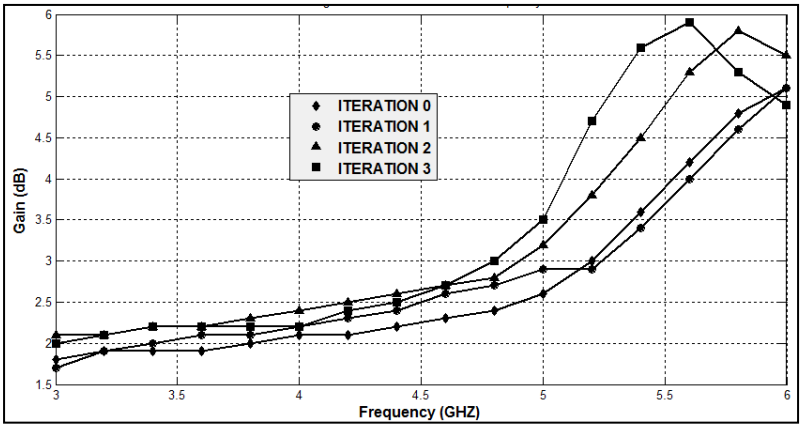
(*) the S_{11} are given in the resonant frequencies
(**) the Gains are given in the bandwidth

3.5 The effect of the iterations

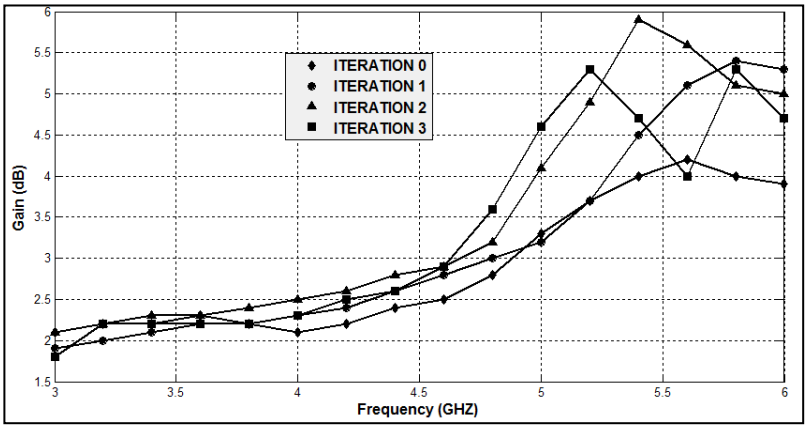
For all the values of the radius R, we observe that in general, the maximum total gain of the antenna increase by increasing the number of iterations (Figure 20). We observe also that in general, the number of the resonant frequencies and the bandwidth increase when the number of iterations increase (figure 21)



(a)R=12mm

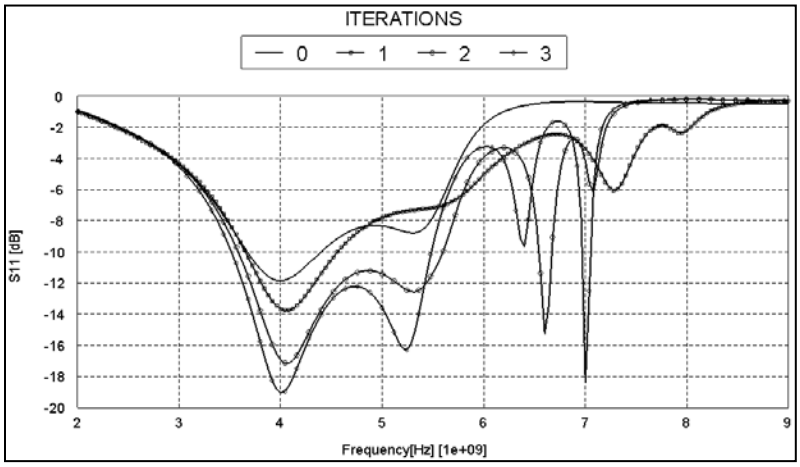


(b)R=13mm

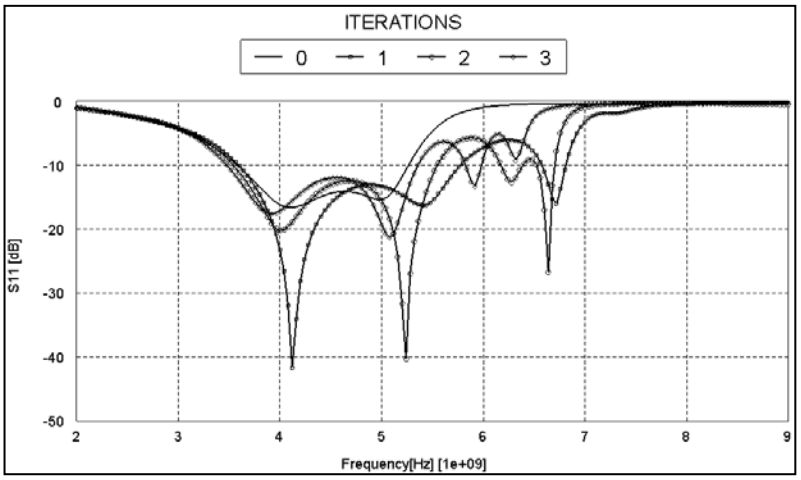


(c)R=14mm

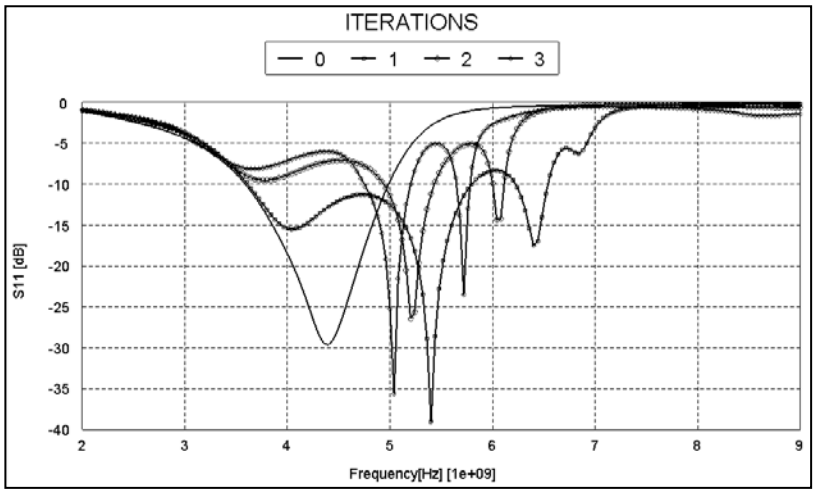
Figure20: Simulated Gain versus frequency graph of the antenna and versus the number of iterations



(a)R=12mm



(b)R=13mm



(c)R=13mm

Figure21: Simulated S_{11} versus frequency graph of the antenna for the 4 iterations

4 Conclusion

The fractal concept is a one of the better solutions to design a simple, low profile and miniaturized antennas, the use of the CPW-Fed technique increases the bandwidth of the antennas and it is very easy to manufacture.

The CPW-Fed KOCH SNOWFLAKE Fractal antenna is a good solution for the UWB applications. Increasing the number of iteration allows obtaining a low profile antenna with good performances, operating for many UWB-applications.

For some configurations of the proposed structures, the antennas are a good solution for the 3.7-4.2GHz C-Band, 5.15-5.82GHz WLAN, and 5GHz WIMAX applications.

Also, further dimensions and iterations can be done to obtain antennas with another sizes, more Ultra Wide Bands and better antenna performances.

REFERENCES

[1]. Aidin Mehdipour, Christopher W. Trueman, Compact Multiband Planar Antenna for 2.4/3.5/5.2/5.8-GHz Wireless Applications, IEEE IEEE Antennas and Wireless Propagation Letters, Vol. 11, 2012, pp 144-147.

[2]. Ming Chen, Chi-Chih Chen, A Compact Dual-Band GPS Antenna Design, IEEE IEEE Antennas and Wireless Propagation Letters, Vol. 12, 2013, pp 245-248.

[3]. Chitra Varadhan, Jayaram Kizhekke Pakkathillam, Malathi Kanagasabai, Ramprabhu Sivasamy, Rajesh Natarajan, and Sandeep Kumar Palaniswamy, Triband Antenna Structures for RFID Systems Deploying Fractal Geometry, IEEE IEEE Antennas and Wireless Propagation Letters, Vol. 12, 2013, pp 437-440

[4]. Cheng Zhou, Guangming Wang, Yawei Wang, Binfeng Zong, and Jing Ma, CPW-Fed Dual-Band Linearly and Circularly Polarized Antenna Employing Novel Composite Right/Left-Handed Transmission-Line, IEEE Antennas and Wireless Propagation Letters, Vol. 12, 2013, pp 1073-1076

[5]. Xu Liqin, Zhong Jin, Wang Chonghua, A Novel Microstrip Antenna with Double Notches, International Conference on Advanced Information Engineering and Education Science (ICAIEES 2013), pp. 44-46

[6]. Moeikham, P , Mahatthanajatuphat, C. ; Akkaraekthalin, P , "A compact ultrawideband monopole antenna with V-shaped slit for 5.5 GHz notched band" , Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2012 9th International Conference on 16-18 May 2012, pp. 1-4

[7]. Raj Kumar, K. K. Sawant, "On the Design of Circular Fractal Antenna with U-Shape Slot in CPW-Feed", Wireless Engineering and Technology, Vol.1 No.2, 2010, pp. 81-87. doi: 10.4236/wet.2010.12012.

[8]. Y. Belhadef and N. Boukli hacene, "Multiband F-PIFA Fractal Antennas for the Mobile Communication Systems", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, March 2012

[9]. Muhammad Naeem Iqbal, Hamood-Ur-Rahman, Syeda Fizzah Jilani, Novel Compact Wide Band Coplanar Waveguide Fed Heptagonal Fractal Monopole Antenna for Wireless Applications, 14th Annual Wireless and Microwave Technology Conference (WAMICON), 2013 IEEE

[10]. Pichet Moeikham, Chatree Mahatthanajatuphat, Prayoot Akkaraekthalin, A compact ultrawideband monopole antenna with V-shaped slit for 5.5 GHz notched band, 9th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2012 IEEE

[11]. Peng Gao and Shuang He, A Compact UWB and Bluetooth Slot Antenna for MIMO/Diversity Applications, ETRI Journal, vol. 36, no. 2, Apr. 2014, pp. 309-312

[12]. Guo-Ping Gao, Bin Hu, and Jin-Sheng Zhang, Design of a Miniaturization Printed Circular-Slot UWB Antenna by the Half-Cutting Method, IEEE Antennas And Wireless Propagation Letters, Vol. 12, 2013, pp 567-570

[13]. Basil K Jeemon, K Shambavi, Zachariah C Alex, "A Multi-fractal Antenna for WLAN and WiMAX Application", 2013 IEEE Conference on Information and Communication Technologies (ICT 2013), pp 953-956

[14]. Shih-Yuan Chen, Po-Hsiang Wang, Powen Hsu, Uniplanar Log-Periodic Slot Antenna Fed by a CPW for UWB Applications, IEEE ANTENNAS AND WIRELESS PROPAGATION LETTERS, VOL. 5, 2006, pp 256-259

[15]. Constantine A. BALANIS, "Antenna Theory : Analysis and design", Third Edition, WILEY, 2006.

[16]. A. Reha and A. Said, "Tri-Band Fractal Antennas for RFID Applications," Wireless Engineering and Technology, Vol. 4 No. 4, 2013, pp. 171-176. doi: 10.4236/wet.2013.44025.

[17]. FEKO 6.3 User's Manual," EM Software & Systems-S. A, October 013, pp.1-1.

[18]. Paul F.Combes, Micro-Ondes 1-Lignes, guides et cavités, DUNOD, 1996

[19]. Shabana Huda, Anirban Karmakar, Rowdra Ghatak , On the Design of Dual Band Notch UWB Antenna and Fractal Slots on the Ground Plane for Bandwidth Enhancement, InternatIonal Journal of electronIcs & communIcatIon technologyVo l.5, Issue spl - 2, Jan-March 2014, pp 50-53.

[20]. J. P. Gianvittorio and Y. Rahmat-Samii, "Fractal Element Antennas: A Compilation of Configurations with Novel Characteristics," 2000 IEEE Antennas and Propagation Society International Symposium, Vol. 3, Salt Lake City, Utah, pp. 1688–1691, July 16–21, 2000.

[21]. J. P. Gianvittorio and Y. Rahmat-Samii, "Fractal Antennas: A Novel Antenna Miniaturization Technique, and Applications," IEEE Antennas Prop

TNC Transactions on Networks and Communications
SOCIETY FOR SCIENCE AND EDUCATION UNITED KINGDOM
VOLUME 2, ISSUE 4
ISSN: 2054 - 7420

Impact of Data-Centre and User-Base Location On Overall Response-Time In A Cloud-Computing Environment

Amina Rashid, Javed Parvez
Department of Computer Science University of Kashmir, Srinagar, India
amina.rashid44@gmail.com; javed_parvez@kashmiruniversity.ac.in

ABSTRACT

Cloud computing is a key component as well as a measure of success for various organizations today. Apart from benefits obtained, it is important to take into account the location of user-base and data-centre, which is essential for performance and security reasons. This information is required since the location of data-centre and user-base can impact the overall response time. In this paper we evaluate the effect on overall response time, of relevant factors such as the location of data-centre and the serviced user-base.

Keywords: Hypervisor, Server Consolidation, Cloud Service Provider (CSP)

1 Introduction

Cloud is essentially a metaphor for the Internet [10].Cloud computing is considered nowadays as a fast growing area in computing research and industry as well. Cloud Computing uses an approach wherein platform, hardware, service are treated as a utility. This utility is metered in cloud computing environment.

Cloud computing is a model, wherein pooling of available shared resources is done. It may mean data centre hosting and understood as utility computing or grid computing [1][2].Cloud computing aims at offering distributed, virtualized and elastic resources as utilities to end users, and has the potential to support full realization of "computing as utility" in near future[14].In cloud computing, there are two important terms data-centre and user-base. Data-centre is used for providing services to the users whose requests are directed to it. User-base can be any organization or a small company, comprising a cluster of users, which gets its requests catered by the data-centre.

In cloud computing, the concept of virtualization technology is used, which enables service providers to run virtual machines and also to share the underlying resources. The software layer which provides virtualization is called hypervisor. Hypervisor emulates the underlying hardware resources with respect to different operating systems. Operating system has the direct access to the underlying hardware. But in case of virtualization, operating systems access

DOI: 10.14738/tnc.24.358
Publication Date: 24th August 2014
URL: http://dx.doi.org/10.14738/tnc.24.358

hardware through hypervisor. The hypervisor executes the privileged instruction on behalf of the virtual machine.

In cloud computing, virtualization technology is used to dynamically allocate or deallocate the resources for an application. Virtualization also helps to co-locate virtual machines to a small number of physical machines, so that the number of active physical machines can be reduced. This approach is called as server consolidation.

1.1 Cloud Computing: Security Concerns

Most of the users of cloud have expectations for the security of their data .The cloud owner and operators have responsibility of ensuring various security measures, and standards and protocols followed appropriately. There are two main aspects of security controls in cloud implementation. First, the presence of control and the second is the effectiveness or robustness of control. Associated with cloud computing are various security concerns. Some of these include:

1. Network Availability: Cloud computing value can be realized only if the network connectivity and bandwidth meet the minimum needs.
2. Cloud Provider Viability: Cloud Providers are relatively new to business and hence there are questions regarding the viability and commitment of the provider.
3. Disaster Recovery and Business Continuity: The users of cloud service require to have confidence that their operations and services will continue even if the cloud providers production environment is subject to disaster.
4. Security Incidents: The users need to be appropriately informed by the provider when an incident occurs. Users may also require provider support to respond to audit or assessment findings
5. Transparency: When a cloud provider does not expose details of their internal policy or technology implementation, the users must trust the cloud provider's security claims.

1.2 Business and IR Perspective

Business organizations are now compelled to deliver IT-enabled services via Internet that are built for end-user to be in control is what is now known as cloud computing. Cloud computing is emerging consumption and delivery model. It enables provisioning of standardized business and computing services through shared infrastructure, wherein end-user controls interaction to accomplish business task. Enterprise resources like processing power, storage, databases are no longer confined to enterprise only. Now, abstract or virtual resources are tapped whenever needed. From computing resources point of view, everything is provisioned by cloud.

2 Cloud Service Provider (CSP)

Business establishments put up a constant pressure on their IT managers for reduced budgets. In current scenario, the need of flexibility and competitive edge are essential requirements for business [8]. Cloud vendors are experiencing growth rates of 50% per annum[11].Such

scenarios lead to the requirement of cost effective and efficient solutions, which are very well provided by cloud computing environment, wherein storage and computing are provided by the infrastructure not owned by the organization. When adopting a public cloud, consumer does not need to be operationally concerned with the details of the underlying cloud infrastructure. However, there are several questions for customers that have to do with security and governance of the cloud service.

Customers of a public cloud service have expectations that the data they put into the service will have integrity and be protected. Customers trust that the CSP will offer the appropriate level of security and governance.

The Cloud Service Provider (CSP) should definitely have the capability to continue the services despite any disaster conditions, if they occur, which may include earthquakes, flood, fire etc. This capability is expected from CSP because the disaster can affect the cloud, and hence recovery measures or plans should be followed periodically and tested. The CSP should also provide a recovery process which in itself should not compromise the security of data.

Cloud Service Providers provide business continuity, recovery, backup through self-healing, but this is not possible to determine with any specificity where data processing takes place within cloud infrastructure [13].

Cloud providers have to safeguard the privacy and security of personal and confidential data that they hold of any organization and users. It is essential for cloud providers to ensure to their users that the security of their data is not compromised.

Hence, various questions and security risks are involved in itself while selecting a cloud service provider, especially while considering the factor of security of data. There are various security-related issues which need to be considered for a cloud service provider, some of the associated concerns are as follows:

1. Policies for Security: Organization which have strict enforcement of security policies, surely give an indication of how seriously the organization is taking the responsibility for security.
2. Independence of Security Staff: Organization maintaining separate staff for security and operations within the organization. Security staff can report independently but need to work in close cooperation to the operations staff.
3. Changes Documented: Any change should be documented well, reviewed and also approved. Change made can be in any aspect but the
4. Authority to make changes and how should be well delineated.
5. Safe Upgrades and also Patch Management: Safe and timely, upgrades and patch management should be done to limit exposure and hence providing security on an on-going basis.

6. Timely Scans: There should be timely scans made to infrastructure and vulnerability assessment should be made. Any issues detected should be evaluated in respect to their potential impact and immediately required corrective steps should be taken.
7. Forensics and Legal Management: To meet forensics and legal requirements any security logs should be maintained long enough. Security logs contribute to knowledge which may provide proper information regarding any breach of security if occurred and hence enabling to understand the scope and its potential impact.
8. Management of Incidents: The customer or a user of cloud should be well aware of any security related incident and the process related to it, hence being transparent to it and the same should also be kept well documented.

Cloud users depend on the providers for the services. These include three types of categories[15]:

I. Cloud Service Provider: Cloud Service Provider, having direct but contractual relationship with the consumer of the service .
II. Cloud infrastructure provider: Provides Cloud Service Provider with some form of infrastructure.
III. Communication Service Provider: Provides transmission service enabling consumer to communicate with Cloud Service Provider.

3 Data Centre Location

Considering the various benefits provided by using cloud computing or cloud service, one tends to forget the importance of the location where data will be stored or in other words the location where cloud is installed. Pooling resources in cloud model allows for greater flexibility and innovation for dynamic business demands [9]:

Traditionally, in a data centre, each application runs in silos, silo is sized for peak load. Here, there is no way to share the capacity between silos, we

need to carry enough capacity for peak workload of every application. Moving to shared or pooled resources will increase utilization rates and carry enough capacity spread across all workloads.

Pooling resources in cloud model allows for greater flexibility and faster innovation for dynamic business demands. If your business is growing fast, has high frequency of new projects, or experiences a sudden spike in demand, we can build new solutions for each of those initiatives much faster without affecting overall performance.

Rise in public computing utilities has led to increased need for better security of the data. Not known to many is the fact that the location of data or the data centre is governed by certain

laws, under whose jurisdiction they fall. The location of the data centre that implements the service utility has both direct and indirect implications. The customer must be aware of the jurisdiction of the nodes that form the cloud fall in.There are certain laws governing the transfer of data, and also what kind of data can be transferred, like what personal data can be collected and where it can be transferred to, even if this transfer is required for backup process.

The main compliance concerns with transborder data flows include whether the laws in the jurisdiction where the data was collected permit the flow, whether those laws continue to apply to the data post-transfer, and whether the laws at the destination present additional risks or benefits [4]. Technical, physical and administrative safeguards, such as access controls, often apply. For example, European data protection laws [5] may impose additional obligations on the handling and processing of European data transferred to the U.S.

The use of cloud computing has increased, this could lead to reduction in demand for high storage capacity consumer end devices, due to cheaper low storage devices that stream all content via cloud is becoming more popular. Jake Gardner explains that unregulated usage is beneficial for IT and tech moguls like Amazon, anonymous nature of cost consumption of cloud usage makes it difficult for business to evaluate and incorporate it into their business plans [12].

4 Simulation Framework, Setup & Result Analysis

Various simulation toolkits have been developed in market that can be very well used for simulating the cloud environment and thereby providing an understanding of large scaled applications floating on internet. Out of the various simulation toolkits available in the market, we are making use of cloud analyst simulation toolkit. This toolkit separates simulation experiments from programming exercise, which in return enables the analyst to dig out on the simulators parameters rather than concentrating on the programming part of it.The graphical output provided by the simulator is one of the key features, highlighting the response time and data processing time for the analyst.

Here we are trying to show that the location of data and data centre does not only affect the security issues and legal issues but also affect the overall response time. In the cloud analyst simulator the world is divided into 6 regions that coincide with the 6 main continents in world. Depending upon the location of data centre the overall response time between the data centre and user base is highly affected, this was established by dividing the entire coverage area into six regions, labelled as R0, R1, R2, R3, R4, R5, respectively.

Six scenarios were created wherein all other aspects of simulation were kept constant which included:

I. Simulation Duration:60 min
II. Service Broker Policy: Closest Data Centre
III. Load balancing policy across VMs in single data centre: Round Robin

IV. Request Grouping factor in UserBase:10
V. Request Grouping factor in DataCentre:10
VI. Executable instruction length per request:100

Using above parameters and changing the location of the user base and keeping the location of data centre as constant 6 scenarios were evaluated as under:

Scenario 1 : Data Centre: Region 0 User Base: Region 0

Overall Response Time:

Average(ms)	Minimum(ms)	Maximum(ms)
50.09	39.55	61.61

Data Centre Processing Time:

Average(ms)	Minimum(ms)	Maximum(ms)
0.48	0.01	0.86

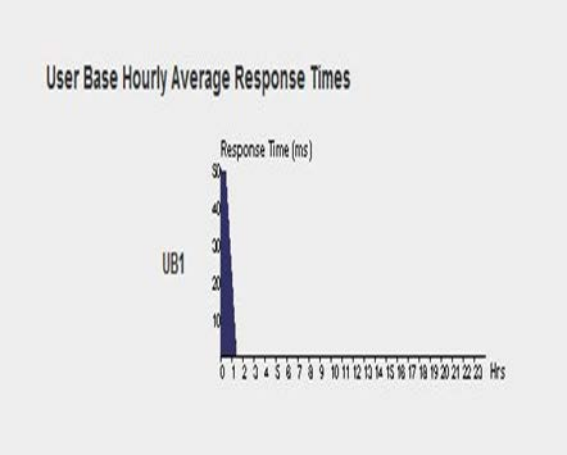


Figure 1: User Base Hourly Average Response Time

Scenario 2 : Data Centre: Region 0 User Base: Region 1

Overall Response Time:

Average(ms)	Minimum(ms)	Maximum(ms)
200.07	158.06	246.12

Data Centre Processing Time

Average(ms)	Minimum(ms)	Maximum(ms)
0.10	0.02	0.11

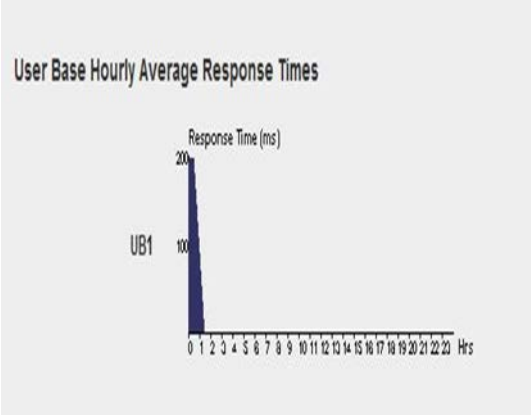


Figure 2: User Base Hourly Average Response Time

Scenario 3 : Data Centre: Region 0 User Base: Region 2

Overall Response Time:

Average(ms)	Minimum(ms)	Maximum(ms)
300.06	237.06	369.12

Data Centre Processing Time

Average(ms)	Minimum(ms)	Maximum(ms)
0.34	0.02	0.61

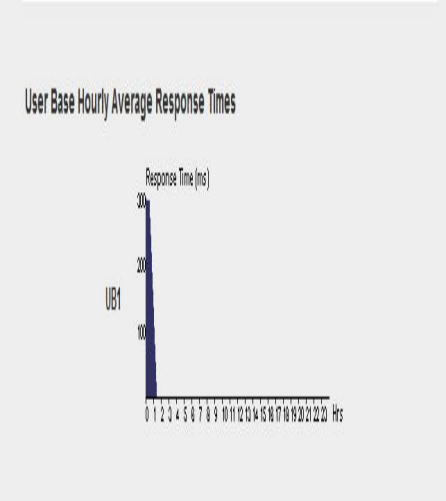


Figure 3: User Base Hourly Average Response Time

Scenario 4 : Data Centre: Region 0 User Base: Region 3

Overall Response Time:

Average(ms)	Minimum(ms)	Maximum(ms)
500.02	395.06	615.12

Data Centre Processing Time

Average(ms)	Minimum(ms)	Maximum(ms)
0.34	0.02	0.61

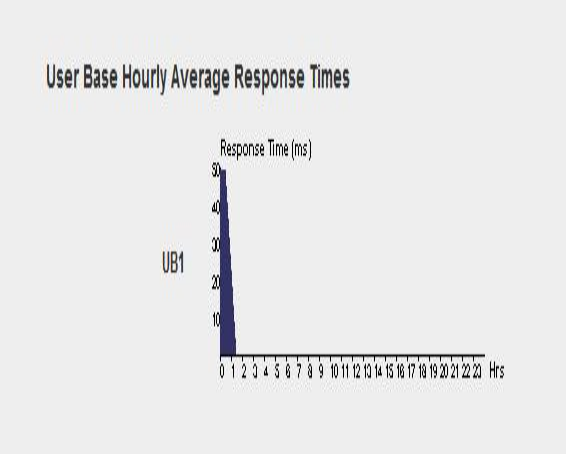


Figure 4: User Base Hourly Average Response Time

Scenario 5 : Data Centre: Region 0 User Base: Region 4

Overall Response Time:

Average(ms)	Minimum(ms)	Maximum(ms)
500.02	395.06	615.12

Data Centre Processing Time

Average(ms)	Minimum(ms)	Maximum(ms)
0.34	0.02	0.61

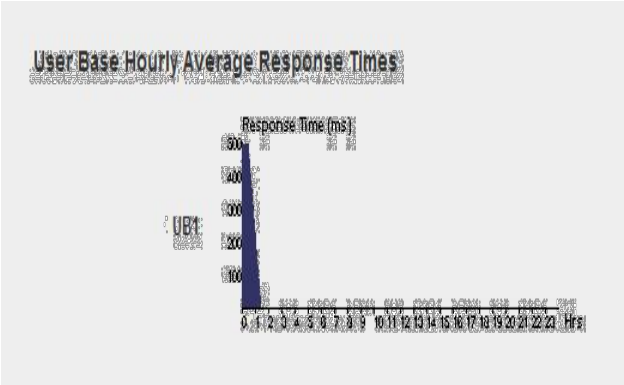


Figure 5: User Base Hourly Average Response Time

Scenario 6 : Data Centre: Region 0 User Base: Region 6

Overall Response Time:

Average(ms)	Minimum(ms)	Maximum(ms)
200.07	158.06	246.12

Data Centre Processing Time

Average(ms)	Minimum(ms)	Maximum(ms)
0.10	0.02	0.11

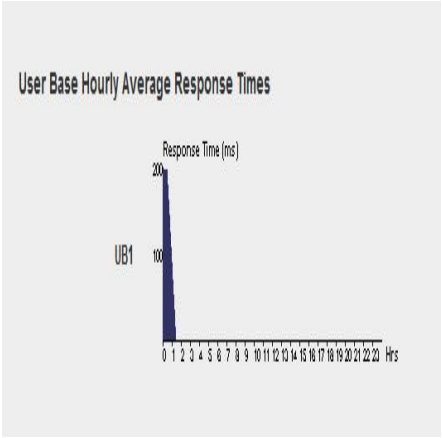


Figure 6: User Base Hourly Average Response Time

From the above scenarios we can easily confer that if the data centre and the user base are in the same region the overall response time calculated at average is very low and goes on increasing as the location of user base is altered, whileas the location of data centre is kept same, which was previously set to region 0 i.e. R0.

Also from the above scenarios it can be easily viewed that the overall response calculated for the regions R1 and R5 is same and so are their data processing time. Similarly, the overall response time calculated for regions R3 and R4 are same and so are their processing times. The overall response time calculated for region R0 is far less compared to any other region in which

user base calculated, hence confirming that if the region of the data centre and user base is same then the response time is far less. Similarly, the overall response times of regions R0 and R2 are entirely different from other regions and do not match to other regions. The data centre processing time calculated for region R0 is entirely different, whileas the data centre processing times calculated for regions R2, R3 and R4 are same.

5 Conclusion

At various instances cloud computing is advocated as providing infinite capacity on demand, but the real part of it is that the capacity of data centres in real world is finite[6].Installing and setting up data centre is not an easy task, it involves various sensitive issues like political and legal issues. Cloud computing is a popular paradigm now-a-days, wherein cloud providers offer scalable resources over Internet. Various providers like Amazons EC2, Google's AppEngine, IBM's Blue Cloud, and Microsoft's Azure provide services to the customers which include primarily storage and computing [7]. From the above scenarios we can well comprehend that there are some regions which have same overall response time, whileas some other regions have less overall response time compared to other. Now depending upon the allowance in a particular region, the cloud service provider can be allowed or rejected to set up a data centre in that region. This in return can affect the performance provided by the cloud service provider in respect of overall response as seen in above scenarios. Also it can lead to an additional charge to the customer if the data centre it is accessing does not fall in the region in its specified jurisdiction.Cloud computing is considered to be in its initial stages,lot more needs to be explored in this area.Various issues are yet to be solved,some of which include the audit.

REFERENCES

[1]. Lijun Mei,W.K.Chan,T.H.Tse,"A Tale of Clouds: Parad igm Comparisons and Some Thoughts on Research Issues",I EEE Asia-Pacific Services Computing Conference,2008

[2]. Thomas B Winans,JohnSeely Brown, "Cloud Computing, A Collection of working papers",2009.

[3]. http://technet.microsoft.com/en-us/magazine/hh536219.aspx

[4]. Amina Rashid,JavedParvez,"Security Issues in Cloud Computing:An Overview"

[5]. http://ec.europa.eu/j ustice/ data -protection/index_en .html.

[6]. Zhen Xiao,Qi Chen, Haipeng Luo," Automatic Scaling of Internet Applications for Cloud Computing Services".

[7]. Haiying Shen*, Guoxin Liu," An Efficient and Trust worthy Resource Sharing Platform for Collaborative Cloud Computing" .

[8]. http://viewer.media.bitpipe.com/1078177630_947/1267474882_422/WP_DC_DataCenterCloudComputing1.pdf.

[9]. http://www.oracle.com/us/products/database/cloud-computing-guide-1561727.pdf.

[10]. http://www.netlingo.com/word/cloud-computing.php.

[11]. http://www.fsn.co.uk/channel_outsourcing/the_economy_is_flat_so_why_are_financials_cloud_vendors_growing_at_more_than_90_perce nt_per_annum#.UbmtsPlJPGA/

[12]. http://www.wired.com/2013/01/beware-7-sins-of-cloud-computing.

[13]. McKinley,P.K.,Samimi,F.A.,Shapiro,J.K.,Chipping,T.:Service clouds:a distributed infrastructure for constructing autonomic communication services,In : Dependable,Autonomic and Secure Computing,IEEE,12-14 Dec 2011,Sydney,Australia,341-348(2006)

TNC Transactions on Networks and Communications
SOCIETY FOR SCIENCE AND EDUCATION UNITED KINGDOM
VOLUME 2, ISSUE 4
ISSN: 2054 - 7420

Adaptable mobile user interface for securing e-learning environment

Mohanned A. aljbori, Shawkat K. Guirguis, Magda M. Madbouly
Department of Information Technology, Institute of Graduate Studies & Research, Alexandria University, Alexandria, Egypt
mohannedta@yahoo.com, Shawkat_g@yahoo.com, mmadbouly@hotmail.com

ABSTRACT

E-Learning is a pedagogy empowered by Information and Communication technologies supporting education/training. While e-Learning exists over the past decade and a half, it is do not receiving considerable attention only in the recent times. Both Industry and Academia are heavily depending on e-Learning in streamlining their teaching process, and also E-learning has provided us with the capability of providing quality education to masses without restricting them to specific time or place, So that E-Learning become the most used and popular teaching method in universities with availability of E-learning tools and techniques, development of technology communications and networks. We can say that distance education's popularity is increasing day by day and has become one of the most preferred methods for obtaining information. And it provides great facilities in many aspects according to traditional education. One of the most effective parameters in Electronic Learning or E-Learning systems' success is the security of these systems. But this feature is ignored in the most of cases. An E-Learning system has different user groups such as authors, teachers and students. Each of these groups has special and unique security requirements. In this paper we will work on secure e-learning environment against unauthorized access through design a system for securing and control access to e-learning environment in distance learning institutions by adaptable mobile user interface associated with the token code generator Technology for learners who use mobile devices to access educational content.

Keywords: E-learning, Mobile learning, E-learning problem, E-learning challenges, Adaptive Mobile user interface.

1 Introduction

Nowadays, e-learning system has becomes popular among the educational institutions. This is because E-learning system gives a lot of benefits to people such as guaranteed 24-hour response to student questions, education taking place anytime, anywhere and searchable

DOI: 10.14738/tnc.24.360
Publication Date: 24th August 2014
URL: http://dx.doi.org/10.14738/tnc.24.360

knowledge base. E-Learning is also quite effective in its ability to produce measurable results by monitoring attendance, effectiveness, performance, and recording test scores [R34], Researchers and Educators have been proposing lots of innovative designs for the development of E-Learning environments. The focus of these designs is to improve the quality of learning and provide personalization and convenience to users. Every researcher, educator believes that there should be major difference between the conventional learning and E-Learning [R35].

One of the major constraints of mobile learning is difficult to develop learning environment for mobile users, since we can't use mobile devices in the same way, we use desktop computers. Mobile devices have distinct capabilities, such as limited computing powers and small size screens. On other hand, mobile devices differ from each other by their hardware and software capabilities like computing power (processor power, memory size), screen size and resolution, operating system, web browser, script languages, file formats, etc. A number of aspects need to be dealt with before the true Potential of m-learning environment can be exploited. Some of these aspects include development of interface compatible to all kind of mobile devices [R36], Trust relationships among learners are important for collaboration activities in e-learning environments. A trust relationship may need to be developed between two unknown learners who find them working together. The meaning of trust differs from one context to another [R37]; the new strategies will reshape the role of education and create enduring advantages for both students and universities. Digital information sent from the organizers to students or agents may not be further disseminated with some commercial reasons. Therefore unauthorized dissemination of digital content has emerged as one of the most problematic and challenging issues in information security on E-Learning [R38].

E-learning can be defined as technology-based learning in which learning material is delivered electronically to remote learners via a computer network. E-learning (or Internet-based learning) could be seen as a professional level of education but with the advantages of lower time and cost. Some other advantages of e-learning include larger learner population, shortage of qualified training staff and lower cost of campus maintenance, up-to-date information and accessibility. In a typical e-learning environment the lecturers, students and information are in different geographical locations (as depicted in Figure 2) and are connected via the Internet [R33] [R32] [R39] [R40] [R41] [R54] [R47] [R48] [R49] [R50] [R51].

There are six technical countermeasures that should be adhered to when implementing information security within any education environment. Implementing these countermeasures will help to ensure that lecturers and students as well as data (such as student marks and financial information) are properly protected against possible security incidents. These information security countermeasures are (Identification and Authentication, Authorization, Confidentiality, Integrity, Non-Repudiation, Availability) [R39] [R33] [R40] [R41] [R42] [R43] [R44] [R45] [R46] [R47] [R50] [R51].

Adaptive User Interfaces (AUIs) can provide potential benefits for addressing usability issues. Adaptation of the UI has been identified as an important aspect to be considered in the design of modern information systems. Adaptation techniques include adapting what information to present (information adaptation), how to present this information (presentation adaptation) and how to interact with this information (interface adaptation) [R53] [R52].

2 Related Work

The security Solution for E-learning Applications by using Open ID: [R10] is one of the works related to this section, this paper presents the main characteristics of Open ID standard and how this standard could be implemented for a distributed, Web-based, e-learning application, And another work by Huping Wang, Chunxiao Fan, Shuai Yang, Junwei Zou, Xiaoying in [R11] presented and describes a framework to enhance the security of OpenID with One-Time Password (OTP), In [R16] by Yu-Lin Jeng, The proposed architecture in this paper emphasizes the advantage of OpenID deployed in a decentralized environment composed of system nodes.

Secure multi agent e-Learning Applications: The related work in this section is [R2] by Carine G. Webber, Maria de Fátima W.P.Lima, Marcos E.Casa, Alexandre M.Ribeiro, in this paper presents some results in the intersection of three technological fields: e-learning, multi agent systems (MAS), and standards to improve the development of secure systems, And another work in [R19] by Shantha Visalakshi. U et al, Author Presented in this paper, proposed architecture with an enhanced security agent along with the other agents of the system, By Sadaf Ahmad, Mohammad Ubaidullah Bokhari in [R23] , proposed a new architecture for Multi agent based system for e-learning environment wherein in addition to these basic feature, the focus is interactivity and eases of use, The study presented by Umit Kocabicak Deniz Dural in [R5] it based the combining different e-learning systems that is necessary for distance education. And then, a solution is proposed to find about the security problems that occur while combining these systems, with XML web services.

Security in E-Learning system: The related work in this section is [R3] by El-Khatib, K., Korba, L., Xu, Y., and Yee, G., in this paper examines privacy and security issues associated with e-learning, Another related work presented by Jianming Yong in [R4] it proposes to use the alias and anonymity to implement the privacy preservation for e-learning systems, In addition, the work presented by Shadi R Masadeh, Nedal Turab, Farhan Obisat in [R9], in this article, he proposing a model for a secure e-learning system designed to be implemented by computer centers at universities.

Security mobile learning: The related work in this section presented by Jianming Yong in [R6], this paper systematically discusses the security and privacy concerns for e-learning systems. Five-layer architecture of e-learning system is proposed, Another related work by Ivica Boticki, Natasa Hoic-Bozic and Ivan Budiscak in [R7], This article presents a system called MILE and its

extensible context-aware architecture which supports the use of mobile devices in blended learning environments.

Secure e-learning systems: The related work in this section presented by Jorge Fontenla Gonza´ lez, Manuel Caeiro Rodrı´guez, Martı´n Llamas Nistal, Luis Anido Rifon. In this paper introduce Reverse OAuth – a protocol to enable the granting of authorization to access protected resources in educational environments [R8].

Secure e-contents system for multimedia interchanges: The related workin this section in [R12] by Shadi R. Masadeh, Bilal Abul-Huda andNidal M. Turab. The main objective of this research is to build a novel multi-media security system (encrypting / decrypting system) that will enable E-learning to exchange more secured multi-media data/information.

Secure distributed e-learning and m-learning environments: The related work in this section presented by Georgios Kambourakis, Denise-Penelope N. Kontoni, Angelos Rouskas, Stefanos Gritzalis in [R13]. This paper discusses the potential application of ACs in a proposed trust model, And another related work it [R21] presented by Amjad Mahfouth. In this paper he proposes authentication techniques between universities in Avicenna Virtual Campus Project in Euro Mid Infrastructure Network.

Author's Security in Electronic Learning: The related work in this section presented by Ali Naserasadi in [R1]. In this paper, Ali NaserAsadi has distinguished security importance in E-Learning systems from authors' point of view, investigated security requirements and the manner of authors' security risk analysis. Also, he suggested some approaches for educational content protection.

Securing an e-Learning Ecosystem: The related work in this section represented in [R14] presented by P.R.Lakshmi Eswari. Through this paper, various security & privacy risks associated with e-Learning are enumerated and a process framework is proposed for securing an e-Learning Ecosystem, which helps to address the security problem in a systematic way in order to foster the benefits of e-Learning.

Secure Collaborative Multimedia Learning: The related work in this section presented by Anastasia Balia, Dimitrios Koukopoulos in [R15]. In this work, present an online collaborative learning environment where the instructors insert learning material that the learners can view. User and course material classification aims at supporting distance learning scenarios that cover the needs of various user groups such as art classes, teachers and students. This learning material is essentially multimedia cultural content, distributed via the Internet and so it must be protected against any misuse, and another related work it [R20] this paper presented by Dimitrios K. Koukopoulos, Georgios D. Styliaras. This paper proposes a web-based system for organizing the creation and the interaction in multimedia web-based environments that permit the collaboration among artists, audience, curators and publishers.

Secure of Open Source Software by using Digital Signature: The related wok in this section represented in [R17] by M. Tariq Banday. This paper discusses methods for attaining authentication and integrity of Open Source Software for the purpose of its distribution.

Secure ICT environment for educational systems: The related work in this section [R18] presented by Yu-Hsiu Chuang • Chi-Yuan Chen • Tzong-ChenWu. Han-Chieh Chao. In this paper, investigate current situation of Taiwan Ministry of Education ICT security development and provide a case study. Also discussed challenges and solutions for improving ICT security environment in educational system.

WiMAX Security Issues in E-learning Systems, The related work in this section [R22] presented by Felician ALECU, Paul POCATILU, Sergiu CAPISIZU, in this paper They discussed the use of WiMAX Security Issues in E-learning Systems, the WiMAX (Worldwide Interoperability for Microwave Access) is a point-to-multipoint wireless network based on IEEE 802.16 standard. Tha WiMAX signal is broadcasted from a base station to the wide-geographically spread receivers. WiMAX enabled mobile devices [R22].

3 Proposed Methodology

3.1 Characteristics of Proposed System

Proposed our system provide access control capabilities, i.e., user authentication and authorization of user actions, as well as confidentiality and integrity of communication, Authentication is the confirmation of a principal identity with a specified or understood level of confidence. Authorization is the process of determining whether the particular entity has the right to perform some action on some resource. Authentication and authorization are the main elements of access control, which provides protection of resources against unauthorized access. Confidentiality and integrity of data transmitted over the network. Through adaptable mobile user interface associated with the token code generator Technology for learners who use mobile devices to access educational content, Fig 3.1: Shows the proposed System architecture to secure e-learning environment.

3.2 The Potential problems

In this section, will explain the potential problems that facing of mobile users, and the most important hacking cases that may be exposed to mobile users, and proposed solution for this cases:

3.2.1 Losing device:

Is one of the common problems experienced by users of mobile, In this case, the intruding on the device and try to use the real user data to access the e-learning environment, so we proposed solutions to solve this problem, First, the real user must be, logon to the e-learning environment of another device in the fastest time, This process leads to automatic logout process for the losing device, Through this process we were able to cut the way for hackers to

access e-learning environment, But in the other case, if the intruder was able to access the e-learning environment Before enabling real user of a logon to the e-learning environment from another device, In this case we worked on making mobile user interfaces have the ability to adapt with the role of the client, This procedure gives us the possibility of a scalable process intruding on the e-learning environment to less space as possible and not to leave full freedom to the intruder for movement within e-learning environment.

3.2.2 Network Monitoring:

Is one of the methods used by the hacker to get a user name and password for the real user, Our solution proposed to this problem is to make the process of using username and password for the real user only once, During login for the first time only, Therefore, the access to username and password in this case are almost impossible, Even if it were to get username and password for the real user, In this case it cannot login from another device because it requires sending additional information about the real user to the server-side, Here we close the road in front of hacker again in the process of hacking the e-learning environment by this method.

3.2.3 Mobile client hacking:

This method is most commonly used by the hacker to access into the database record For the Pirate device, In the hope of getting username and password for the real user, Or trying to decode the token code to getting the username and password through which, So it was our proposal to solve this problem is to work on make the process of generating token code based on (unique device ID, current time), So we cannot use the same token code by another device, As for the decode the token code to getting a username and password from through it, So we worked on making this task impossible by making token code encrypted by one way (Hashing), and trying to get a username and password real user through the mobile client data hacking Will be a failed, Because username and password are not stored within the mobile client database record, but they are stored on the server Side only, Therefore cannot be accessed in this way and so we In this case were able to stop the hacker access into e-learning environment again.

3.2.4 The proposed technical to solve the problem:

Adaptable mobile user interfaces with the role of the mobile client and integration with Token Code technology that depend on the idea of reduce the number of times you send your username and password to the server. Therefore the Idea proposal is to generating user interface appropriate with the role of the client and the type of content requested, and sending requests to the learning service. Means responsible for generating user interfaces for applications, adapted to a particular user, the currently used access device and the current context, and Generate token code sent to the server as an alternative for the username and password. The idea briefly is: send the username and password to the server only once (i.e. in the login process the first time), During this process the token code is generated based on the

unique device ID, User ID, username, password and current time, then the token code is sent to the mobile client to be stored as a database record, then each time you request electronic content it will be sent by the token code without username and password.

3.3 System components

3.3.1 Mobile client

Also called mobile apps, it is a term used to describe Internet applications that run on smartphones and other mobile devices. Mobile applications usually help users by connecting them to Internet services more commonly accessed on desktop or notebook computers, or help them by making it easier to use the Internet on their portable devices. Basic idea behind the Client Framework is to provide services to client applications. In addition to that, its important function is the manifestation of distributed events as .NET events on the client side [R7]. Such as operating systems and browsers act as the primary client software that is using application programs of smart phones. The browsers of smart phones are used to access data in the mobile learning system server. And JavaScript to communicate between user requests and server results [R26].

3.3.2 API (web service)

APIs (Application Program Interface) in order to use the available web services. Learning resources retrieved from the web consist of text, pictures, and videos. APIs are not standard [R24]. A mediator between The Mobile Client (MC) and the Security Manager (SM), it creates a session for MC and exchanges data with the Identity Provider (IP), token code repository (TCR), UI generator, and e-learning service.

3.3.3 Identity provider (validator):

It is home institution of the User within the federation. The Identity Provider that encapsulates information about the User (e.g. authentication, profile attributes) and sends them to the Service Provider [R8]. In other words, is responsible for the registration of new users, checking the name and password of the previously registered users, and determines the role of the client.

3.3.4 User repository:

Database stores information about system's legitimate users [R15].

3.3.5 Role repository:

It's responsible for storing the user's role [R31].

3.3.6 UI generator:

It's responsible for generating user interface appropriate with the role of the client and the type of content requested, and sending requests to the learning service. Means responsible for

generating user interfaces for applications, adapted to a particular user, the currently used access device and the current context [R27] [R28].

3.3.7 Token code generation:

it's Responsible for generating the token code For each client after the login process and it is stored in the token code repository, this code is sent to the client, Through which the client can have access to the educational content, Each client keeps his own code, which is the second phase of the authentication process to access educational content. Do not change this code unless it is through a request from the client after each new login process from the same device or another one and can be changed after it expires which is determined in previously, but after the client is notified and has agreed to changing the code.

3.3.8 Token code repository:

it's responsible for the storage token Code for each Existing user and the new ones.

3.3.9 Learning service:

It provides the possibility to host the digital educational resources, which can be accessed by the lecturer and all students either locally, or throughout the Internet. Additionally, all students, as well as the lecturer over the Internet can access the Server Platform to collect, or download the data that needs to be computed in an e-learning environment [R25]. The System database stores the basic information of students and teachers. It further contains the processing information of students learning and faculty member's teaching. The learning resource database consists of mobile learning courseware, electronic lesson plans, e-books, dictionaries and other mobile learning software [R26]. Briefly responsible for the educational content storage, this is an essential component in each e-Learning System.

3.3.10 JavaScript Object Notation (JSON):

It is an open standard format that uses human-readable text to transmit data objects consisting of attribute–value pairs. It is used primarily to transmit data between a server and web application, as an alternative to XML. Although originally derived from the JavaScript scripting language, JSON is a language-independent data format, and code for parsing and generating JSON data is readily available in a large variety of programming languages. Is designed to be a data exchange language which is human readable and easy for computers to parse and use. JSON is directly supported inside JavaScript and is best suited for JavaScript applications; thus providing significant performance gains over XML, which requires extra libraries to retrieve data from Document Object Model (DOM) objects [R29] [R30].

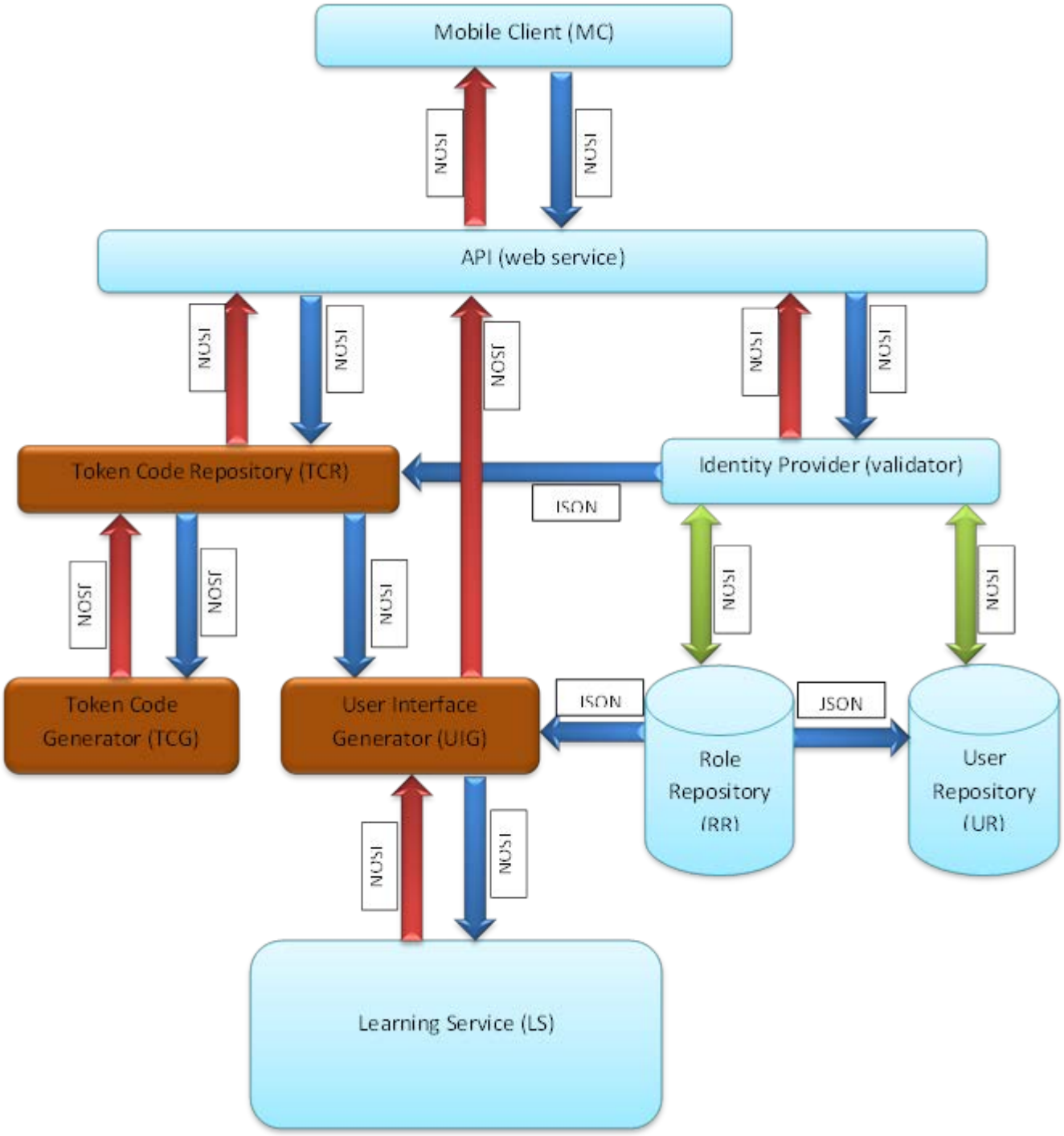


Figure 1: The proposed System architecture to secure e-learning environment

3.4 Data flow in system architecture:

There are three scenarios for the data flow in the system; the first scenario begins the process of recording data of the user who wishes to register in the system. The second scenarios are the process login to the system by the user for the first time and request the electronic content. And ending system processes by the third scenario Special Process of electronic content

request through the proposed technology for the protection of educational content in which it operates technology adaptable mobile user interfaces Enhanced by token Code technology. These three scenarios will be explained below.

3.4.1 The registration request case:

1. Mobile client (MC) sends the registration request to the (API).
2. The (API) send the registration request to the identity provider (validator).
3. The (validator) verification of registration information, If information previously registered then returns an error message in the registration process, If the information is not previously registered then complete the registration process by store the user information in user repository (UR) and role repository (RR) and return message to complete this process.

3.4.2 The Login and educational content request case:

1. Mobile client (MC) sends Login and learning service request to the (API).
2. The (API) send request to the (validator).
3. The (validator) Verifies the customer's identity by check information in (UR) and (RR), If the client is not registered, then Return the message refuse to accept login request, If the client is registered, then request is accepted and send a request to token code repository(TCR) for verification of the token code.
4. (TCR) Verifies from the token code, if it was token code for this client, then going directly to the Seventh step, if it was not token code for this client, then (TCR) send request to the token code generator (TCG) to generate token code.
5. The (TCG) generate token code and send it to (TCR).
6. The (TCR) store the token code and sent it to the (API) and the (API) send the token code to the (MC), In addition, the (TCR) send a request to user interface generator (UIG) to generate user interface.
7. The (UIG) generate user interface fit with the role of the client and the type of content requested, and send request to learning service (LS) for the purpose of sending educational content.
8. The (LS) send educational content to the (UIG).
9. The (UIG) send user interface and educational content to the (API).
10. The (API) send this content to the (MC).

3.4.3 The educational content request by adaptive mobile user interface and token code case:

1. The (MC) send educational content request by the token code to the (API).
2. The (API) send this request to the (TCR).

3. The (TCR) Verifies from the token code, if the token code was not correct then Return refused for accept the request message, if the token code was correct then (TCR) send educational content request to the (UIG).
4. The (UIG) generate user interface was fit with the role of the client and the type of content requested, and send request to learning service (LS) for the purpose of sending educational content.
5. The (LS) send educational content to the (UIG).
6. The (UIG) send user interface and educational content to the (API).
7. The (API) send this content to the (MC).

4 Experiments and Results

4.1 Research Material

4.1.1 Used tools:

The proposed system described in chapter 3 has been tested by using (Advanced REST client for Google Chrome) this tool it web developer's helper program to create and test custom HTTP requests. Have many advantages, but will mention some of the features that concerns us in our research (Integrated with Google Drive, Debug socket (via web socket API), JSON response viewer, XML response viewer, In addition, we used (Bulk URL Opener Extension): This tool used in Open multiple URLs at once; Bulk URL Opener Extension just lets our open multiple URLs at once (in new tabs or windows) And we used HashKiller.co.uk allows you to input an MD5 hash and search for its decrypted state in our database, basically, it's a MD5 cracker / decryption tool.

4.1.2 Used Device:

The algorithm, presented in this thesis, is implemented with a laptop HP model with the following specifications of Intel Core i7 3612QM 2.1 GHz with 4GB RAM, Video Graphics ,ATI HD 7670 Video Memory 1GB of Turbo-Cache™ video Memory including 3021 MB dedicated video memory and Display 15.6 LED High Definition Bright View Widescreen (1366 x 768). This machine is equipped with operating system Windows 7 Home Basic.

4.1.3 Used Software:

The proposed image watermarking scheme has been implemented using Firstly, JavaScript (JS): is a dynamic computer programming language. It is most commonly used as part of web browsers, whose implementations allow client-side scripts to interact with the user, control the browser, communicate asynchronously, and alter the document content that is displayed. It is also being used in server-side programming, game development and the creation of desktop and mobile applications, Secondly, PHP: is a server-side scripting language designed for web development but also used as a general-purpose programming language. Originally created by (Rasmus Lerdorf) in 1995, the reference implementation of PHP is now produced by The PHP Group. PHP code is interpreted by a web server with a PHP processor module, which generates

the resulting web page: PHP commands can be embedded directly into an HTML source document rather than calling an external file to process data. It has also evolved to include a command-line interface capability and can be used in standalone graphical applications, Thirdly, JSON or JavaScript Object Notation: is an open standard formatting that uses human-readable text to transmit data objects consisting of attribute–value pairs. It is used primarily to transmit data between a server and web application, as an alternative to XML.

4.2 Research Results:

4.2.1 First experiment:

In the first experiment, (Results illustrate the differences between JSON and XML encoding under varying transmission scenarios. This section presents the metrics obtained for the average measurements, compares the metrics of transmitting high versus low number of encoded objects, and determines whether JSON and XML are statistically different for each of our measurements. We present both scenarios' measurements and discuss their implications) [R29] in this Scenario is a time-consuming transmission of a large quantity of objects. Large numbers of objects are used in order to achieve accurate average measurements. The client sends one million encoded objects to the server for both JSON and XML. We measure timing and resource utilizations. Table 1 and table 2 list the measurements and respective values obtained from this trial [R29].

Table 1: JSON vs. XML Timing [R29]

	JSON	XML
Number Of Objects	1000000	1000000
Total Time (ms)	78257.9	4546694.78
Average Time (ms)	0.08	4.55

Table 2: JSON vs. XML CPU/Memory [R29]

	Average % User CPU Utilization	Average % System CPU Utilization	Average % Memory Utilization
JSON	86.13	13.08	27.37
XML	54.59	45.41	29.69

4.2.2 Second experiment:

In this test, we compared the difference results between the processes of login to e-learning environment from client side to server side, By using the token code once and by (user name, password) again, We did this test in the case of synchronization login to e-learning environment, We used the number of samples begin ten login process and then gradually increasing to sixty login process and we got the results shown in the table 3 and Figure 2.

Table 3: Different login time by using token code & (username and password)

number of login process	Average login time by token cod (MS)	Average login time by username & password (MS)
10	9.85	26.2
20	11.3	28.34
30	13.7	30.17
40	15.65	32.45
50	17.23	34.66

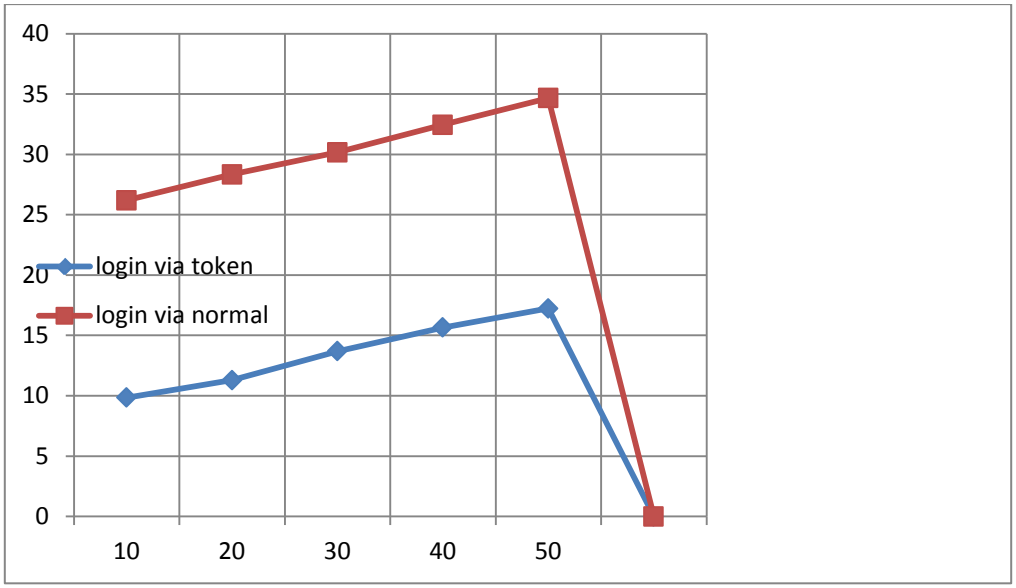


Figure 2: different login time by using token code & (username and password)

4.2.3 Third excrement:

In this test, we compared the difference results between the processes of getting the e-learning content from client side to server side, By using the token code once and by (user name, password) again, We did this test in the case of synchronization to get the e-learning content, We used the number of samples begin ten users and then gradually increasing to sixty user and we got the results shown in the table 4 and Figure 3.

Table 4: different result to getting e-learning content by using token code & (username and password) in synchronization case

synchronization		
No. of users	Average Getting time via token by (S)	Average Getting time via normal(S)
10	0.66	0.74
20	1.15	1.39
30	2.25	2.71
40	3.2	3.37
50	4.36	4.81
60	5.4	5.86

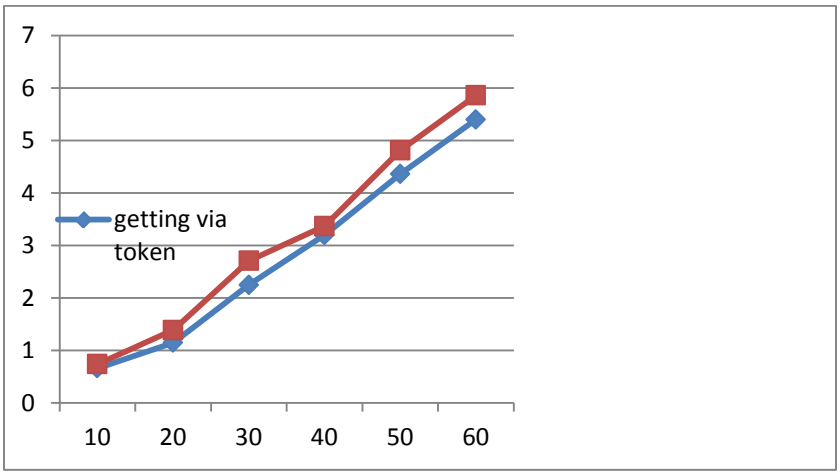


Figure 3: different result to getting e-learning content by using token code & (username and password) in synchronization case

4.2.4 Fourth experiment:

In this test, we compared the difference results between the processes of getting the e-learning content from server side to client side, By using the token code once and by user name and password again, We did this test in the case of (A synchronization) to get the e-learning content, We used in our test this ten users asynchronously where are not dealing with the second user until the completion of the first user, as well as order until the completion of all subscribed users and we got the results shown in the table 5 and Figure 4.

Table 5: different result to getting e-learning content by using token code & (username and password) in (A synchronization) case

A synchronization		
No. of users	Getting time via token by(MS)	Getting time via normal(MS)
1	17.44	21.14
2	17.56	21.27
3	17.61	22.85
4	19.15	23.45
5	19.23	23.92
6	20.36	24.26
7	20.42	24.78
8	21.17	25.11
10	21.28	25.65

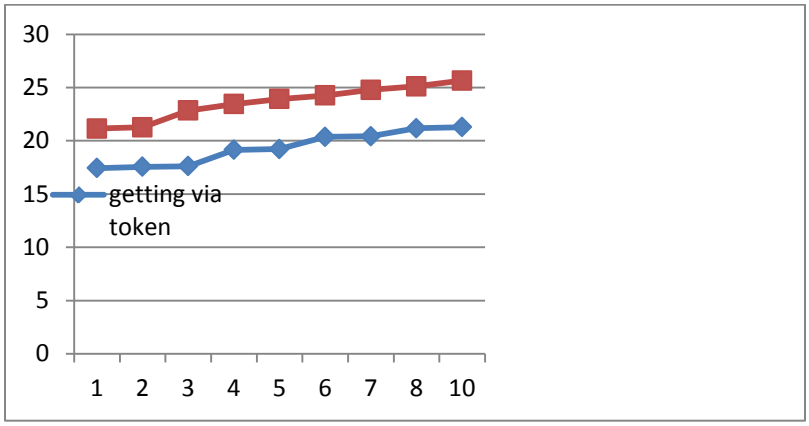


Figure 4: different result to getting e-learning content by using token code & (username and password) in (Asynchronization) case

4.2.5 Other experiment:

In this experimentation, we put summary table shows the proposed solutions to the problems faced by mobile users secure environment for e-learning and the results of these solutions.

Table 6: Potential problems, solution and the results

Cases	Potential problems	Proposed solutions	Expected Results
Device losing	1. Try the hacker to access e-learning environment by user's data.	1. Must the user to make logout from another device as soon time possible. 2. Adaptable mobile user interface based on the user role, this solution is activated if not to use the first solution.	1. Make automatic logout from losing device. 2. Restrict the hacker in user e-learning area, and not a legacy to roam freely entered the e-learning environment.
Network monitoring	1. Trying getting username & password.	1. User name and password are sent from client side to server side only once time, during login for the first time only.	1. Hacker not or need to large luck to get the data it sent only once time across the network. 2. Cannot login from another device by same user name and password, if the primary device is connected.
Mobile client hacking	1. Trying to hacking token code. 2. Trying decoding the token code to getting username & password. 3. Trying to hacking username & password.	1. The code generation process token based on (unique ID device & current time), each device has a special token code. 2. After token code generating process is encrypted by one way method (hashing). 3. Do not store user name and password on the mobile client; it is stored on the server Side.	1. Cannot access to e-learning environment from another device by same token code. 2. Cannot decode the token code and therefore cannot get username & password. 3. Cannot login from another device by same user name and password even if the primary device in disconnected case, because that it requires additional information by the real user.

5 Conclusion and future work

In our research we have proposed new method To protect e-learning environment, Through the use of adaptable mobile user interfaces and Token Code technology, We used this method rather than of traditional method which is based on (User name & password) to get the electronic content from e-learning environment, A summary of our proposal based on: Adaptable mobile user interfaces with the role of the mobile client and integration with Token Code technology that depend on the idea of reduce the number of times you send your username and password to the server. Therefore the Idea proposal is to generating user interface appropriate with the role of the client and the type of content requested, and sending requests to the learning service. Means responsible for generating user interfaces for applications, adapted to a particular user, the currently used access device and the current context, and Generate token code sent to the server as an alternative for the username and password. The idea briefly is: send the username and password to the server only once (i.e. in the login process the first time), During this process the token code is generated based on the unique device ID, User ID, username, password and current time, then the token code is sent to the mobile client to be stored as a database record, then each time you request electronic content it will be sent by the token code without username and password.

Adaptive User Interfaces (AUIs) can provide potential benefits for addressing usability issues. Adaptation of the UI has been identified as an important aspect to be considered in the design of modern information systems. Adaptation techniques include adapting what information to present (information adaptation), how to present this information (presentation adaptation)

and how to interact with this information (interface adaptation), and from our view we think that adaptation of mobile user interfaces will have a major role in supporting the security system for e-learning environment.

Therefore, adaptively makes it possible for a system to behave in a different way for different users. In order to achieve that feature, adaptive systems need a user model which holds information about individual users. There are two types of Inputs when collecting data about users when creating a user model (Requesting direct input from users “explicitly” and Observing user's interaction with the system and automatically collecting information “implicitly”).

In addition, the learner needs can be classified as follows (User Knowledge, User's Interests, User's Goals and Tasks, User's Background, Individual Traits, Context of Work).

All of these things can take into consideration in future works, And use them as tools to develop the concept of adaptable mobile user interfaces, That will depend upon the security system for e-learning environment in the future.

REFERENCES

[1]. Ali Naserasadi, “Author’s Security in Electronic Learning Systems”, International Journal of Computer Applications, Vol. 21, Issue 10, pp. 25-29, 2011.

[2]. Carine G. Webber, Maria de Fátima W.P.Lima, Marcos E.Casa, Alexandre M.Ribeiro, “Towards Secure e-Learning Applications: a Multi agent Platform”, Journal Of Software, Vol. 2, Issue 1, pp. 60-69, 2007.

[3]. El-Khatib, K., Korba, L., Xu, Y., and Yee, G., "Privacy and Security in E-Learning", International Journal of Distance Education Technologies (IJDET), Vol. 1, No. 4, pp. 1-19, 2003.

[4]. Jianming Yong, “Enhancing the Privacy of e-Learning Systems with Alias and Anonymity", International Conference on Computer Supported Cooperative Work in Design, pp. 534-544, 2008.

[5]. Umit Kocabicak, Deniz Dural, “Secure and Interoperable e-Learning Platforms Based on Web Services ", International Conference on New Horizons in Education, pp. 1265 – 1271, June 2012.

[6]. Jianming Yong, "Security and Privacy Preservation for Mobile E-Learning via Digital Identity Attributes“, Journalz ofUniversal Computer Science (J.UCS), Vol. 17, No. 2, pp. 296-310, 2011.

[7]. Ivica Boticki, Natasa Hoic-Bozic, Ivan Budiscak, " A System Architecture for a Context-aware Blended Mobile Learning Environment", Journal of Computing and Information Technology(CIT), Vol. 17, No. 2, pp. 165–175, 2009.

[8]. Jorge Fontenla Gonza´ lez, Manuel Caeiro Rodrı´guez, Martı´n Llamas Nistal, and Luis Anido Rifo´n, “Reverse Oath: A solution to achieve delegated authorizations in single sign-on e-learning systems”, computers & security, Vol. 28, No 8, pp. 843-656, 2009.

[9]. Shadi R Masadeh, Nedal Turab, Farhan Obisat, “A secure model for building e-learning systems”, Network Security, Vol. 2012, No 1, pp. 17–20, 2012.

[10]. Felician Alecu, Paul Pocatilu, George Stoica, Cristian Ciurea, Sergiu Capisizu, “OpenID, a Single Sign-On Solution for E-learning Applications “,Journal of Mobile, Embedded and Distributed Systems(JMEDS), Vol. 3, No. 3, pp. 136-141, 2011.

[11]. Huping Wang, Chunxiao Fan, Shuai Yang, Junwei Zou, Xiaoying Zhang, “A New Secure OpenID Authentication Mechanism Using One-Time Password (OTP) “,Wireless Communications, Networking and Mobile Computing (WiCOM), 7th International Conference on, 2011.

[12]. Shadi R. Masadeh,Bilal Abul-Huda andNidal M. Turab, “a novel secure e-contents system for multimedia interchange workflows in e-learning environment”, International Journal of Computer Networks & Communications (IJCNC), Vol. 15, No 5, pp. 131–139, 2013.

[13]. Georgios Kambourakis, Denise-Penelope N. Kontoni, Angelos Rouskas, and Stefanos Gritzalis, “A PKI approach for deploying modern secure distributed e-learning and m-learning environments “,Computers & Education, Vol. 48, No. 1, pp. 1–16, August 2007.

[14]. P.R.Lakshmi Eswari, “A Process Framework for Securing an e-Learning Ecosystem “, 6th international conference on internet technology and secured transaction, pp. 403 - 407, Abu Dhabi, United Arab Emirates, 11-14, December 2011.

[15]. Anastasia Balia, and Dimitrios Koukopoulos, “A Secure Collaborative Multimedia Learning Scheme in Cultural Environments “,international conference on Information, Intelligence, Systems and Applications (IISA), pp. 1-5, Piraeus, 10-12 July 2013.

[16]. Yu-Lin Jeng, “An OpenID Based Authentication Mechanism in a Distributed System Environment”, International Journal of Computer and Communication Engineering, Vol. 1, No. 3, pp. 250-252, September 2012.

[17]. M. Tariq Banday, " Ensuring Authentication and Integrity of Open Source Software using Digital Signature”, International Journal of Computer Applications, IJCA Special Issue on Network Security and Cryptography NSC, Vol. 4, No. 2, pp. 11-14, 2011.

[18]. Yu-Hsiu Chuang, Chi-Yuan Chen, Tzong-ChenWu, and Han-Chieh Chao,” Establish a secure and trustworthy ICT environment for educational systems: a case study “,Journal of Intelligent Manufacturing, Vol. 23, Issue 4, pp. 965-975, August 2012.

[19]. Shantha Visalakshi. U and Shyamala. K, “Multi-agent coordination in distributed e-learning environment providing access permissions “, International Journal of Engineering and Technology (IJET), Vol. 5, No. 2, pp. 1306-1310, May 2013.

[20]. Dimitrios K. Koukopoulos, and Georgios D. Styliaras," Security in Collaborative Multimedia Web-based Art Projects", Journal Of Multimedia, Vol. 5, No. 5, pp. 404-416, October 2010.

[21]. Amjad Mahfouth, "The Authentication Techniques in Distributed E-Learning between Universities in Avicenna Virtual Campus Network", International Journal of Computer Science Issues (IJCSI), Vol. 9, Issue 3, No 2, pp. 418- 422, May 2012.

[22]. Felician ALECU, Paul POCATILU and Sergiu CAPISIZU, " WiMAX Security Issues in E-learning Systems", Journal of Mobile, Embedded and Distributed Systems(JMEDS), Vol. 2, No. 1, pp. 15-20, 2010.

[23]. Sadaf Ahmad and Mohammad Ubaidullah Bokhari, “A New Approach to Multi Agent Based Architecture for Secure and Effective E-learning “,International Journal of Computer Applications(IJCA), Vol. 46, No22, pp. 26-29, May 2012.

[24]. Mohammed Alzaabi, Jawad Berri and Mohamed Jamal Zemerly, “Web-based Architecture for Mobile Learning “,International Journal for Infonomics (IJI), Vol. 3, Issue. 1, pp. 207-216, March 2010.

[25]. MD. Anwar Hossain Masud and Xiaodi Huang, "M-learning Architecture for Cloud-based Higher Education System of Bangladesh ", Mobile Computing, Vol. 2, Issue. 4, pp. 84-94, November 2013.

[26]. T. Altameem, "Contextual Mobile Learning System for Saudi Arabian Universities ", International Journal of Computer Applications, Vol. 21, No 4, pp-21-26, May 2011.

[27]. Krzysztof Walczak, Jacek Chmielewski, Wojciech Wiza, Dariusz Rumiński and Grzegorz Skibiński, "Adaptable mobile user interfaces for e-learning repositories ", IADIS International Conference on Mobile Learning, 2011.

[28]. Krzysztof Walczak, Wojciech Wiza, Dariusz Rumiński, Jacek Chmielewski and Adam Wójtowicz, "Adaptable User Interfaces for Web 2.0 Educational Resources ", IT Tools in Management and Education-Selected Problems, pp. 104-124, 2011.

[29]. N. Nurseitov, M. Paulson, R. Reynolds, and C. Izurieta, "Comparison of JSON and XML Data Interchange Formats: A Case Study", in Proc. CAINE, 2009, pp.157-162.

[30]. Antonio Sarasa-Cabezuelo and José-Luis Sierra, "Grammar-Driven Development of JSON Processing Applications", Proceedings of the Federated Conference on Computer Science and Information Systems, pp. 1545 – 1552, 8-11 Sept. 2013.

[31]. Adam Wójtowicz, Jakub Flotyński, Dariusz Rumiński, and Krzysztof Walczak, "Securing Learning Services Accessible with Adaptable User Interfaces", Information Systems Architecture and Technology, Service Oriented Networked Systems, pp. 109-118, 2011.

[32]. Georgios Kambourakis, " Security and Privacy in m-Learning and Beyond: Challenges and State-of-the-art", International Journal of u- and e- Service, Science and Technology, Vol. 6, No. 3, pp. 67-84, June, 2013.

[33]. Roberto G´omez C´ardenas and Erika Mata S´anchez, "Security Challenges of Distributed e-Learning Systems ", 5th International School and Symposium, ISSADS, Volume 3563, pp. 538-544, Guadalajara, Mexico, January 24-28, 2005.

[34]. Zainal Fikri Zamzuri, Mazani Manaf, Adnan Ahmad, and Yuzaimi Yunus, "Computer Security Threats towards the E-Learning System Assets", Second International Conference, ICSECS, Volume 180, pp. 335-345, June 27-29, Kuantan, Pahang, Malaysia 2011.

[35]. Alok Tripathi, and Abhinav Mishra, "A Web-based E-Learning Environment for Information Security", International Journal of Computer Applications (IJCA), Vol. 45, No. 4, pp. 50- 54, May 2012.

[36]. Rajesh Wadhvani, and Devshri Roy, "Developing Agent Oriented Mobile Learning System ", International Journal of Computer Science and Information Security (IJCSIS),, Vol. 10, No. 4, PP. 93-98, April 2012.

[37]. Mohd Anwar and Jim Greer, "Facilitating Trust in Privacy-Preserving E-Learning Environments", IEEE Transactions on Learning Technologies, Vol. 5, No. 1, pp. 62-73, January -March 2012.

[38]. Lili Sun, Hua Wang, and Yan Li, "Protecting Disseminative Information in E-Learning ", 6th International Conference Advances in Web Based Learning (ICWL), pp. 554–565, UK, August 15-17, 2008.

[39]. E. Kritzinger, "Information Security in an E-learning Environment ", IFIP International Federation for Information Processing, Volume 210, pp. 345-349, August 21–24, Chile 2006.

[40]. Miguel, J., Caballe, S. and Prieto, J, "Information Security in Support for Mobile Collaborative Learning ", Seventh International Conference on Complex, Intelligent, and Software Intensive Systems, pp. 379- 384, 3-5 July Taichung 2013.

[41]. Najwa Hayaati Mohd Alwi and Ip-Shing Fan, " E-Learning and Information Security Management", International Journal of Digital Society (IJDS), Vol. 1, Issue. 2, pp. 148-156, June 2010.

[42]. Ateeq Ahmad and Mohammed Ahmed Elhossiny," E-Learning and Security Threats ", (IJCSNS) International Journal of Computer Science and Network Security, Vol. 12, No. 4, pp. 15-18, April 2012.

[43]. Vladimir I. Zuev, "E-Learning Security Models", (JMIS) Journal of Management Information Systems, Vol. 7, No. 2, pp. 024-028 April 2012.

[44]. Im Y. Jung and Heon Y. Yeom, "Enhanced Security for Online Exams Using Group Cryptography ", IEEE Transactions on Education, Vol. 52, No. 3, pp. 340-349, August 2009.

[45]. Defta (Ciobanu) Costinela – Luminita, "Information security in E-learning Platforms ",3rd World Conference on Educational Sciences, Volume 15, pp. 2689–2693, Istanbul, Turkey 2011.

[46]. Professor Aurel ŞERB PhD, Lecturer Costinela - Luminiţa DEFTA, PhD. Candidate, Junior Lecturer Nicoleta Magdalena IACOB, PhD and Lecturer Marius Cristian APETREI, PhD. candidate, "Information Security Management In E-Learning ",Knowledge horizons Journal , Vo. 5, No. 2, pp. 1 - 6, 2013.

[47]. Nikhilesh Barik and Dr. Sunil Karforma, "Risks and Remedies In E-Learning System", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.1, pp. 51-59, January 2012.

[48]. S.Hameetha Begum, T.Sheeba and S.N.Nisha Rani, "Security in Cloud based E-Learning ",International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue. 1,, pp. 270-278, January 2013.

[49]. Mr. Dhiraj K. Chandak and Prof.Mr. M.M. Bartere, "Security in Cloud Based M-learning", International Journal of Computer Science and Management Research, Vol. 2 Issue 4, pp. 2163-2170 , April 2013.

[50]. Defta (Ciobanu) Costinela – Luminita, "Security issues in e-learning platforms ", World Journal on Educational Technology, Vol. 3, issue. 3, pp. 153-167, December 2011.

[51]. Maria Nickolova and Eugene Nickolov, "Threat Model for User Security in E-Learning Systems", International Journal "Information Technologies and Knowledge, Vol. 1, No. 1, pp. 341-347, 2007.

[52]. Kyle Montague, Vicki L. Hanson, and Andy Cobley, "Adaptive Interfaces: A Little Learning is a Dangerous Thing ", 6th International Conference Universal Access in Human-Computer Interaction. Design for All and eInclusion (UAHCI), Volume 6765, Orlando, FL, USA, pp. 391–399, July 9-14, 2011.

[53]. Janet L. Wesson, Akash Singh, and Bradley van Tonder ", Can Adaptive Interfaces Improve the Usability of Mobile Applications, Second IFIP International Federation for Information Processing, pp.198–187 , Australia, September 20-23, 2010.

[54]. E. Kritzinger, and S.H von Solms, " E-learning: Incorporating Information Security Governance", Issues in Informing Science and Information Technology, Vol. 3, pp. 319-325, 2006.

TNC Transactions on Networks and Communications
SOCIETY FOR SCIENCE AND EDUCATION UNITED KINGDOM
VOLUME 2, ISSUE 4
ISSN: 2054 - 7420

Path loss prediction models for Corridor propagation at 24GHz

Femi-Jemilohun Oladunni .J and Walker Stuart .D
School of Computer Science and Electronic Engineering, University of Essex, United Kingdom;
ojfemi@essex.ac.uk

ABSTRACT

Mm-wave bands have recently become major options for short-range, high speed communication systems especially in the indoor wireless local area networks (WLANs). The pathloss prediction model is one of the metric parameters for determining the system effectiveness and performance in wireless indoor propagation. The channel characterization of 24GHz band in corridor propagation through extensive field strength measurements in real time application was conducted in this work. The results were used to derive the path loss equation for corridor propagation at this spectrum band based on log-distance path loss model and log-normal shadowing model. The pathloss realized falls within the estimated values in such scenario, it is therefore concluded that the predicted mathematical model for the described environment is accurate. Also the predicted pathloss which is lower than the free space propagation path loss results in aggregate high data rate, hence improved system performance is achieved.

Keywords: Pathloss, millimeter wave, multipath, Quality of Service, and fading

1 Introduction

The ever increasing supply of, and demand for, broadband multimedia to match up with the ever increasing capacity of wireless networks, had led to wireless transfer demand that is far beyond what the current bands in the Industrial, Scientific and Medical (ISM) and Unlicensed National Information Infrastructure (UNII) bands can accommodate. A way out is to resort to the millimeter wave (mmw) bands. Also the high data rates intended for 4G infrastructures will require the use of unlicensed spectrum with high and sufficient bandwidth to accommodate such huge capacities [1]. Mm-wave bands such as 24 GHz and 60 GHz have recently become the major options for short-range, high speed communication systems especially in the indoor wireless local area networks (WLANs). These bands offer the gigabit per second (Gb/s) throughput required by multimedia consumer-oriented applications. For the dramatic growth in appreciation and application of wireless communications, high quality of service (QoS), increase in the system reliability and capacity are inevitable for seamless communication systems. To

DOI: 10.14738/tnc.24.361
Publication Date: 24th August 2014
URL: http://dx.doi.org/10.14738/tnc.24.361

achieve this in mobile radio channel, the technical challenges peculiar to mmw such as multipath fading, polarization mismatch, and co-location interference must be adequately addressed [2]

Also, as e-commerce is becoming more widely used, it is expected that good internet services are available to end-users as they commute from place to place. In this scenario, as mobile terminals move from one office to the other through corridor and the like, wireless services should retain their high-throughput during the transit events [3]. The task of modelling radio propagation at hallway and tunnels is enormous. Among the various channel modelling techniques, ray tracing is well accepted [4-6]. It is noted that propagation in corridors and hallways suffers less losses than free space loss, on the contrary propagation through walls and floors incurs higher losses than free space loss [7].

This is similar to the experience in the corridor propagation as revealed by the results of the experimental work. This work carried out extensive signal strength measurements along a level four of a multi-storey building corridor. The results were used to determine the path loss exponent and standard deviation based on Log-distance path loss model and Log- normal shadowing respectively. An equation that describes the path loss of our propagation scenario was derived through numerical analysis of the results. The remainder of this paper is arranged as follows: Section two discussed the previous research works by different authors in the relevant area. The relevant background study of the topic was presented in section three, while the results and discussion of the experimental work carried out were presented in section four. Finally, the conclusion was given in section five.

2 Related Work

A lot of research works have been done and still on going in the area of wireless communication performances. Interest is been focused on the WLAN technology to provide the gigabits throughput required by multimedia applications, video conferencing, data streaming and many more services especially in an office environment as well campuses. In literature, there are some works on system performance evaluation and interference mitigation techniques in WLAN. However, very few of these authors have engaged physical devices in their works to realize real values. Likewise, the possibility of engaging 24GHz bands for wireless indoor propagation in multipath rich environment such as corridor has not been conducted by any author to the best of my knowledge. The first set of results in indoor WLAN at 24GHz is presented in this work. Some of the findings of the previous authors related to this work are enumerated as follows:

The overview of the newest technologies promised to deliver multi-gigabits throughput through IEEE802.11ac and IEEE802.11ad standards was carried out in [8]. The author described the channelization of physical (PHY) design, medium access control (MAC) modifications, and beamforming in the standards. In [9], the pathloss and delay characteristics of indoor radio channels from 2.4 GHz to 24 GHz were carefully investigated in a typical modern building. One

particularly interesting conclusion was that delay variation increased with frequency in the Non-Line-of- Sight (NLoS) case in contrast to Line-of-Sight (LoS). In [10], the same authors used ray-tracing techniques to model, with good accuracy, 2.4 to 24 GHz path loss in the NLoS cases. They also found that delay variation was only predicted reliably in the LoS case. A 2.4 GHz indoor radio WLAN in a dense office environment was examined in [11]. It was concluded, inter alia, that the antenna properties can have a large impact on performance. The effects of wall materials on the attenuation of radio waves in indoor propagation up to 5 GHz were considered in [12]. They observed that signal attenuation is differentiated by wood or concrete construction and its dependence on frequency.

From this review, it is concluded firstly that the 24 GHz band is worth considering for the indoor environment. Secondly, we believe this present work to be the first investigation of 24 GHz band, high-data rate, within-building, wireless systems. Research showed that there is a logarithmic decrease relationship between the average signal power and the distance in a theoretical and measurement based propagation models. The computational complexity involved can be reduced by empirical models while prediction accuracy is increased [13]. This work is based on Log-distance path loss model and Log-normal shadowing.

3 Basic propagation property at MMW

The success of radio wave propagation in a building is affected by the topology, construction and materials of the building. A modern building with open-plan design containing walls with large glass windows will give added path loss of about 5dB while a building made of thick stone walls with small windows and many internal solid walls will add an extra path loss of several tens of dB (decibel). Some of the physical effects of wireless indoor propagation are fast decay of signals, constrained coverage by walls, and attenuation by walls, floors, furniture, and scattering of radio waves [14].

3.1 Fresnel Zone

It is important to maintain a radio frequency (RF) LoS between the transmitting and receiving terminals for effective long range wireless communication systems. Visual LoS is a straight line path that enables a clear sight between two terminals. In any case RF LoS requires both virtual LoS as well as a Fresnel zone that is void of obstacles to achieve optimum data transfer from one point to another. Fresnel zone is defined as the long ellipsoid path between two terminals that creates a path for RF signals. It is very essential that the Fresnel zone be freed of any obstructions such as buildings, trees, humans, as these will degrade the communication networks and reduce the range. As a rule of thumb, 60% of this zone must be cleared of obstruction. Any transmission path void of Fresnel zone is termed RF NLoS, this a typical experience in indoor propagation environment [15].

3.2 Multipath and fade margins

Multipath is the splitting of the RF signals from the transmitter along different paths. This phenomenon can be constructive when the waves travelling along different paths combined in phase at the receiver, otherwise destructive when they combine out of phase thereby cancelling out the signals. Fading is as a result of multipath, it is the difference between the normal received power and the power required for minimum acceptable performance. Greater fade margin imply less frequent occurrences of minimum performance levels, this also means that the received signal during unfaded condition is so strong that bit errors are virtually non-existent. Severe fading due to multipath can cause a signal degradation of more than 30dB, which will affect the reliability of the communication links [16].

3.3 Pathloss models

A propagation model is a set of mathematical expressions, diagrams, and algorithms used to represent the radio characteristics of a given environment. The pathloss prediction models can be either empirical (also called statistical) or theoretical (also called deterministic), or a combination of these two. The empirical models are based on measurements, while the theoretical models deal with the fundamental principles of radio wave propagation phenomena [17]. Some existing pathloss models are listed below:

3.3.1 Okumura-Hata Model

This is a combination of two models developed by Masaharu Hata and Okumura. This model accuracy is high as it is based on measurements in a specific environment but it can only be used to predict the path loss of outdoor propagation. It is expressed mathematical as follows [18]:

$$L_{50}(dB) = 69.55 + 26.16\log(f_c) - 13.82\log(h_{te}) - a(h_{re}) + (44.9 - 0.55\log(h_{te}))\log(d) \quad (1)$$

Where, $L_{50}(dB)$ is the 50th percentile median pathloss, f_c is the center frequency in megahertz, h_{te} and h_{te} are base and receiver stations antennas heights in meters respectively, a(h_{re}) is a vehicular station antenna height-gain correction factor depending on the environment, and d is the link distance in kilometers.

3.3.2 Log-distance pathloss model and Log-Normal shadowing

These are acceptable models for prediction of pathloss in an indoor/NLoS propagation environment. They show the linear relationship between the pathloss in decibel and the logarithmic variation of the transmitter and receiver separation [2]. The path loss exponent (n) on which large scale pathloss of random T-R separation depends is a function of the propagation environment while reduced value of n gives lower signal loss. The value of n for free space is 2, it ranges from 1.2 (waveguide effect) to 8 in general. Equations (2 and 3) depict the parametric relationship of Log-distance pathloss model.

The different level of clustering on the signal propagation path leads to random shadowing effects. This is not accounted for in Log-distance path loss but in Log-normal shadowing as shown in (4). The average pathloss for a given transmitter and receiver distance d is given by [19, 20] as follows:

$$PL_d \propto \left(\frac{d}{d_0}\right)^n \quad (2)$$

$$PL_{dB} = UL_{d0} + 10nlog\left(\frac{d}{d_0}\right) \quad (3)$$

Where PL is the average pathloss between transmitter and receiver, UL_{d0} is the reference pathloss at d_0==1m for indoor propagation, n is the pathloss exponent and d is the separation between transmitter and receiver in meters. (2) is modified as shown below to give the Log-Normal Shadowing equation.

$$PL_{dB} = UL_{d_0} + 10nlog\left(\frac{d}{d_0}\right) + X_\sigma \quad (4)$$

3.3.3 Joint Technical Committee (JTC) Model

The mathematical representation of this model is given according to [21] [22] as:

$$L_{Total} = A + Blog_{10}(d) + L_f(n) + X_\sigma \quad (5)$$

Where A is an environmental dependent fixed loss factor in dB, B is the distance dependent loss coefficient, d is the separation between transmitter and receiver in meterL_f is a floor/wall penetration loss factor in dB, n is the number of floors/walls between the transmitter and receiver, and X_σ is a normal (Gaussian) random variable in dB with zero mean and standard deviation σ in d.

4 Experimental methodology

The experimental set up shown in Fig 1 consists of the 24GHz point-to-point link with maximum output power of 20dBm. It has delivery capacity of 1.4Gbps using the HDD in bidirectional mode at 6X64 QAM modulations scheme (highest) and is backward compatible to lower modulation scheme of QPSK through the automatic rate adaptation to accommodate low signal transmission. The feature enables a link pair to sustain up to 142.5 dB path loss when switched to basic QPSK modulation mode. Full duplex transmission is used with slight different carrier frequency of 24.1 and 24.2GHz; a bandwidth of 100MHz. The transmitting and the receiving terminals have an antenna gain of 33dBi each [23][24]. For the empirical experiment, both antennas were mounted on tripods 1.7m above the floor level, and connected to PCs for signal transmission monitoring. The link was set up in the corridor as shown in Fig 2, where the signal strength measurements at eight different distance locations from 1m-36m at step of 5 were taken during propagation.

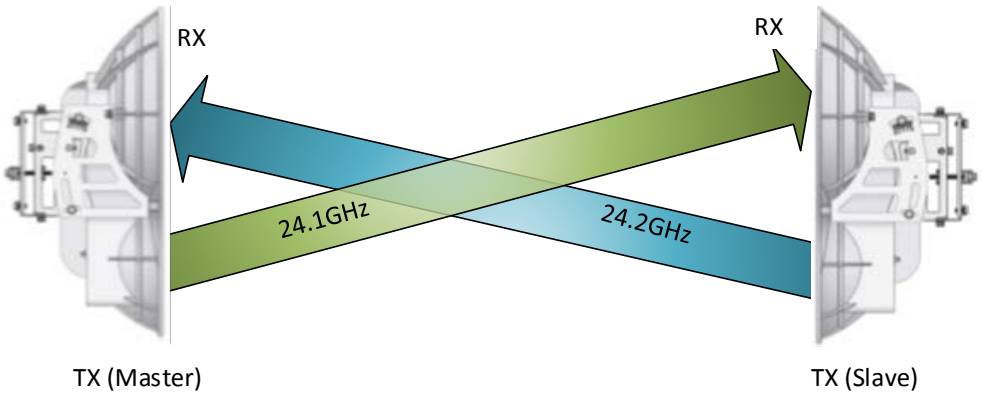


Fig.1: airFibre Ubiquiti 24 GHz back-to-back set-up in full duplex operation

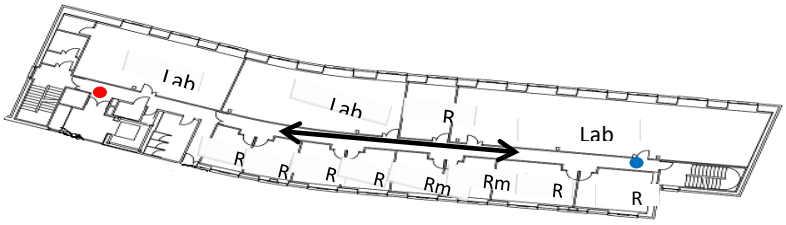


Fig.2: detailed map of signal propagation at the corridor

4.1 Results and Discussion

In order to predict the pathloss model for the environment under consideration at 24GHz spectrum, the values for predicted pathloss (UL) are calculated using (2) and (3), the pathloss exponent (n) is derived from the measured values using Linear Regression concept to minimize the difference between the measured and predicted pathloss values means square error, and to compute the values of n and σ [20] as represented by the following equations:

$$\mathrm{e(n)} = \sum_{k=1}^{m} (PL - UL)^2 \qquad (6)$$

The computation procedures are as simplified in the table below:

Table 1: Computation of Mean square error

Distance(m)	PL(dB)	UL(dB)	(PL-UL)dB	$(PL-UL)^2$dB
1	54.033	54.033	0	0-
6	56.37	54.03+7.7n	2.33-7.7n	5.43-35.88n+59.29n^2
11	63.46	54.03+10.04n	9.43-10.04n	88.93-189.35n+100.80n^2
16	68.09	54.03+12.04n	13.72-12.04n	188.23-330.37n+144.96n^2
21	69.03	54.03+13.22n	14.66-13.22n	214.91-387.61+174.76n^2
26	73.26	54.03+14.14n	18.89-14.14n	356.83-534.20n+199.94n^2
31	79.91	54.03+14.91n	25.54-14.91n	652.29-761.60n+222.31n^2
36	82.12	54.03+15.56n	27.75-15.56n	770.06-863.5n+242.22 n^2

From the table,

e (n) =1144.17n2-3100.51n+2276.68 (7)

By differentiate (7), the value of n was computed as;

n = 1.4

The standard deviation was derived in a similar manner using:

$$\sigma(dB) = \sum_{k=1}^{m} \sqrt{\frac{(PL-UL)^2}{m}} \quad (8)$$

m = 8, is the number of locations where measurements were conducted

σ (dB)=4.9dB

The model for the considered propagation environment using (4) and the calculated parameters therefore is,

PL (dB) =54.03 +10(1.4) log (d) + 4.9

PL (dB) = 54.02+14log (d) +4.9 (9)

The results of the experiments yielded the path loss exponential of 1.4 and standard deviation of 4.9dB. Since the path loss falls within the estimated values in such scenario (1.2-8) [3], then it can be concluded that the predicted mathematical model for the described environment is accurate. Also the low value of the path loss suggests that the signal loss in this scenario is low. This peculiarity can be traced to the wave guiding effects that enhance the signal propagation in the corridor. Since the predicted path loss is lower than the free space propagation path loss, aggregate throughput of data rate is high, hence improved system performance is achieved.

The equation generated from pathloss prediction is used to create the models shown Figs 1-3, to visualize the propagation phenomenon for the propagation environment. The Figs reveal that the measurements models outperformed both the free space model and proposed model by an average of 10dB and 8dB respectively, while a convergence is seen between the measure and predicted models as the distance increases (Fig 4).The predicted models though outperformed the free space model, both are seen to be almost same the at the initial stage but deviate as the distance increases with an average difference of 10dB at 36m distance (Fig 5).

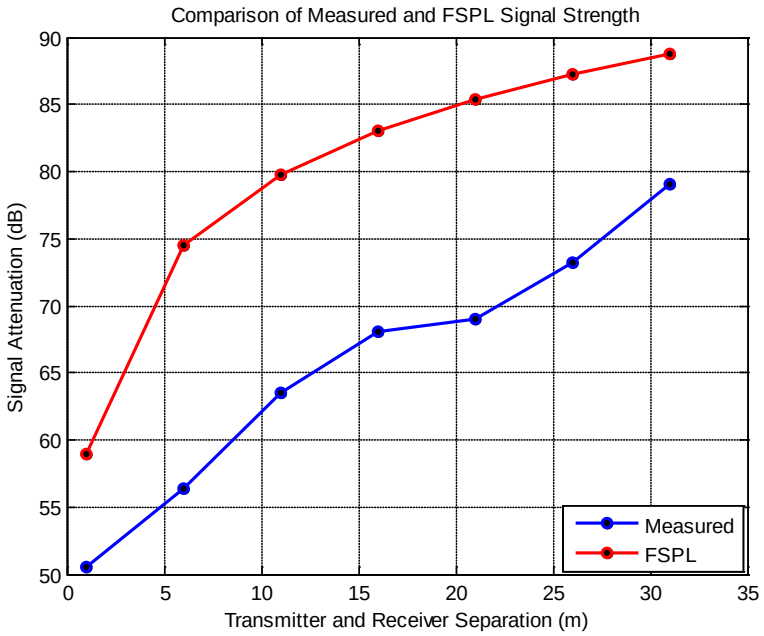


Fig 3: Measured Signal Pathloss and FSPL compared

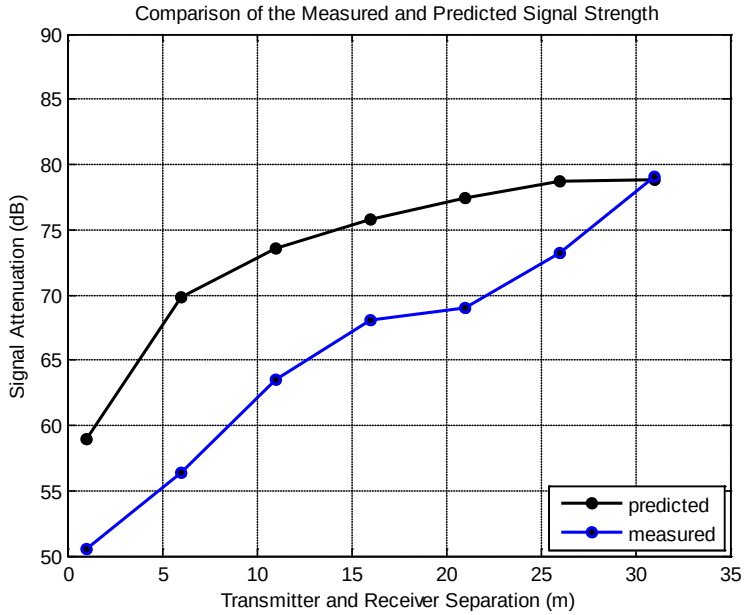


Fig 4: Measured and Predicted Signal Pathloss compared

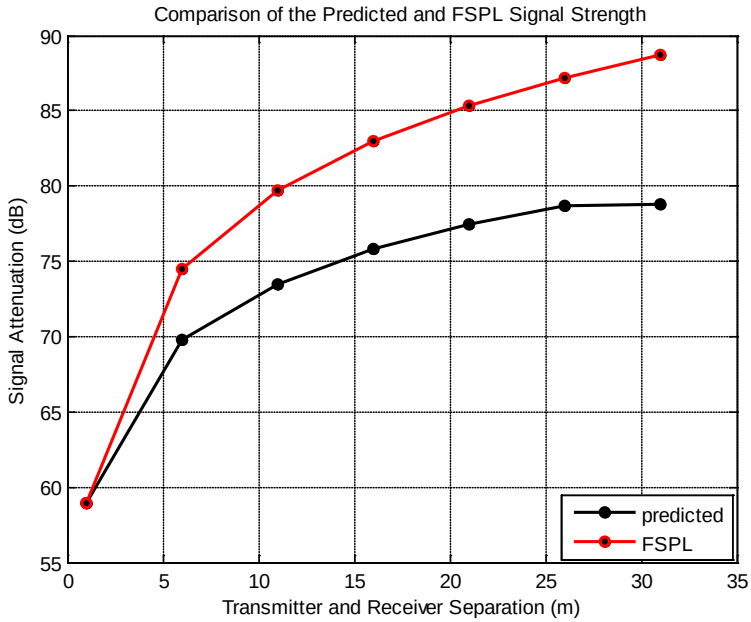


Fig 5: Predicted Signal Pathloss and FSPL compared

5 Conclusion

In this work, indoor propagation model was developed for a corridor based on empirical model of Log-distance path loss model and log-normal shadowing .The path loss equation for our scenario was determined through numerical analysis of measurement results. The results of the experiments yielded the path loss exponential of 1.4 and standard deviation of 4.9dB. The pathloss exponent of 1.4 realized through the pathloss prediction empirical analysis is

significant: Since the path loss falls within the estimated values in such scenario (1.2-8), then it can be concluded that the predicted mathematical model for the described environment is accurate. Its low value confirmed the good signal strength achieved in this scenario during wireless transmission as reported in earlier work [25], establishing the fact that the waveguide-like effects of the corridor enhanced the signal throughput through reflection; it also represents the different obstruction the signal passed through during propagation. Since the predicted path loss is lower than the free space propagation path loss, aggregate throughput of data rate is high, hence improved system performance is achieved. The results show that a hallway/corridor as well as typical office can be flooded with gigabit/s through wireless transmission to enable seamless communication and adequate bandwidth requirement for multimedia applications services.

REFERENCES

[1]. Xingang G, Sumit R, and W. S. Conner, *Spatial reuse in wireless ad-hoc networks,* in Vehicular Technolohg Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th .IEEE 2003, vol. 3 pp. 1437-1442 .

[2]. Yann L, et al, *Beamforming techniques for enabling spatial-reuse in MCCA 802.11 s networks,* EURASIP Journal on Wireless Communications and Networking, vol. 2011, pp. 1-13, 2011.

[3]. Andrej H, *et al, A Survey of Radio Propagation Modeling for Tunnels.*, *IEEE Communications Surveys and Tutorials*, vol. 16, no. 2, pp. 658–669, IEEE 2013

[4]. Youngmoon K, et al, *Analysis of radio wave propagation characteristics in rectangular road tunnel at 800 MHz and 2.4 GHz*, in Antennas and Propagation Society International Symposium, 2003. IEEE, 2003, vol. 3, pp. 1016-1019.

[5]. CG Liu, et al, *Modelling radio wave propagation in tunnels with ray-tracing method,* in Antennas and Propagation (EuCAP), 2013 7th European Conference on IEEE, 2013, pp. 2317-2321.

[6]. Yue P. Z, *Novel model for propagation loss prediction in tunnels,* Vehicular Technology, IEEE Transactions on, vol. 52, pp. 1308-1314, 2003.

[7]. Jadhavar R and Sontakke TR, *2.4 GHz Propagation Prediction Models for Indoor Wireless Communications Within Building*, International Journal of Soft Computing and Engineering (IJSCE), vol. 2, pp. 108-113, 2012.

[8]. Pengfei X, et al, *Short range gigabit wireless communications systems: potentials, challenges and techniques,* in Ultra-Wideband, 2007. ICUWB 2007. IEEE International Conference on IEEE, 2007, pp. 123-128.

[9]. Dai L and Dave R, *Investigation of indoor radio channels from 2.4 GHz to 24 GHz,* in Antennas and Propagation Society International Symposium, 2003. IEEE, 2003, pp. 134-137.

[10]. Dia L and David R, *Indoor wireless channel modeling from 2.4 to 24 GHz using a combined E/H-Plane 2D ray tracing method,* in Antennas and Propagation Society International Symposium, 2004. IEEE, 2004, pp. 3641-3644.

[11]. John C. S, *Indoor radio WLAN performance part II: Range performance in a dense office environment,* Intersil Corporation, 1998.

[12]. Ali-Rantala P, et al, *Different kinds of walls and their effect on the attenuation of radiowaves indoors,* in Antennas and Propagation Society International Symposium, 2003. IEEE, 2003, vol. 3 pp. 1020-1023.

[13]. Robert G A, et al,*Indoor propagation modeling at 2.4 GHz for IEEE 802.11 networks,* International Association of Science and Technology for Development, 2005.

[14]. I. Rosu, *Basics of Radio Wave Propagation*. YO3DAC/VA3IUL, 10.

[15]. Jim Z and Al P, *Tutorial on basic link budget analysis,* Application Note AN9804, Harris Semiconductor, 1998.

[16]. Aleksandar N, et al*, Modern approaches in modeling of mobile radio systems propagation environment,* Communications Surveys & Tutorials, IEEE, vol. 3, pp. 2-12, 2000.

[17]. Muzaiyanah H, et al, *Wifi signal propagation at 2.4 GHz*, in Microwave Conference, 2009. APMC 2009. Asia Pacific, 2009, pp. 528-531.

[18]. Iskander M. F. and Yun Z., *Propagation prediction models for wireless communication systems, Microwave Theory and Techniques, IEEE Transactions on*, vol. 50, pp. 662–673, 2002.

[19]. Jorgen B A, et al, Propagation measurements and models for wireless communications channels, Communications Magazine, IEEE, vol. 33, pp. 42-49, 1995.

[20]. Scott Y S and Theodore S R, *914 MHz path loss prediction models for indoor wireless communications in multifloored buildings,* Antennas and Propagation, IEEE Transactions on, vol. 40, pp. 207-217, 1992.

[21]. Cebula S, *et al, Empirical channel model for 2.4 GHz ieee 802.11 wlan,* in *Proceedings of the 2011 International Conference on Wireless Networks*, 2011.

[22]. Halford K. and Webster M, *Multipath measurement in wireless LANs, Intersil Application Note AN9895*, vol. 1, 2001.

[23]. Yun S., *et al., Hybrid division duplex system for next-generation cellular services,* Vehicular Technology, IEEE Transactions on, vol. 56, pp. 3040-3059, 2007.

[24]. Sang Y. J., et al *An Overlaid Hybrid-Division Duplex OFDMA System with Multihop Transmission*, ETRI Journal, vol. 33, p. 201, 2011.

[25]. Femi-Jemilohun O.J, et al, *An Experimental Investigation into GbE Wireless Data Communication at 24GHz in Non-Line-of-Sight and Multi-path Rich Environments* in IEEE Antenna and Wireless Propagation Letters, 2014, vol. 13 pp1219-1222,

TNC Transactions on Networks and Communications
SOCIETY FOR SCIENCE AND EDUCATION UNITED KINGDOM
VOLUME 2, ISSUE 4
ISSN: 2054 - 7420

The Impact of Information Systems on the Governmental Administration in the Arab Republic of Egypt in Light of the Digital Revolution

Aryan Abdullwahab Qader
Department of Information Technology
Institute of Graduate Studies and Researches, Alexandria University
163 Horreya Avenue, El Shatby 21526, P.O. Box 832, Alexandria, Egypt
arean96@yahoo.com

ABSTRACT

With the emergence of the digital revolution, the world has changed drastically. The impact was great enough to drag the developing world into using information systems in governmental administration; changing the entire course of administration in those developing countries. The information systems are a better substitute for the systems the governments use in order to offer a better service for its citizens. Most of those services that the governmental administrations offer are connected to the internet and can be accessed through it. The developing countries including the Arab world understood the importance of information systems and began to employ them gradually.

The governmental information systems in Arab countries are currently under pressure due to the growth. Those obstacles and challenges occur due to the technical change which showed the effects of information systems in all developing fields. Today, it is impossible to think of developing the social and economic fields without paying a great deal of attention to the information systems.

This research aims to study the effect of using and applying the information systems in the administrations of the Arab countries and the problems and obstacles that occur in using those systems.

1 Introduction

One of the major problems in the Arab world in general is administration. Especially when it comes to governmental administration, the problems vary due to the lack of resources, poverty and whatnot. However, those are merely reasons for the problem with Egypt. Egypt's main

DOI: 10.14738/tnc.24.362
Publication Date: 24th August 2014
URL: http://dx.doi.org/10.14738/tnc.24.362

problem is with administration regardless of its reasons and that reflects on the problems that it faces.

The physical resources and the human resources are the most important for governmental companies and ministries. However, it wasn't until the rising of the information role was revealed that those companies and ministries realized the importance of information. Information is the core of all modern governmental administrations. Information systems are without a doubt necessarily for communications and monitoring.

With the recent revolution of information systems the world has witnessed, it is of great importance to make use of those systems in the Arab Republic of Egypt. Those resources can form the strategy to overcome the current circumstances which change rapidly. The competition is growing as well, not only locally but on a world wide scale which means that the country must be able to keep up and avoid the routine in order to keep up with the era of technology.

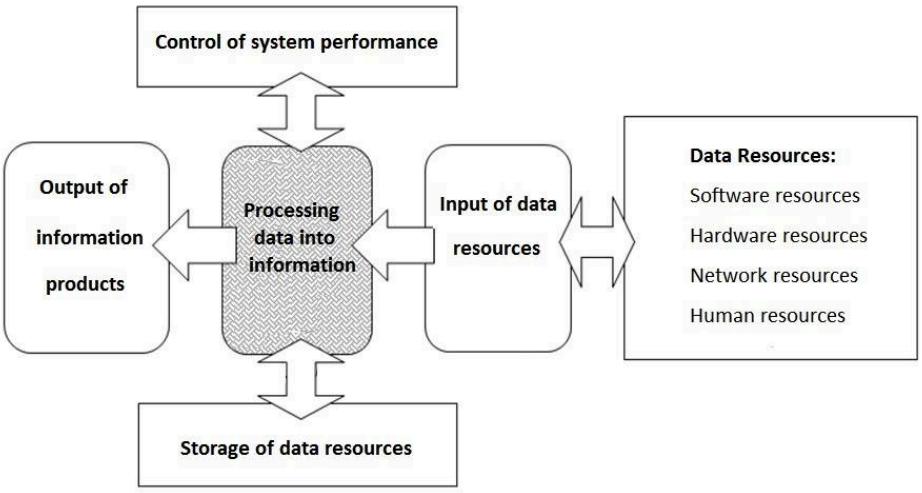
Information Systems as a Pathway to Develop Administrations:

Information Systems are systems that are made of a set of elements which use information resources. The information systems receive the data of programs, equipment, networks and human resources and process them into information under supervision. The information and the data are stored in storages that keep the data secure.

The Classifications of Data

In [figure 1], a virtual model of the components of information systems in shown.

Figure 1 [The Components of Information Systems]



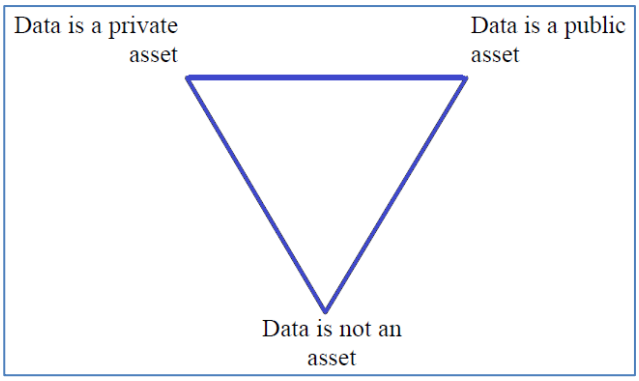
The information plays a major role in keeping the harmony between the rapid changes and the needs and capabilities of the administrative institutions. There are many ways that show the

need for having an information system. Of those, one of the most important is increasing the specialities, dividing tasks, new decision-making methods and heading to a non-centric administrative system.

Governments and How They See Information:

Data security has been an issue for a long time which has troubled the governments. However, as a mean for security, different governments had different ideas on how to make the availability of the data most secure. This has led to three different viewpoints on data as shown in [figure 2]. The three extremes represented in [figure 2] vary the levels of barriers that governments put on the data in order to secure it.

Figure 2: Governments Different Viewpoints on Data



- Data as a public asset: governments identify that the data is public because it has been collected from everyone, thus making it a public property. This point of view can assist both social and economic development. After all, citizens should be given the right and freedom to access the data held about them; however, not without exceptions.
- Data as a private asset: this point of view allows citizens to see the data about themselves and other general kinds of data as long as they pay. The investment of the production of data often has commercial value, thus it should be sold to the highest possible price to earn a valuable revenue for the public sector.
- Data is not an asset: this is where governments don't see data important enough to consider ownership, value or charging. Here, data is a personal asset of specific public sector staff and it is not made available for citizens to access it. [1]

The Private-Public Gap:

Governments often try very hard to fit the information systems designed for private sectors into the public sectors. Those tries die so often because the public sector often has uncompetitive rates of pay in contrast to the private sectors. Simply put, the high quality IT professionals will not be recruited and the public sector recruitments will lack the experience or the skill. As a result, the e-government projects become underdone in comparison the private sector projects. [2]

The Importance of Information for Administrative Institutions:

Typically, information can be perceived in three different types:

- Information as a Resource: as information is used to obtain a certain goal. Information should be used and administrated to achieve the goals of a certain project.
- Information as an Asset: as it can be in the assets the administration owns. For instance, the assets of buildings or machinery which aid the production. That allows the administrative system to have the edge against the competition.
- Information as a Commodity: as information can be considered one of the products of the administration whether to monitor the performance or to aid in the decision making process. [2]

The Value of Information Systems to the Administration:

The information systems are of crucial importance to the administration of the country. The information system is generally used to operate, collect and transport the information into electronic data. That is known as Information Technology (IT) which includes computers, communication systems, networks, faxes and other means of communication.

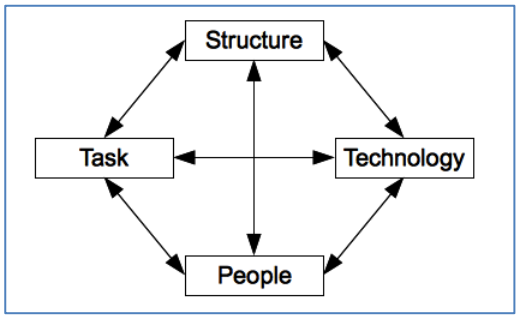
The success of the administrative system truly depends on the decision-making technology used by the system. In the United States of America, 50% of the investor's capital in the administrative system relies on information. In the US, there are approximately 63 computers for each 100 workers and about 88% of the administrations use computers in their daily work. In 1996, the United States spent over the 500 million dollars on IT.

However, the administrative systems may fall into what is known as the 'social inertia' when it comes to information systems. Typically, 'social inertia' means that no matter how hard you try, nothing gets done. The main causes for social inertia in information systems are:

1. Information takes a small part of organizational decision processes.
2. Organizations prefer to take smaller steps to avoid any damage.
3. Data is a political resource and new information systems may affect particular groups' interests. [2]

Harold Leavitt defined organizations as diamond [figure 3] in which people, technology, structure and tasks are constantly adjusting as they are interrelated. This is an indication of the complexity of the social systems in general. [3]

Figure 3[Leavitt's Diamond Shape]



The Different Types of Information Systems:

Information systems can be divided into four different types within the administration. The main types of information systems are:

- Operation Processing Systems: those systems process the main operations to allow different activities to be available in the administrative system.
- Administrative Information Systems: they consist of groups of operations which permit different levels of administration with the necessary information to aid in processing the operations and decision making.
- Decision Making Systems: the decision making system is considered to be the core of the administrative operation which can be quite troublesome to the administrators in the governmental agencies. The system aids in making the best decision, making up plans and substitutions and choosing the best solutions depending on the available sources.
- Secretary Information Systems: those systems aim to increase the better performance for the secretaries and the official workers in the administrative system.

2 Aspects of Applying Information Systems in the Administrative Agencies of the Government

Computers and other means of communications are playing a major role in our daily lives. It isn't known where this technology would stop if it ever would and the evolution it has brought to society is seen best in the developed world. However, there are signs of applying the methods of information systems in the Arab Republic of Egypt:

- Electronic Governments: which applied the technology and use information systems to ease the administrative processes for the citizens in order to obtain the necessary documents, permissions and services.
- The Gap between Information Systems: there is a gap between different places and it varies depending on how the governments respond to the digital revolution. In the developed world, we see that the information systems are improving rapidly as the

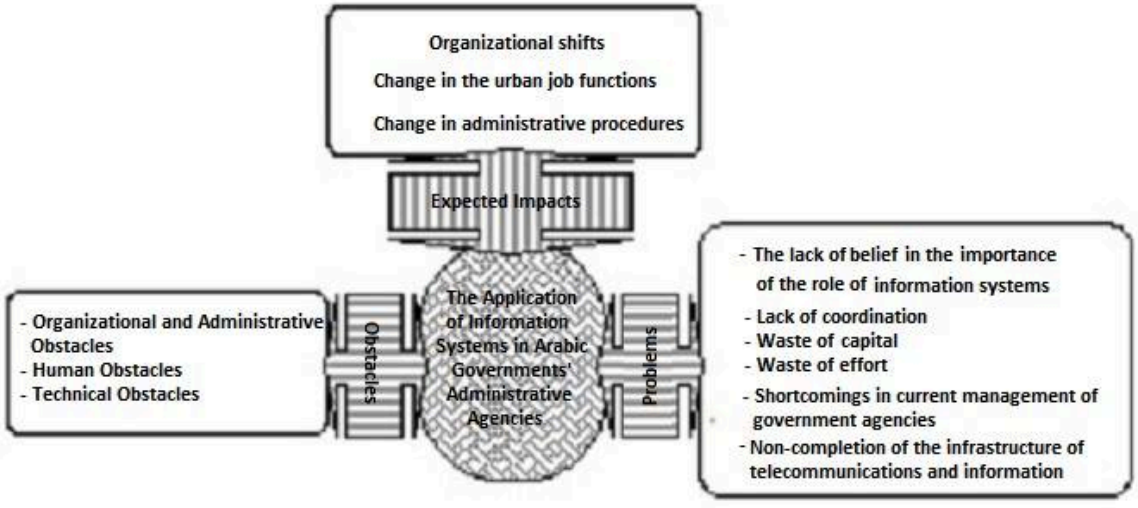
governments work on the necessary infrastructure for the next stage of the digital revolution in what is known as the Information Superhighway.

The Differences in Providing the Informational Services

There is a great difference between areas that receive informational services and the areas that don't receive the same service in one city. This variety in one city led on to a drastic change in the way organizations think. For instance, IBM decided to shut down entire physical branches and replaced them with branches all across the city as they adopted the experience.

The changes that are expected to happen to information systems [figure 4] especially in Arabian cities and Egypt would have obstacles occurring constantly. Problems and obstacles can divert the course of the usage of information systems.

Figure 4[Impacts, Problems and Obstacles Facing Information Systems]



3 The Quality of Administrative Decisions

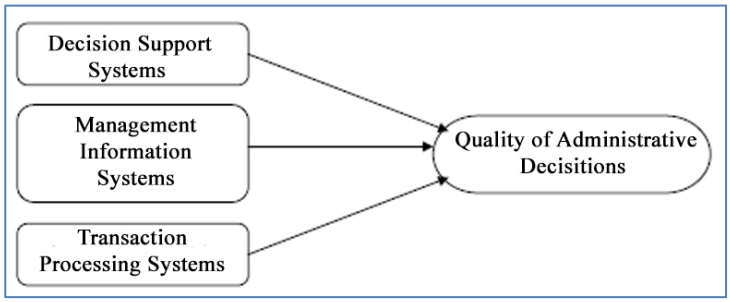
The quality of administrative decisions relies on three major elements: the decision support systems, the management information and the transactions processing systems [figure 7]. The main function of information systems is to provide the citizens with accurate information. Without any of the mentioned elements, the quality of the administrative decisions would fall apart.

Decision Support Systems:

The Decision Support Systems (DSS) are easily defined. They are a mean to aid in making the decisions for administrative systems. However, the DSS does not replace the decision maker, it

only does the preparation for the ultimate decision. Those systems also aid in the planning and preparation for the long run in the administration.

Figure 5[The Quality of Administrative Decisions]



Management Information Systems

Management Information Systems or otherwise known as Administration Information Systems are systems made up of groups of employees, organizations, operations and sub systems to supply the administration with all the required information.

Transaction Processing Systems:

Transaction Processing Systems (TPS) are related to the daily operations as they supply the administration with accurate and detailed data. The supply of information happens throughout the day on daily basis, informing the administration of the changes that occur such as the departure or arrival of a certain personnel, the amount of imported or exported goods…etc.

4 Expectations on the Effects of Information Systems in Egypt

Drastic changes can occur due to the effects of the information systems on the Arab Republic of Egypt which could possibly change the ordinary routine. Of the major changes that would occur, an organized would address the entire basis of the administration system. That change would decrease the number of levels in the administration and increase the area of monitoring.

Electronic mail would be a great necessity with the changes that would occur as it would be the main method of addressing citizens and employees alike. E-mails would ease the organizing between colleagues who are working on the same or similar tasks. That also means that the routine of having to attend work every day would cease and it means that more concentration would be on the job itself rather than the daily unnecessary tasks that only waste time.

Other changes would be in the form of sharing information through extremely fast methods of delivering information and combining communication tools. That also means that there will be no limited time or place to import or export the information.

Services will be delivered at an increasingly rapid pace whether from the house or office which means that it will be really easy to 0064eliver the tasks before deadlines. Citizens will wait less for responses and the service provided will not take as long to operate or maintain. Bills will be

paid through the internet or the telephone without a problem and obtaining a passport or a birth certificate will take much less time. Speed will be the trend and complaints would drastically decrease and cease at a point.

While the past decades have witnessed extremely slow reactions from the governmental administrations in the developing countries, that would definitely change with the rapid changes that will happen due to the usage of information systems. In short, information systems will simply make life a lot easier.

5 The Problems and Obstacles Facing the Administration Systems in the Arab Republic of Egypt

There are major problems that face Egypt as it progresses and develops. Some of the problems and obstacles can be quite consistent that they slow down the process of using the information systems and others are only habitual problems that can be solved in time.

5.1 The Belief that the Information Systems Are Unnecessary:

One of the initial problems that face the information systems in Egypt is the fact that many people will claim that the best place for information systems to be used is the private sector of business. However, even though the private sector in Egypt is more independent and can change the moment the owner or the council of the company desire, the governmental sector also needs information systems to be applied even more than the private sector which already uses them to a certain extent.

5.2 Lack of Organization:

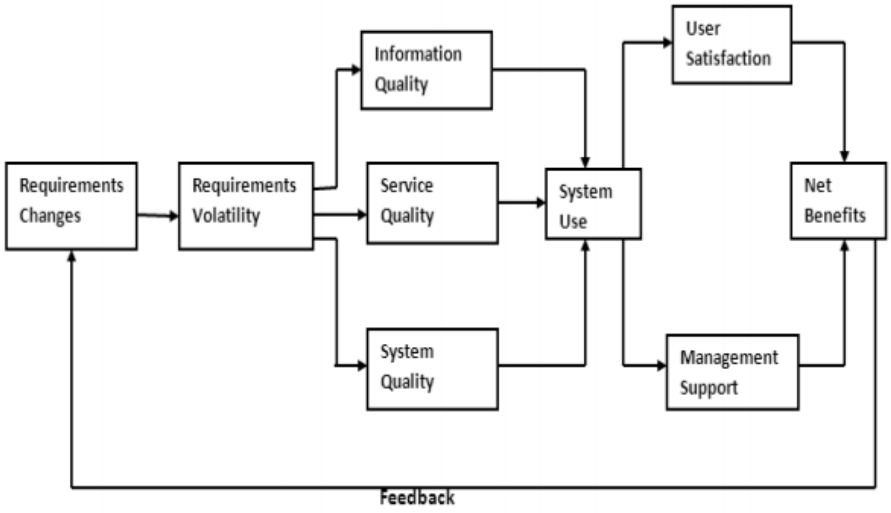
Although many developing countries have founded enormous centres for research and collected numerous technicians and specialists, those centres did not face much success because there was no organizing between them to know whether they are working on something unique or not which eventually wasted a lot of money. The lack of strategy and vision not only wastes money on research, but truly doesn't get any of them anywhere.

5.2.1 User Satisfaction:

As a part of the success of developing countries, there is also three facilitating constructs that ensure the success: requirement changes, requirements validity and top management support. User satisfaction is directly related to the quality of information, service quality and system quality. The only way to achieve user satisfaction is through those three elements. [6]

In [figure 5] the relationship between user satisfaction and the success of information systems in the developing world is explained.

Figure 6[User Satisfaction and How It Affects the System]



5.3 The Shortcomings in the Governmental Administrations:

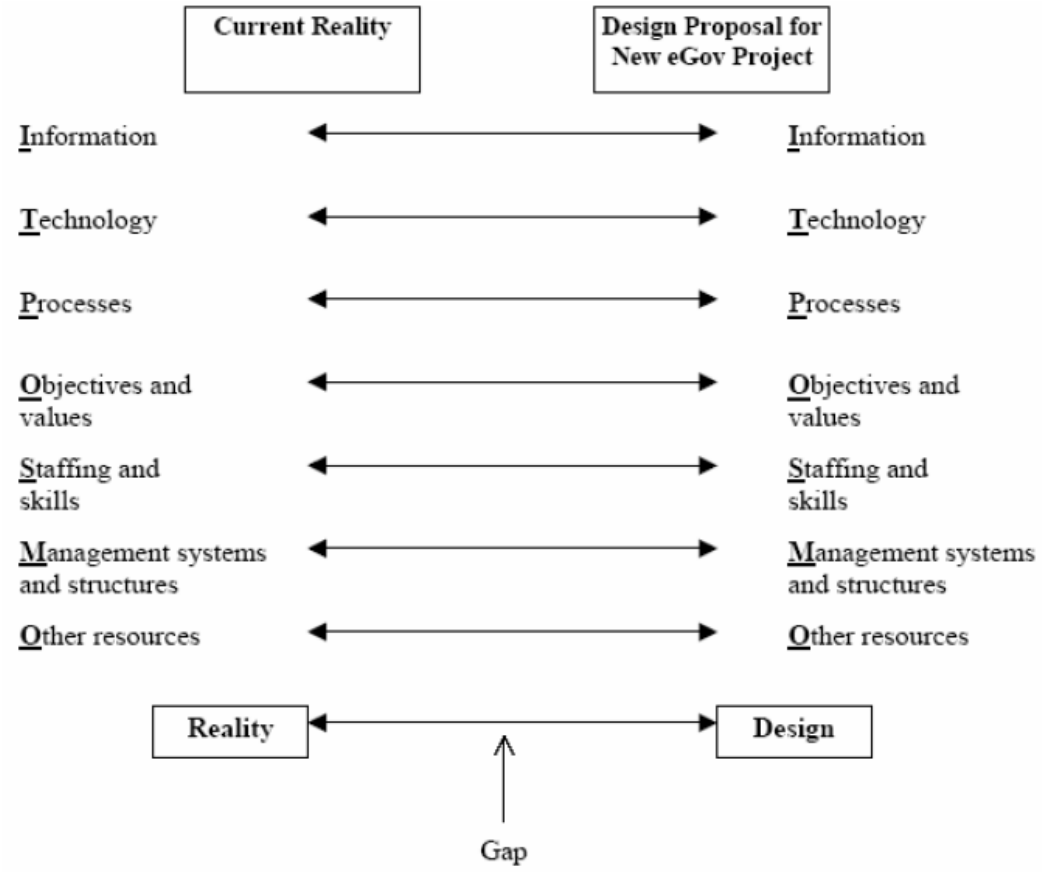
Because the administrations do not make the best use of their resources and information especially the likes of municipalities which are the core of the city, they have had plenty of shortcomings. The increasing population and the increasing needs of the people demand more yearly which cannot be achieved due to the old methods of the administrations. The governmental administrations do not make the best of the materials they have and thus they are unable to make the best use of the information systems so far.

5.3.1 Causes of Failure in Applying IT Systems:

E-governments fail with a percentage of 35% being a total failure and 50% being partial failure in the developing countries. This is due to the limited number of resources available in developing countries and therefore cannot afford to spend great amounts of money on the IT projects. The focus of technology in the developing countries is ordering the administration and the citizen and in ensuring of greater accountability and transparency. [5]

However, the motive for applying IT systems in developing countries is highly questionable. The transparency does not require e-government to be achieved and if the motive is such then the IT systems in developing countries are doomed to fail. The gap between the reality of the IT system and the design is often considered a cause of damnation for the IT system as seen in [figure 6]. [6]

Figure 7 [The Gap between Reality and Design]



5.4 The Incomplete Infrastructure:

The infrastructure of communications is incomplete in most of the Arab world which prevents the Arabs from being able to make the best out of the information systems proposed. Computers and communications are facing a disaster with the incomplete infrastructure which overall is the least in the world. The United Arab Emirates is an exception when it comes to the incomplete infrastructure, however, Egypt is not.

5.5 Administrational and Technical Obstacles:

One of the biggest obstacles that stand in the way of using information systems is the lack of a unified policy that can organize, arrange and monitor the usage of information systems across the country. Egypt stands amongst the second class of Arab countries following the likes of Kuwait and Emirates and before the likes of Syria and Morocco in a list of the Arab countries that use information systems. [4]

The reason there is this huge gap between the expected interests which the information systems should bring and the actual interests that have been accessible is due to two main reasons:

- The lack of a unified policy and the independence of each sector of the administrations all over the country rather than using the same network with the same rules to organize the usage of information systems.
- The information systems have been admitted without making any changes in them to the infrastructure or in the operating methods which means that the information system will be another manual tool that would scarcely decrease the time needed to get the job done.

5.6 Human Obstacles:

The human element is the base of every system, yet with over 273 million over 16 and under 60 in the Arab world, most of them do not contribute in the information system. There a number of reasons as to why they do not contribute effectively. [4]

- Illiteracy which was around 39% of the Arab world in 2002 in contrast to the 22.5% world-wide.
- The lack of technical specializations in the field which means that there are few programmers who can contribute to information systems and even less technicians who can operate and maintain it.
- The huge gap between the interest of the technicians in the field and the ones who use the information systems.
- The capability of using that technology to threaten the private lives of people and other social elements which could be instantly threatened.
- Using foreign expertise and depending solely on them in some of the Arab countries which means that they will have less interest as they are not a part of the country and their interest will only be temporary.

6 Conclusion:

Information can easily be considered one of the most strategic resources in any administrative agency. Without information, those agencies would not be able to access most of their operations without depending on information and they cannot reach the decision making methods without such information. Due to the importance of information to those agencies, they cannot help but consider information systems the cores of the operations they could make and more importantly with the information systems more opportunities could be found and made use of.

Without a doubt, information systems could alter the direction of advancement in the Arab world entirely. Egypt could witness a great rise in its system with the usage of the information systems that could possibly change the direction of how people perform their duties and the slowness would be diminished with the usage of information systems.

In light of the digital revolution, it is necessary to keep up with the incline of the era. It is most crucial to adjust and overcome the flaws in the system and reshape the entire administrative system that the government uses in order to make it a better place and greater service.

If the Arab countries resist the change and insist on following the outdated systems they use, they will fall under a lesser category. The consequences would be severe especially for countries like Egypt. Doubtless, everything will change gradually with information systems from economics to society and if the Arab world is unable to keep up with the technology, they will be unable to keep up with the rest of the world.

REFERENCES

[1]. R. Heeks, "Information Systems for Public Sector Management," Working Paper Series (Paper no. 9), 2000.

[2]. Ciborra, C. & Navarra, D., "Risks and Challenges of E-Governments in Jordan," in Development Theory, and Aid Policy, Information Technology for Development, 2005.

[3]. Gordon, Judith R. & Gordon, Steven R.,, Information Systems: A Management Approach., New York: Harcourt Brace College publishers, The Dryden Press, 1999.

[4]. P. G. W. Keen, "Information Systems and Organizational Change," Communications of the ACM, vol. 24, no. 1, 1981.

[5]. H. J. Leavitt, "Applying Organizational Change in Industry: Structural, Technological and Humanistic Approaches," in Handbook of Organizations, Chicago, 1965.

[6]. P. Ssemaluulu, An Instrument to Access Information Systems Success in Developing Countries, Groningen, Netherlands: University of Groningen, 2012.

[7]. D. Dada, "The Failure of E-Government in Developing Countries: A Literature Review," The Electronic Jounral on Information Systems in Developing Countries, London, 2006.

[8]. C. Cibora, "Good Governance, Development Theory, and Aid Policy: Risks and Challenges of E-Government in Jordan," Information Technology for Development, 2005.

[9]. M. J. Shio, "An Approach to Design of National Information Systems for Developing Countries," in Information Systems in the Public Administration, Amesterdam, North-Holland Pub. Co.,, 1983.

TNC Transactions on Networks and Communications
SOCIETY FOR SCIENCE AND EDUCATION UNITED KINGDOM
VOLUME 2, ISSUE 4
ISSN: 2054 - 7420

An Agent-Based Model for Cross-Enterprise Supply Chain Management

Tarini Prasad Panigrahy[1], Manas Ranjan Patra[2]
[1]*Gandhi Institute for Technological Advancement, BPUT, Bhubaneswar, India*
[2]*Department of Computer Science, Berhampur University, Berhampur, India*
tarinip@yahoo.com, mrpatra12@gmail.com

ABSTRACT

In order to cope with the dynamic scenario of fast changing business requirements enterprises have embraced web technologies to manage their business processes. However, the ability to integrate business processes like procurement, customer relationship management, finance, human resources and manufacturing in a typical supply chain on the web is a challenging task. Today's virtual enterprises need to integrate different workflows within and across enterprises efficiently so as to provide seamless services. Cross-enterprise workflows can not only streamline and coordinate business processes across organizational boundaries in a dynamic Web environment but can provide low cost and flexible solution to supply chain management. In this paper, we have proposed an agent-based cross-enterprise workflow Management System (WFMS) architecture which can dynamically integrate the workflows and compose a workflow execution community customized to different workflow specifications. The model allows the process agents to update the execution plans dynamically and coordinate the functions of the participating service agents.

Keywords: Supply Chain Management, Workflow Management System, Cross Organization Workflow, Agent based workflow.

1 Introduction

Supply Chain Management (SCM) is referred to as the logistics network, which synchronizes a series of inter-related business processes in order to: (1) acquire raw materials from a supplier, (2) transform these raw materials into finished products(manufacturing), (3) add value to these products, (4) distribute and promote these products to either retailers or customers, (5) make information exchanges among various business entities (e.g. suppliers, manufacturers, distributors, retailers and customers). There are mainly three stakeholders to play their roles in a typical supply chain, namely, the Manufacturer, who produces/provides the products, the

DOI: 10.14738/tnc.24.380
Publication Date: 24th August 2014
URL: http://dx.doi.org/10.14738/tnc.24.380

Customer, who purchases the products, the Supplier, who provides raw materials to the manufacturer based on their demand.

Figure 1 show an inter-organizational co-operation system where each of the stakeholders has its own SCM. So SCMS-supplier, SCMS-Manufacturing and SCMS-Customer should perform all supply chain activities in a coordinated fashion. Here the cooperation process model tries to ensure business interoperability with other enterprises. The logistics supply chain coordination includes both vertical and horizontal logistics supply chain coordination and risk management processes. The SCMS-Manufacturing has the goal to optimize their production planning and resource utilization, SCMS-Supplier have the goal to balance supply and demand, negotiate with the supply and demand process and minimize the inventory and number of stock-outs for the whole logistics supply chain, SCMS- Customer has to provide the demand through an order and receives the stock from the manufacturer by maintaining its own inventory system.

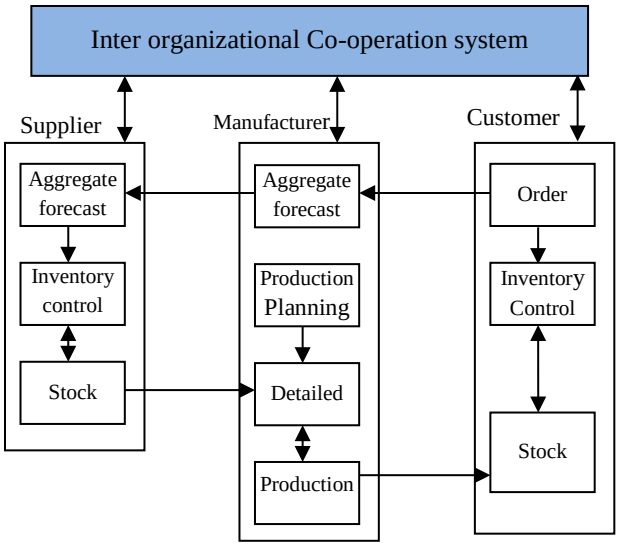


Figure 1: Inter organizational Co-operation system

The main aim of the Supply Chain Management (SCM) is to enhance the operational efficiency, profitability and competitive position of an organization and its supply chain partners. The performance of a SCM is measured in terms of the objectives such as superior quality, cost minimization and delivery on-time etc. All the entities of a logistics supply chain are highly interdependent. As a result, performance of any entity in the supply chain depends on the performance of others, and their ability to coordinate activities within the supply chain [1][2][3][4]. The Supply Chain is a network of several businesses and their relationship [5]. In a typical SCM the independently managed companies coordinate their activities to form a Virtual Enterprise [6]. For an example, the order placement process, order fulfilment process and shipment process in a typical SCM might be done by different companies. These companies provide their offerings as independent functional units called as web services. According to Erl

[7][8] these web services (Sub process) combine together (as shown in Fig 2) to make up a larger part of the business logic automation and each one of them can be distributed.

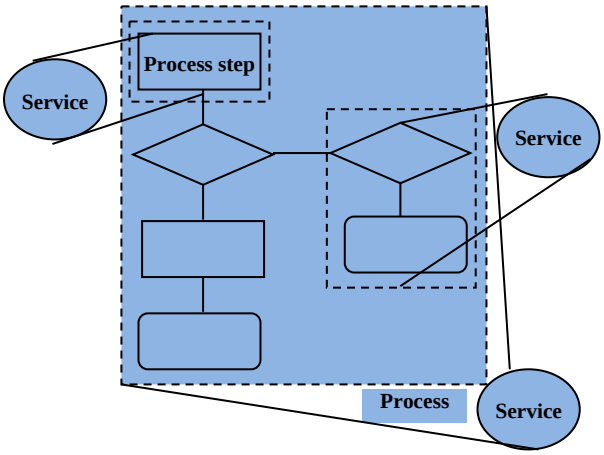


Figure : 2 Communications between Process and Service

Such an environment can be called as a service oriented cross organization environment which incorporates the interoperability of web services from various organizations. For example in a SCM the stakeholders supplier, customer and manufacturer can be considered as independent components, which can be specified with web services technologies, have the capability of being discovered and accessed from distributed locations. We specify these web services through Web Services Description Language (WSDL) [9] and can invoke them using the Simple Object Access Protocol (SOAP). In addition to advertising the specifications of distributed services universally, we use Universal Description Discovery and Integration (UDDI)[9] architectures.

Further, dynamics and unpredictability of the business such as faults or breakdown in utility equipment or an extended delay in taking delivery of raw materials, failure of production facilities, customers change or cancel orders, etc. make real-time cooperative operations on the supply chain complex and difficult [11]. For example, whenever there is a change in a customer order, then the partners in supply chain should be immediately communicated and react to the changes accordingly. Thus the occurrence of an event should be immediately propagated throughout the supply chain so as to do timely coordination and interaction of business processes (according to the changes) within and between the enterprises. So in designing a SCM, the key principle is timely coordination and interaction between various business processes in order to meet the challenge [12]. Workflow management systems have been widely adopted in providing solutions to facilitate SCM implementation in an organization. However, because of the lack of flexible mechanisms with cross-organizational business activities workflow management technology has had little success in achieving dynamic coordination and interaction in a supply chain management. Software agents are autonomous and goal-oriented software entities, which with other agents can operate asynchronously and

co-ordinate when needed [13]. Further in a cross organizational collaboration, the web services have the following shortcomings which we can resolve by using Software agents:

i) When we examine a web service, it is a self-describing software process/component for an application and does not have enough knowledge about its environment, users, software components, and outside world. On the other hand, software agents are capable of reasoning, and interacting with other entities.

ii) When we think of a web services it is discoverable by XML-based UDDI standard. Current standard of UDDI is only able to recognize terms "syntactically". But the main dispute in service discovery is how to find services, which are "semantically" the same as clients' needs. But when we use Software agents, they can operate at the knowledge level, at which they are able to reason semantically on the service requesters.

In this paper we take advantage of software agent technology under the control of a workflow management system, to effectively integrate cross-organization workflows. The difficulty with current workflow technology is its inability to cope with pro-activeness, dynamic interactions and component autonomy which agent-based system can provide.

Rest of the paper is organized as follows. In section 2, we formally specify the workflow model. In section 3 we present an agent-based workflow architecture that we use to describe workflow process management system. In section 4, we present the execution of the SCW for the proposed architecture, in section 5, we present our current implementation. A scenario of using agent based workflow is reported in section 6, finally we discuss some related works and summarize our findings in section 7.

2 Workflow Specification Model

We propose a service oriented workflow model. Using this model, major parts of a workflow process can be represented as web services (i.e., tasks or workflows).Thus, to represent a cross-organizational workflow process we use higher-level specification that can be composed from existing component workflows. Workflow components can be reused and specialized in different organizational settings.

We represent a workflow process as a tuple W:

$W = (S, E_w, R_w)$ where:

1. S is a set of services: $S = \{s_1, s_2 \ldots s_n\}$

2. E_w, is a set of workflow Event-Condition-Action-Monitor (ECAM) rules:

$E_w = \{e_1, e_2, \ldots e_n\}$. The workflow ECAM rule specifies the coordination among the tasks. We have a monitor agent to monitor the execution of the workflow and to inform process agent and other monitor agents if there is any exceptional event during the execution of the workflow. In order to

Define the ECAM rules, we use the following operations:

- ■Δ s: Enables the execution of the service s;
- ■∇ s: Disables the execution of the service s;
- ■ ↪s: Sends a message to the service s;
- ■ ∗W : Starts the execution of the workflow W;
- ■ ⊙W: Finishes the execution of the workflow W.

A workflow ECAM's rule is defined as follows:

(s_i . result == R)→ Δs_i

Which means enable the execution of service s_j when execution the service s_i returns R.

3. R_w, is the result of the workflow execution. It can be success, failure or null .Before the workflow execution begins it is initialized to null. A service can be represented as a tuple s_i:

$s_i = (N_i , O_i , E_{si} , D_i , R_{si})$ where:

1. N_i Represent the name of the service, which is a string to identify the service.

2. O_i is the task object (type of service), which is a tuple (P, T, TR, OP) where:

(a) P Represent set of properties which reflect the general information

about the task object (e.g., the creator of the task).

(b) T Represent a set of possible states: $T = \{t_1, t_2, ... t_n\}$, where:

i) t_i is the initial state: $t_i \in T$

ii)t_f is the final state: $t_f \in T$, if object's State changes to t_f, it implies that the execution of the task is successful.

(c) TR Represent a possible set of transitions (t_i , t_j) , where t_i , $t_j \in T$

(d) OP Represent a set of operations on T, such that TR ⊆ T X O P X T

3. E_{si} is a set of ECAM rules: $E_{si} = \{ e_{i1} , e_{i2}, ... e_{in}\}$. The ECAM rules for a service are used to guide the execution procedure of individual services, for example when to trigger related operations. Further it should be noted that a service can be atomic or complex (i.e a sub process in the workflow). Two kinds of rules are supplied:

C → A: if condition C is true, then operation A might be executed.

C ⇒ A : if condition C is true, then operation A must be executed.

4. Di Represent the deadline to complete a service/task.

5. R_{si} Represent the result of the task execution which may be success, failure, or null. In the beginning we set R_{si} to null. In this model, we distinguish workflow ECAM rules from task/service ECAM rules. Workflows ECAM rules are used to specify the interaction among

workflow services, where as the ECAM rule for a service are used to guide the execution procedure of individual services. In our model, the definition of a cross-enterprise workflow involves the identification of the services/tasks that compose the workflow and specification of the interactions between them. This is different from traditional workflow where it is also necessary to define who will be responsible for the execution of each task and how much time is allocated for each task at specification time. In our approach, tasks are dynamically assigned to service providers (i.e. entities that can perform the tasks, e.g., programs) during the enactment of a cross-enterprise workflow. The dynamic composition of services to provide a cross-enterprise workflow will be discussed further in section 4.

3 Agent based Workflow architecture

Figure 3 describes architecture for an agent based workflow. The entire architecture can be classified into three logical components. They are: workflow definition tool, agent community and actual service.

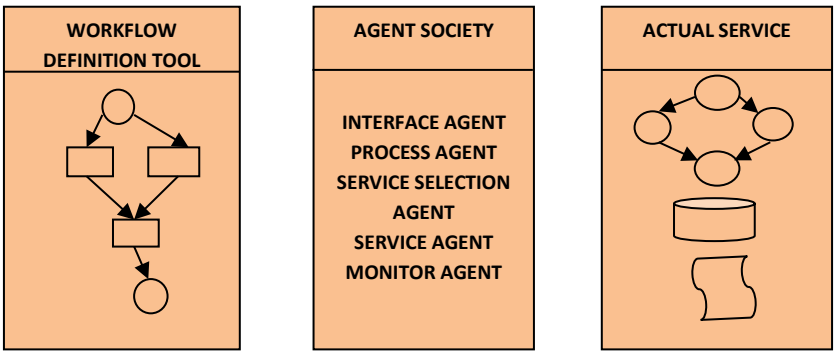


Figure :3 Agent based Workflow Management System

The task of the Workflow Definition Tool is to define cross-enterprise workflow specifications through the end user by using a standard GUI tool. The Agent Community is a set of agents that forms an agent Society which acts cooperatively to provide the general functionalities of a cross-enterprise workflow execution engine. Actual Services offer applications (called as services) from the physical organizations that allow the user to access and use them to perform the specified tasks during workflow execution.

The detail architecture of the agent based workflow is presented in Figure 4. It supports cross enterprise workflow that involves multiple organizations. For executing such a workflow we use five types of agents in the system, namely interface agent, service agent, service selection agent, process agent and monitor agent. For each workflow instance these agents form an agent community to execute the workflow.

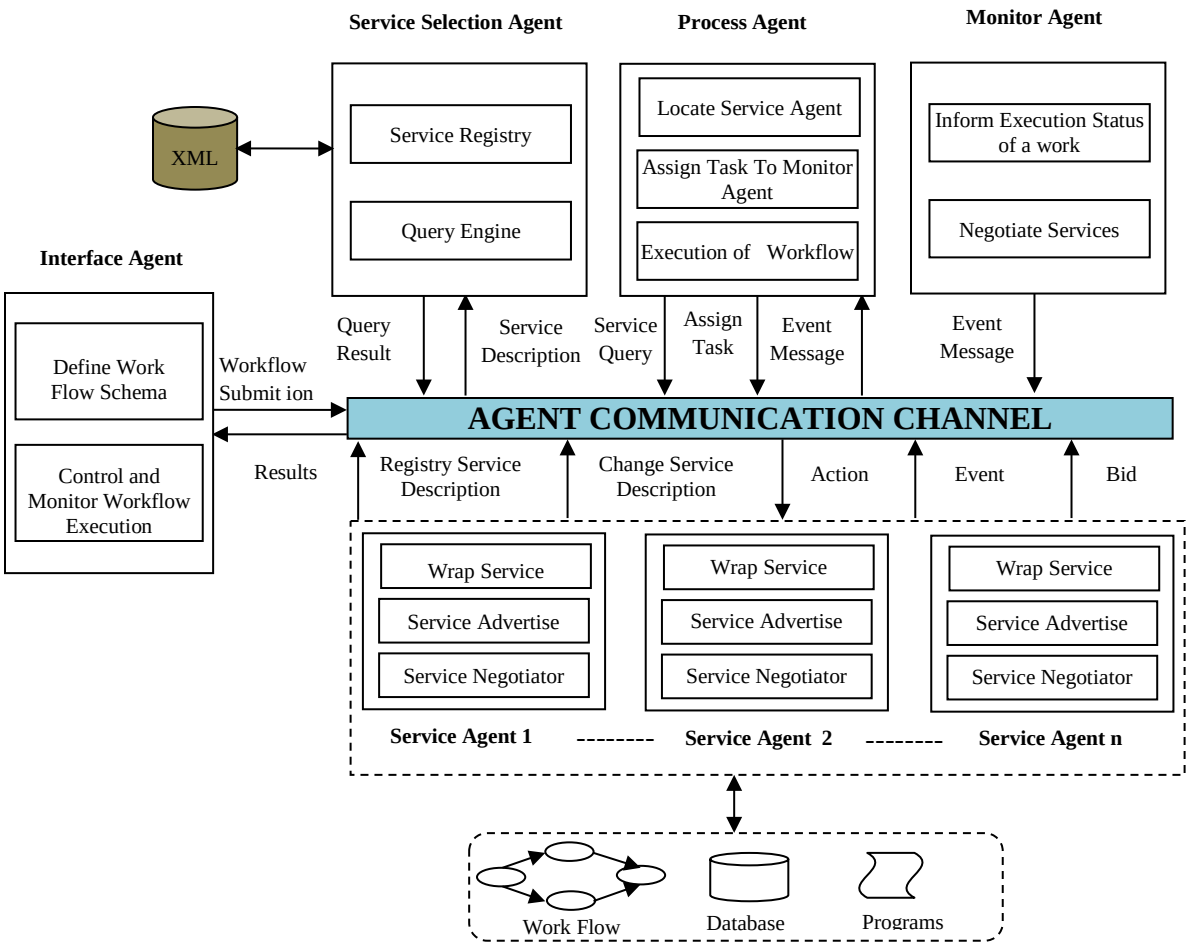


Figure 4: Architecture of agent Based Workflow

3.1 Interface Agent

It is through this agent the user can interact with the system. Here the user plays two types of roles; (i) as workflow process composer to define workflow schema (ii) as end user to create and start workflow instances, control and monitor the execution of workflow instances. The interface agent provides a tool to define the workflow schema, which is represented by UML state chart diagram. In order to draw the workflow schema we follow the following methodology:

1. Identify various tasks that constitute the workflow where each task in a state chart diagram constitutes input data, output data, states and transitions.
2. Draw the workflow by specifying the control flow among the tasks using transitions, fork and Join

Once the process composer draws the UML state chart diagram for the workflow schema, the end user generates an XML document for it. Further the end user provides the parameters required to select the appropriate service agents to execute the workflow. The XML document is submitted to the process agent to execute the workflow.

3.2 Service Agent

Service agents are used to abstract the business processes from their physical organisations. The agents capture different states of a business process which can be expressed in XML as follows:

```
<?xml version=”1.0” encoding=”UTF-8”?>
<!DOCUMENT SUPPLY CHAIN MANAGEMENT “Customer Order”>
<CustomerOrder>
<Service ID=”001” Name=”customer order process”/>
<Services>
<States>SendOrder1, ReceiveItem1,ReleasePayment</states>
<Transitions>
<Transition>
<From>SendOrder1</From><To>ReceiveItem1</To>
<TransitionString>
<Event>ReceiveItem1</Event>
<Condition>Avail(Item1)==true</Condition>
<Action>ReceiveItem1</Action>
</TransitionString>
</Transition>
<Transition>
<From>ReceiveItem1</From><To>ReleasePayment</To>
<TransitionString>
<Event>ReleasePayment</Event>
<Condition>avail Credit >= PriceQuoted</Condition>
<Action>ReleasePayment</Action>
</TransitionString>
</Transition>
</Transitions>
<Services>
</CustomerOrder>
```

(Customer_orderProcess.xml)

A service agent contains the following information:

(i) Service identification, which represents the port that contains the service, the format of the request message that it can understand and process

(ii) Agent capabilities which specify the name and the operations that the underlying service provides, and

(iii) Agent properties which specify constraints associated with the service

For example, the Customer Order Processing in a SCM can be represented in a service agent as shown below:

Agent Identity

Agent name: OrderItem1Agent

Agent address: 203.4.5.101.2323

Agent type: service

Agent interface: XML, SQL92

Agent Capabilities

Supported object: OrderItem1

Supported operations: SendOrder1, ReceiveOrder1,ReleasePayment

Supported query: price

Agent properties

Agent constraint: Delivery period {within 30days}

(Service Agent)

3.3 Service Selection Agent

The service space in a web-based environment is large and highly dynamic. In order to search a specific service in such an environment efficiently we use a service selection Agent. The service agents advertise and hence register their offerings like identity, capabilities and constraints in a meta data repository (UDDI). The meta data is used to locate the service agents. The process agent who is responsible for transforming the workflow specification to a workflow instance makes a query to the service selection Agent to find the suitable service agents. Then the service selection Agent finds one or more suitable service agents from the meta data repository for a given task as per the workflow specification. Service agents construct the advertisement message in XML. Such an advertisement message is as follows:

```
<?xml version=”1.0” encoding=”UTF-8”?>
<Message>
<Message Type>Advertise</Message>
<Repository> yellowpages <./Repository>
<AgentIdentity>
<AgentName>OrderItem1Agent</AgentName>
<AgentAddress>203.4.5.101.2323</AgentAddress>
<AgentType>service</AgentType>
```

```
</AgentIdentity>
<AgentCapability>
<SupportDTD>
http://awascm.gita.cse.edu.in/supply_chain.dtd
</SupportDTD>
<SupportService>
http://SupplyChain.gita.cse.edu.in/OrderItem1.xml
</supportServices>
</AgentCapability>
</Message>
```

(Advertisement Message.xml)

3.4 Process Agent

The main task of the process agent is to transform a workflow specification into a workflow instance. It gets the workflow specification from the interface agent and integrates the service agents to execute the workflow. The various responsibilities it is assigned with are

1. The process agent for a particular task in the workflow queries to the service selection Agent and finds the relevant available service agents. Then it negotiates with the service agents about task execution. When the process agent receives many choices to perform a particular task, it allows the user to do selection among the available service agents. Finally, it makes connections to that service agent and assigns the task specifications to it.
2. Once a task is assigned to a service agent, a monitor agent is then created and sent to the task execution site. The process agent instantiates the task ECAM rules only after the monitor agents are migrated to the task execution sites .The process agent do the workflow execution according to the workflow's ECAM rules. It coordinates the tasks to achieve a certain goal and also enable, disable or suspend the tasks according to the workflow ECAM rules.
3. When they do not have the ability to process a task, it forwards the workflow specifications to another process agent. For example, a process agent specialized in workflow implementation may not be able to process a supply-chain workflow.
4. The process agent during the workflow execution receives all the event messages from the monitor agents. This makes the user to know the status of the workflow instance without having to subscribe to any of the service agents

3.5 Monitor Agent

A monitor agent monitors the actual execution of a given task at the site of the service provider. Its functionalities are:

1. During process instantiation the monitor agent supervise the task execution at the corresponding service provider's site where the task is actually executed.
2. It downloads the ECA rules of the corresponding task from the process agent which will guide the service agent in executing the task.
3. It updates the execution plan based on the changes, for example when a service agent fails while executing a task. In such a case the monitor agent can be called back and updated by the process agent and then can re-migrate to continue its monitoring function at the local site of the service provider.
4. When a service agent finished certain action during the execution of a task, it informs the monitor agent regarding its action. Then the monitor agent informs the process agent and other monitor agents about the execution status of the task. The process agent then forwards such messages to the interface agent so as to make the user aware of the progress of workflow execution.

4 EXECUTION OF Cross-organization workflows

In order to execute a workflow, the above five agents form a community according to the particular workflow specification, also the community decides the workload of individual agents as well as the quality of the service they should provide. Once the execution of the workflow completes the agent community disbands.

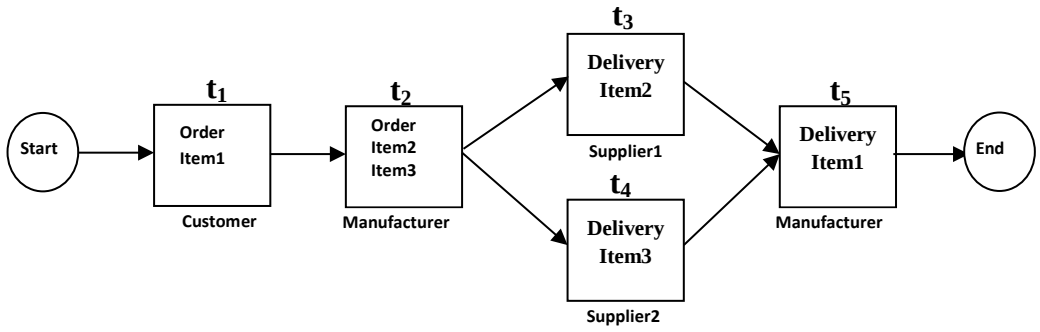


Figure 5: SCM planning Workflow

4.1 An Example

Consider the workflow of a typical Supply Chain Management (SCM) as shown in Figure 5. It involves interaction among agents from a customer company, Manufacturer Company, and supplier company. The business workflow has to execute the following tasks:

OrderItem1 task: where a customer, order for an item called as Item1 to a manufacturer.

OrderItem2Item3 task: where the manufacturer orders for Item2 and Item3 to Supplier1 and supplier2 respectively, in order to Produce Item1.

DeliverItem2 task: where supplier1 supplies the raw material, Item2 to the manufacturer.

DeliverItem3 task: where supplier2 supplies the raw material, Item3 to the manufacturer.

ProduceItem1 task: where the manufacturer produce Item1 and supplies to the customer.

We can define the workflow W for the SCM process as follows:

Workflow W = {T, E_w, R_w}, where:

T= {t_1, t_2, t_3, t_4, t_5}

E_w = {e_{w1} ,e_{w2}, e_{w3}}, where

e_{w1} :*W$\Longrightarrow$ $\Delta t1 \wedge \Delta t2$

e_{w2} : (t_1.result == success) $\wedge$ (t_2.result == success)$\Longrightarrow$ $\Delta t_3 \wedge \Delta t_4$

e_{w3} : (t_3.result==success)$\wedge$ (t_4.result==success)$\Longrightarrow$ Δt_5

Then the tasks:

t_1= {N_1, O_1, E_{t1}, D_1, R_{t1}} ,where

N_1 is customer Order Process

O_1 is OrderItem1 defined as:

States :{callForBid, Negotiate, Assign, ReceiveDelivery, ReleasePayment}

Operations

Negotiation :{CallForBid, Negotiate}

Assignment :{ Negotiate, Assign}

E_{t1} ={e_{11},e_{12},e_{13}},where

e_{11} : (t_1.Item1.state==CallForBid)$\Longrightarrow$ ($\hookrightarrow$ t_2)

e_{12} : (t_2.Item1.state==Bid) $\Longrightarrow$$t_1$.Item1.Negotiate

e_{13} : (t_1.Item1.state==Assign) $\Longrightarrow$$t_2$.Item1.ReceiveOrder1

D_1=20 Sept. 2013

R_{t1}=Null

t_2={N_2,O_2,E_{t2},D_2, R_{t2}} ,where

N_2 is ReceiveItem2Item3 Process

O_2 is Manufacturer OrderItem Process, defined as:

States :{ Bid, ReceiveOrder1,OrderForItem, ReceiveItem,ReleasePayment}

Operations

Receive-Order :{Bid, ReceiveOrder1}

Receive-Item :{OrderForItem, ReceiveItem}

Payment :{ ReceiveItem, ReleasePayment}

E_{t2} ={e_{21},e_{22},e_{23}},where

e_{21} : (t_2.Item1.state==Bid)⟹ (↪ t_1)

e_{22} : (t_2.Item1.state==ReceiveOrder1)⟹t_2.Item3.OrderForItem⋀ t_2.Item4.OrderForItem

e_{23} : (t_2.Item2Item3.state==ReceiveItem) ⟹t_2.ReleasePayment

D_2=20 Sept 2013

R_{t2}=Null

t_3= {N_3, O_3, E_{t3},D_3, R_{t3}} ,where

N_3 is Supplier1 Process

O_3 is DeliveryItem2 Process, defined as :

States :{ReceiveOrder, DeliveryItem, ReceivePayment}

Operations

Delivery-Item :{ReceiveOrder, Deliveryitem}

Send-Invoice :{DeliveryItem, SendInvoice}

ReceivePayment :{SendInvoice, ReceivePayment}

E_{t3} ={e_{31},e_{32},e_{33}},where

e_{31} : (t_2.Item2.state==ReceiveOrder)⟹ t_3.Item2.DeliveryItem

e_{32} : (t_3.Item2.state==SendInvoice)⟹(↪ t_5)

e_{33} : (t_5.Item2.state==ReleasePayment) ⟹t_3.Item2.ReceivePayment

D_3=21 Sept. 2013

R_{t3}=Null

t_4= {N_4, O_4, E_{t4}, D_4, R_{t4}} ,where

N_4 is Supplier2 Process

O_4 is DeliveryItem3 Process, defined as:

States :{ReceiveOrder, DeliveryItem, SendInvoice, ReceivePayment}

Operations

Delivery-Item :{ReceiveOrder, Deliveryitem}

Send-Invoice :{DeliveryItem, SendInvoice}

ReceivePayment :{ SendInvoice, ReceivePayment}

E_{t4} ={e_{41},e_{42},e_{43}},where

e_{41} : (t_4.Item3.state==ReceiveOrder)⟹ t_4.Item3.DeliveryItem

e_{42} : (t_4.Item3.state==SendInvoice)⟹(↪ t_5)

e_{43} : (t_5.Item3.state==ReleasePayment) ⟹t_4.Item3.ReceivePayment

D4=21 Sept. 2013

R_{t4}=Null

t_5= {N_5, O_5, E_{t5}, D_5, R_{t5}} ,where

N_5 is Manufacturer DeliveryItem Process

O_5 is DeliveryItem1 Process, defined as:

States :{ReceiveItem2, ReceiveItem3,Produce,Delivery,ReceivePayment}

Operations

Produce-Item1 :{ReceiveItem2, ReceiveItem3,Produce }

Send-Invoice :{DeliveryItem,SendInvoice}

ReceivePayment :{SendInvoice,ReceivePayment}

E_{t5} ={e_{51},e_{52},e_{53}},where

$e_{51:}$(t_5.ReceiveItem2.state==success)∧(t_5.ReceiveItem3.state==success)⟹t_5.Item1.Produce

e_{52} : (t_5.Item1.state==Delivery)⟹ t_1.Item1.ReceiveDelivery

e_{53} : (t_1.Item1.state==ReleasePayment) ⟹t_5.Item1.ReceivePayment

D_5=22 Sept. 2013

R_{t5}=Null

4.2 Composition Procedure

The workflow integrator is used to specify the supply chain workflow W. An instance of the workflow is executed as described below.

4.2.1 Parsing Workflow Specifications and Searching for Service Agents

The process Agent parses workflow specifications W that consists of five tasks: t_1, t_2, t_3, t_4, and t_5.The main responsibility of the process agent is to assign the different tasks t_1, t_2, t_3, t_4, t_5, to the available service agents on the Web. The process agent queries the service selection Agent for the appropriate service agents which can carry out these tasks t_1, t_2, t_3, t_4, t_5. The

content of the query message that the process agent sends to the service selection Agent for a task t_1, is as given below:

Message Type : query
Agent Identity : ?
Group Identity : ?
Task Object : t1.customerOrder
Search : all
HOP : 3

(Query Message)

When the service selection Agent receives such a message it Searches everywhere in its yellow pages and catalogue repositories, as the query indicates to search in all repositories of the service selection Agent. Here the hop count is set to 3, which indicates that the request will be propagated to at least three service selection Agents. The result is then returns to the process agent as shown below.

Message Type: reply
Yellow page: (ip=172.16.1.7,port=2034, agent name=SupplyItem1)
Catalogue: (ip=230.15.1.7, port=2221, group name=SupplyItem)

(Result Message)

The above message indicates that the process agent discovers one service agent and one group service agents which can execute the task t_1.

4.2.2 Assigning Tasks

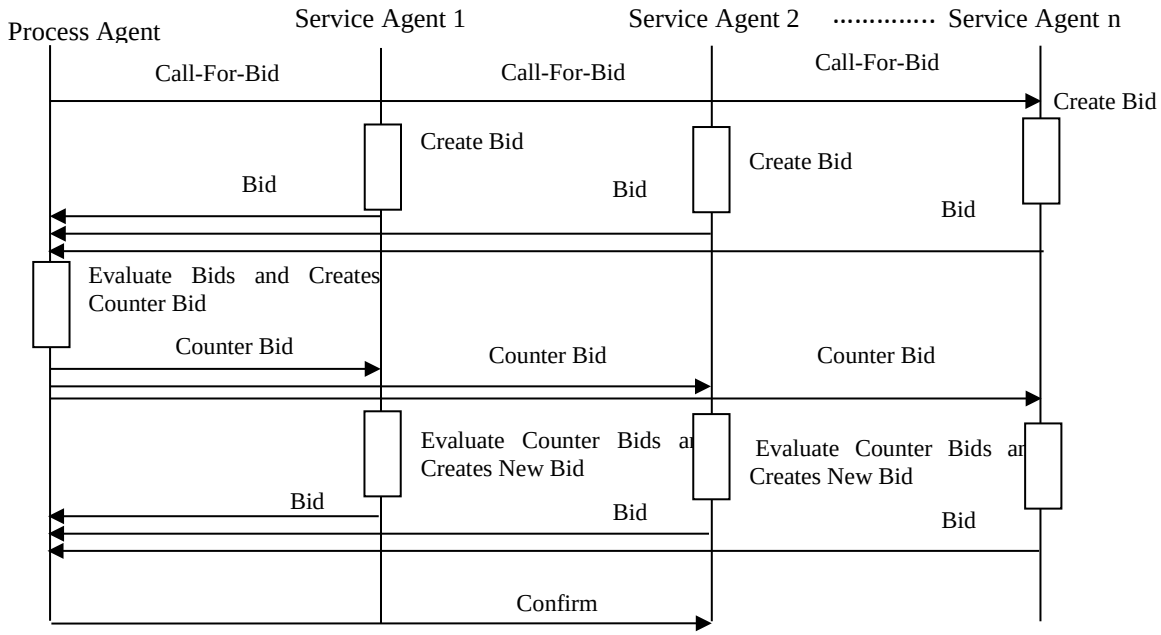


Figure 6: Negotiation Protocol

A task can be assigned to the service agent in two phases.

- Negotiation Phase:

The negotiation protocol is as shown in the above figure 6. In this phase, the process agent sends a Call-for-Bid message as shown below to all the service agents.

Message Type: Call-For-Bid
Sender: 203.5.15.21: 1234: Process-agent
Task Object: t1.customerOrder
Price: ?

(Call-For-Bid Message)

When the service agents receives the Call-For-Bid message from the process agent then depending upon the task specification, it decides whether to respond or not with a Bid in XML. Example of such a Bid is as given below:

```
<?xml1 version=”1.0” encoding =”UTF-8”?>
<!DOCTYPE Bid SYSTEM “bid.dtd”>
        <Bid>
         <TaskBid>
      <Task>Supply_Item1</Task>
      <Cost>200000 Rupees </cost>
     <WorkDuration>2-Days</WorkDuration>
          </TaskBid>
<AcceptDeadline>20/10/2013</AcceptDeadline>
</Bid>
```

(XML Respond Message)

- Task Assignment Phase:

After the process agent receives the bids, it sends a counter bid to the service agents. In the counter-bid the service agent bargains the execution cost and work duration of a task. Upon receiving the counter-bid from all the service agents, the process agent decides and assign to the best service agent based on minimal execution cost and task execution duration. Then the process agent sends task assignment message as given below to the appropriate service agent. After the service agent receives the assignment message, it sends a confirmation message to the process agent.

Message Type : assignment
Sender : 203.5.15.21: 1234:Process-agent

Task : tl

Receiver : 203.5.1.2: 1334:Supplier-agent

(Task Assignment Message)

4.2.3 Monitor Agents and their activities

The process agent creates Monitor agents that must be deputed to the site of service agents. The monitor Agent gets migrated to the site of the service agent where the actual task is executed. Once the monitor agent arrives at the service agent site, it will send a confirmation message to the process agent to indicate that it is ready to monitor the tasks.

When the user defines the ECAM rules, they (ECAM rules) do not have any execution context information and cannot be executed. Once the monitor agents have migrated to the task's execution site, the rules can be instantiated by the process agent. For instance, assuming that the tasks t_1,t_2,t_3,t_4,t_5 have been assigned to service agents *OrderItem1-agent, OrderItem2-agent, DeliverItem2-agent, DeliverItem3-agent, ProduceItem1-agent* and *monitor agents* MA1, MA2, MA3, MA4, MA5 have migrated to tasks' execution sites respectively, then the following ECAM rule is instantiated.

e_{12} :(t_2.Item1.state==Bid) $\Longrightarrow t_1$.Item1.Negotiate

can be instantiated to

(t_2(MA2).Item1.state==Bid) $\Longrightarrow t_1$(MA1).Item1.Negotiate

The monitor agent downloads the ECAM for the instantiated task. Once all the tasks have been assigned to the service agents, all the monitor agents have been created and migrated to the tasks' execution sites and have downloaded the instantiated task ECAM rules then the workflow agent society is ready to execute the cross-enterprise workflow instance. The composed agent society is not a static entity. It might dynamically change during workflow execution. Therefore if the assigned service agent fails to execute the task then the process agent can locate an alternate service agent and execute the workflow.

4.3 Distributed Enactment of a Cross-Organization Workflow

The workflow engine acts as a central task coordinator. Based on the workflow specification, it creates process instance and subsequently the list of different tasks and also controls the execution of the tasks and coordinates task execution as well. The disadvantage with such a central control model is that when there is an exception occurs during the coordination and the task execution it results in a sole point of failure; when an anomaly occurs at the runtime, central server needs to suspend the whole workflow instance to handle it.

We put forward a distributed coordination approach which adopts the dynamic agent technology. We segregate the task control flow and the task coordination: the process agent are responsible for the task execution flow control while the monitor agents do the task coordination for the task those are to be distributed in all the task execution sites. Here to

demonstrate, the working principle of distributed coordination approach we consider a Simple example. Here, we assume workflow agent-community has been formed for the workflow specification W, five tasks have been assigned to three types of service agents (Customer-agent, Supplier-agent, Manufacturer-agent). Five monitor agents MA1,MA2,MA3,MA4,MA5 have been created and deputed to each task's the execution sites , all the tasks' ECAM rules have been instantiated and downloaded by the monitor agents.

Starting the Workflow:

At the start, the process agent will execute the first ECAM rule that is:

e_{w1} : *W$\Longrightarrow \Delta t_1(MA1) \wedge \Delta t_2(MA2)$

The action Δt_1(MA1) and Δt_2(MA2) results in sending messages to monitor agent MA1 and MA2 which informs the service agents, viz., Customer-agent and Manufacturer-agent to start executing their tasks.

Executing the Task t_1 to t_5 :

Once the customer orders for an item(Item1) then the Customer-agent begin to execute its task and also send the enable signal t_2(MA2) message(from process agent) to all the Manufacturer-agent. When the task is assigned to a manufacturing agent , then the manufacturer, order for Item2 and Item3 to supplier1 and supplier2 represented with the task $t_3$and t_4.The monitor agent t_3(MA) and t4(MA) will inform the service agents supplier1 and supplier2 to execute their tasks. After the manufacturer agent gets the results from the supply-Agents, supplier1 (t_3) and supplier2 (t_4) then, the manufacturer-agent will finish the workflow with the monitor agent t_5 (MA) and pass the result to the customer. The monitor agent periodically pings the service agents just to check whether any of them fails or not. If any of the service agent has exhausted the estimated execution time and yet not completed the task, in such case the monitor agent pings it more frequently, because such service agents are more likely to fail. Service agents also sends message to the process agent, when they have completed certain activities during their execution of a task. Then the process agent forwards such message to the interface agent, so as to make the user to know the progress of workflow execution. The process agents also keeps log of execution results of all the tasks which may require selecting the execution plan in future. Once the workflow has been finished then the agent society will dismiss the workflow and a new agent community will be formed to build a new workflow instance.

5 Prototype Implementation

A prototype implementation of the agent based workflow as depicted in figure 4 has been implemented. The prototype is deployed by using Enterprise Java Beans (EJB). Agent communication channel is implemented using Java Shared Data Toolkit (JSDT). The Service agents and Interface agent are implemented using Java.

In the service agent, the service wrapper provides an interface to the actual business process of an organization. Service description is an XML document that describes the service provided by the business process. Service advertiser registers the services into the service selection Agents. Service Negotiator negotiates with the integration agent about service execution.

In the service selection Agent service registry and Query Engine are implemented as Entity Beans. We use Oracle 8i Database as meta-data repository to store information about the service (Such as content, type, location etc).Each XML document is stored in ORDBMS. The Query Engine takes a query from the process agent and translates it into SQL query. Here we use Oracle XML SQL Utility for java to pass an SQL-Query to the underlying Oracle8i Database. Then the results are sent to the utility which then embed it with XML .This result is a set of service agents descriptions. In the process agent the Locate-service is implemented as entity bean and workflow-Execution is implemented as Session Beans. In the Monitor agent execution-status-of –workflow and Service negotiator is implemented as Session Beans.

6 Scenario

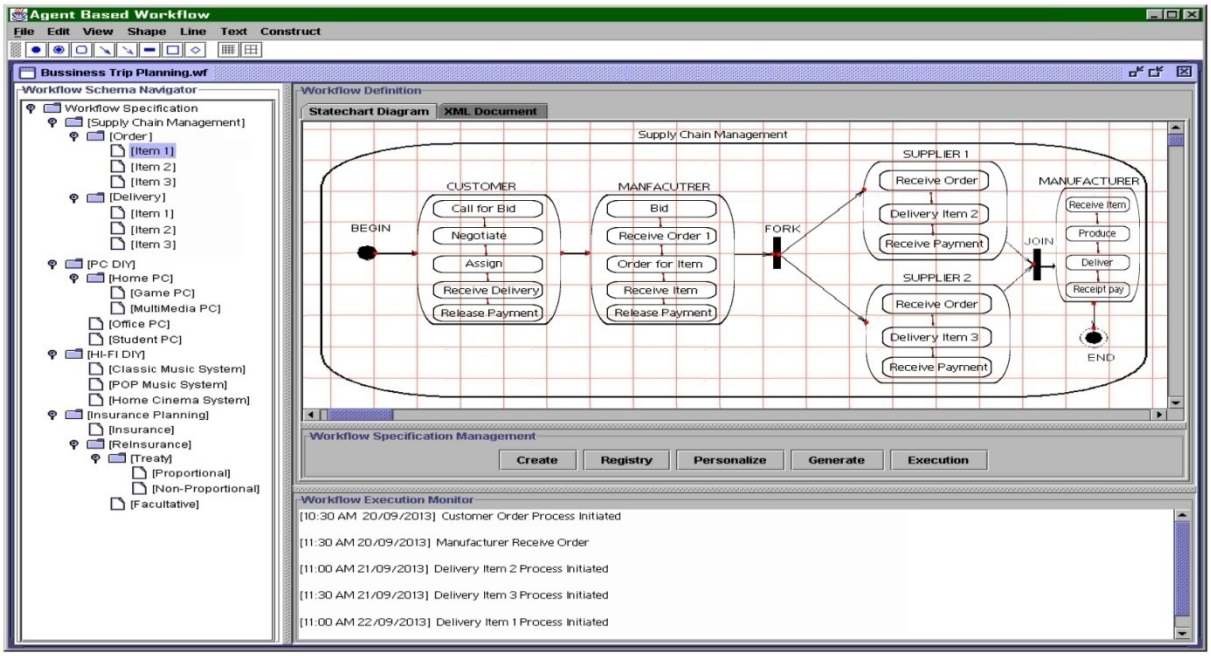


Figure 7: Scenario of Supply Chain Management

We consider the SCM-workflow to explain the use of agent based workflow. The workflow schema consists of five tasks which are OrderItem1 (t1), OrderItem2Item3 (t2), DeliveryItem2 (t3), DeliveryItem3 (t4), DeliveryItem1 (t5).The workflow specification can be explained by taking the business process of M/s HP Ltd, to supply HOME PC,OFFICE PC and STUDENT PC to one of its valued customer. In order to fulfil the order it needs the raw materials from M/s

Fablin Retailer and M/s Radiant Suppliers. The various tasks carried out during the entire supply chain can be explained as below:

The Order PC DIY task where the customer orders for different types of PC to M/s HP Ltd.

The OrderRaw Materials task where M/s HP Ltd orders the raw materials to M/s Fablin Retailers and M/s Radiant Suppliers in order to satisfy client's requirement.

#The DeliverElectronicsRawMaterial task where the M/s Fablin Retailers supplies the raw materials (Electronics Items) to M/s HP Ltd.

The DeliverCabinetRawMaterial task where the M/s Radiant Suppliers supplies raw materials (Cabinets and other mechanical Items) to M/s HP Ltd.

The Produce PC DIY task will be carried out only when M/s Fablin and M/s Radiant supplies Electronics and Mechanical items to M/s HP Ltd.

We created 16-service agents namely a1, a2, a3,.....a16 all of which registered with the service selection Agent. In the following portion we will describe how to define the workflow schema, and then create workflow instance and then to execute it by using agent based workflow architecture.

Describing workflow schema: A workflow panel is provided by the interface agent present in the upper right panel as shown in figure 7. The process composer with the help of this workflow panel draws the UML state chart diagram that defines the workflow schema. These workflow schemas are organized using domain specific hierarchy. There are leaf and non-leaf

For the nodes in the left panel, the leaf nodes represent the schema of specific workflows. For an instance (as shown in figure 7) there are four workflow domains namely Supply Chain Management, PC-DY, HI-FI-DIY, Insurance planning. Home PC is a sub-domain of PC-DY. This sub-domain in turn has workflow schemas Game PC and Multimedia PC. Every non-leaf node in the hierarchy represents a set of workflow schema of a particular domain.

Create Workflow Instance: It is possible for a user to access the workflow schema with the help of workflow Schema navigator panel. When the user clicks on the leaf node the respective UML state chart will be displayed on the workflow definition panel. An instance of the workflow can be created by clicking on the create button on the workflow management panel. In order to execute the workflow the user gives the appropriate parameters like Item1 and delivery date. Afterwards the user can generate the XML document (that describes the workflow) by clicking on the generate button on the workflow management panel. Once the user clicks the execution button then the workflow (XML document) will go to the process agent to execute the workflow

Dynamic Integration: The integration agent parses the XML document into five tasks as required by our SCM. For each task it queries the service selection Agent for the relevant service agents. Based on the query results from the process agent we separate each group of

service agent based on the task-group they are responsible to perform .For example in our supply chain process

$T_1=\{t_1\},T_2=\{t_2,t_3\},T_3=\{t_1,t_3\},T_4=\{t_2,t_4,t_5\},T_5=\{t_5\},A_1=\{a_1,a_2,a_3\},A_2=\{a_4,a_5,a_6,a_7\},A_3=\{a_8,a_9\},A_4=\{a_{10},a_{11},a_{12},a_{13}\},A_5=\{a_{14},a_{15},a_{16}\}$.Since there are five set of task sets, the process agent creates five negotiation sessions to negotiate with the service agents. The process agent creates a set of execution plans based on the available bids but only one execution plan is selected and executed.

7 Related work and Conclusion

Approaches related to integrating business processes exist in many fields including component-based E-commerce systems, cross-organization workflow and software agents.

An early solution to B2B integration is Component-based E-commerce systems [14], typically rely on distributed object frameworks such as CORBA and DCOM. Various organizations present their high level services as business objects. The combination of middleware technologies, and the business objects, provides services. It is suitable for integration of small number of tightly coupled applications.

Other advanced approaches to B2B integration is the cross-organization workflow. Related projects in this area includes the project at MCC[15] where they proposed a Service Oriented Process model and the idea is to be able to provide a framework for flexible, plug and play approach to cross-organization workflow composition. However they could not addressed the issue of brokering and selection of services that goes beyond what is stated in the service inter-faces.

The use of software agents is one of the promising technologies in B2B integration and E-commerce applications. The use of agents in automating a single organization WFMS have been discussed in [16][17]. In [16], each workflow is represented by multiple personal agents, actor agents and authorization agents. These agents act as personal assistants which carry out actions on behalf of the workflow participants and facilitating interaction with other participants or organization specific WFMS. In [17], the MAS architecture consists of a number of independent agencies. Each single agency consists of a set of subsidiary agencies which is controlled by an accountable agent. A single agent is able to execute one or more services. These atomic agents can be united to form complex services by adding ordering constraints and conditional control. However, neither [16] nor [17] speak about the agent technology to create workflow execution engine dynamically. The workflow processing logic is hard-coded and thus it is difficult to reuse this workflow execution engine, for other business processes.

Even though a little work has been done for agent integration, they can be extended successfully to include integration capabilities. In doing so, the integration solution can take advantage of the agents' negotiation capability and the ability to adapt to dynamic changes in environments.

In our approach, we have implemented agent based workflow system for dynamic B2B integration. In our approach the agent-community for specific workflow is optimally and automatically composed based on the context of workflow execution and can self-adapt and react to changes during the execution. We show how the workflow agent-community gets constructed by taking the example of supply chain management. We illustrate how the agent community executes the workflow specification and modifies themselves during the execution of the workflows. We also used monitor agents for monitoring cross-enterprise workflows. This facilitates the end user to know the status of the workflow instance.

REFERENCES

[1]. K. Kogan, A. Herbon, "A supply chain under limited-time promotion: The effect of customer sensitivity," European Journal of Operational Research, Vol. 188, 2008, pp. 273-292

[2]. C. Lin, H. Chiu, P. Chu. Agility index in the supply chain. International Journal of Production Economics, Vol. 100, No. 2, 2006, pp. 285–299.

[3]. Simchi-Levi, P. Kaminsky and E. Simchi-Levi, Managing the Supply Chain – The Definitive Guide for the Business Professional, New York: McGraw-Hill, 2004.

[4]. D. Simchi-Levi, P. Kaminski, Designing and managing the supply chain–concepts, strategies and case studies, New Jersey: McGraw-Hill, 2006.

[5]. B. Manouvrier, L. Ménard,Application Integration,EAI, B2B, BPM and SOA ,John Wiley & Sons, Inc., pp. 134-142,2008.

[6]. D. Georgakopoulos, editor. Information Technologyfor Virtual Enterprises, Proc. of the 9th Int. Workshop on Research Issues on Data Engineering. IEEE Computer Community, March 1999.

[7]. T.E rl, Service-Oriented Architecture Concepts , Technology , and Design, Prentice Hall professional Technical Reference ,pp. 33-37, 2009.

[8]. T.E rl, Service-Oriented Architecture: A Field Guide to Integrating XML and Web Services, Prentice Hall professional Technical Reference, pp. 48-50, 2005 .

[9]. F.Curbera, M.Duftler, R.Khalaf,W.Nagy,N.Mukhi, S.Weerawarana, IEEE Internet Computing Magazine, "Unraveling the Web Services Web An Introduction to SOAP, WSDL, and UDDI", 2002.,Avialble : http://ieeexplore.ieee.org.www.ezplib.ukm.my/servlet/opac?punumber=4236, (Last accessed: 12 July 2011)

[10]. P. Massimo, K. Sycara, T. Kawamura, Delivering Semantic Web Services, Proceedings of the WWW2003, Budapest, Hungary, 2003 May.

[11]. M. Fox, M. Barhuceanu, and R. Teigen, "Agent oriented Supply-chain Management," The International Journal of Flexible Manufacturing Systems, Vol. 12, pp.165-188, 2000.

[12]. J. Gou, X. Yang, W. Dai, " On Demand Integration of Dynamic Supply Chain Application Based on Semantic Service Oriented Architecture" , IFIP International Federation for Information Processing, Volume 254,Research and Practical Issues of Enterprise Information Systems II Volume 1, eds. L. Xu, Tjoa A., Chaudhry S. (Boston:Springer), pp. 589-598 , 2007.

[13]. T. Hess, L. Rees, and T. Rakes, "Using Autonomous Software Agents to Create the Next Generation of Decision Support Systems," Decision Sciences, Vol. 31, No. 1, pp. 1-31,2000.

[14]. A. Dogac, editor. ACM SGMOD Record: Special Issue on Electronic Commerce, ACMSIGMOD RECORD. ACM, December 1998.27(4).

[15]. D. Georgeakopoulos, H. Schuster, A. Cichocki, and D. Baker. Managing process and service fusion in virtual enterprises. Information System, Special Issue on Information System Support for Electronic Commerce, 24(6):429-456 1999.

[16]. J. Chang and C. Scott. Agent-based workflow:TRP support Environment (TSE). Computer Networks and ISDN Systems, 28(7-11):1501-1511, 1996.

[17]. N. R. Jennings, P. Faratin, M. J. Johnson, T. J. Norman, P. O'Brien, and M. E. Wiegand. Agent- based business process management. International Journal of Cooperative Information Systems, 5(2&3): 105-130,1996.

TNC Transactions on Networks and Communications
SOCIETY FOR SCIENCE AND EDUCATION UNITED KINGDOM
VOLUME 2, ISSUE 4
ISSN: 2054 - 7420

Social Networks: A Curse or a Blessing? (A Case Study of Selected Students from Auchi Polytechnic)

[1]Uduiguomen Usifoh Collins, [2]Agwi Uche Celestine and [1]Aliu Nefishetu Faith
[1]Department of Computer Science, Auchi Polytechnic, Auchi, Edo State, Nigeria.
[2] Department of Mathematical and Physical Sciences, Samuel Adegboyaga University, Ogwa, Edo State, Nigeria.
mailusifoh@yahoo.com ; ucheworld2002@yahoo.com ; aliunefishetufaith@yahoo.com

ABSTRACT

This paper presents the findings from an investigation into the question whether a social network is a blessing or a *curse. We used a sample population of 320* students at Auchi Polytechnic, Auchi in Edo Sate Nigeria as our case study. This investigation was borne out of the ever-increasing interest that a lot of people are expressing in their fraternity with the various social networks and the obvious opportunities and prospects as well as the virtues and vices these social networks portend. Social networks are like legal tenders; on their own, they are neither good nor bad. What defines them and gives them their characteristics are what a user does with them. A lot of unsavory activities (ranging from fraud, identity theft to outright blackmail) have been known to be carried out using social networks as a platform but in retrospect, varying degrees of positive achievements (such as building of mutually beneficial relationships and ties, reestablishment of lost contacts and effective communication) has also been recorded using social networks. From the investigation that we carried out, it was observe that social network can serve as a blessing and it can also serve as a *curse depending on how and what a user use it for.*

Keywords: Social networks, Facebook, Twitter, 2go, Eskimi, Naijapals, Gnaija.

1 Introduction

Social networks like Facebook, twitter and others have provided a platform where people communicate, make friends, meet old friends, share ideas, share photos and so on. Social media is all around us and it has come to encompass every aspect of our lives. Social networks have been very useful to almost everyone across the globe especially the youth. These social sites have created the platform for both the young and old to do so many things which would have been impossible without the presence of these sites. Many making new friends, others finding old friends and reconnecting. Some users have found boyfriends and girlfriends and

DOI: 10.14738/tnc.24.405
Publication Date: 24th August 2014
URL: http://dx.doi.org/10.14738/tnc.24.405

even life partners thus to talk of a few. Business men and women are using these sites to advertise and market their products and services with ease. Social media has contributed immensely to the development of arts especially musicians. Musicians are using social media sites to interact with their fans and also putting up download links for people to download their music. Aside musicians, prominent pastors also use these sites to win souls for Christ. In the recently held general elections in the USA and in Nigeria, facebook and twitter were particularly the dominant social sites [1]. Prior to the gubernatorial July 14th, 2012 election that was held in edo state, nigeria, a lot of persons and corporate bodies were using the facebook social network to advice stakeholders on various issues as they relate to the conduct of the election [2].

Generally, a lot of interesting activities takes place on these social sites daily. Among all these advantages lies the bad side of social networks. Social media have been of very good use to society since its invention but there have been some abuses or disadvantages in relation to these sites. Impersonation has been a common abuse of the social media which some fraudulent minds has been using to misrepresent themselves to others especially celebrities to perpetrate fraud on others. Also social vices such as prostitution, fraud among others have always existed [1]. Akinwale cited a case that involved one Cynthia Ozokogu, 24, the last child and only daughter of major general Ozokogu (rtd). She was killed on July 22, 2012 in a hotel in Festac, Lagos state by so-called friends that she met on facebook. Her alleged killers have been arraigned for murder [3].

The Associated Press reported on the 1st of May, 2013 that in the early days of the evolution of social networking websites there were four major social networking sites in common use. They were Facebook, LinkedIn, MySpace and Twitter. Facebook, was introduced in February 2004 and is one of the most popular social networking websites today. This website was originally open only to students at Harvard University, but this no longer holds true. As at March 1, 2013, Facebook said it had 1.11 billion people using the site each month.

Linkedin was started in May 2003, and is less focused on social networking. This tool is used to network within a desired professional atmosphere and allows individuals to build professional, career-oriented relationships. Linkedin is the most business-oriented of the four big social networking websites. Hempel hinted that as of June 2013, LinkedIn has more than 225 million members in over 200 countries and territories [5].

MySpace was founded in August 2003. It is more directed toward the musically inclined. This social networking website is no longer solely for social networking. It is more about connecting different bands and groups, rather than connecting individuals. The membership for MySpace is about 126 million.

2 Background to the Study

From the Auchi Polytechnic student handbook of information, Auchi Polytechnic, Auchi is a government tertiary institution owned by the federal government of Nigeria. The polytechnic is located in Edo State of Nigeria. The polytechnic is home to students from different socio-economic background and different ethnicities within Nigeria. The Polytechnic was established to provide for studies, training and development of techniques in applied sciences, engineering, art and business as well as in other spheres of learning, cultural development and the inculcation of good character which are integral parts of education and training. The unity in diversity that the Polytechnic exudes is apparent in all segments of her operations [9]. Though the Polytechnic has its share of challenges that ranges from infrastructural deficiency to inadequate manpower to tackle the rigors that are prevalent in similar institutions of learning, most students and staff are still actively involved in the use of social networks here for one activity or the other.

From a new demographic breakdown by the Pew Research Institute, it was shown that the majority of social media users lives in the city and prefers Facebook as their main medium. The breakdown, which was based on a late 2012 survey, also showed that young adults are, unsurprisingly, the most likely group to use major social media. While internet users under the age of 50 are more likely to use any social networking site, those in the 18-29 age group are the most likely at 83 percent [10].

Taking a clue from the result of the Pew Research Institute survey, we decided to do a survey in the Polytechnic to ascertain possible outcome from our students and as it turned out, the cooperation was massive. Most of the students in the Polytechnic had one or more social network account.

3 Methodology and Materials

The data used was derived from the responses that were received from a total of 320 respondents who were able to properly answer and return the questionnaires that were administered. Initially, 350 questionnaires were prepared but in the course of their administration and collation only 320 were selected as meeting the minimum standard that was set for the questionnaire acceptability. One of the criterion that was used to screen out some respondents was their response to the question “Do you own an account with any social network site like Facebook, Twitter, 2go or any other?” Ten questions including the benchmark question above were however contained in the questionnaire to elicit information from the respondents.

For the analysis of data we used the simple percentage method. The decision rule that was used is the acceptance of majority of opinion or high percentage. In view of the nature of this

investigation, detailed data representation of the responses we got from six (6) out of the ten (10) items in our questionnaire are presented below.

Table 1 shows the response we got when we asked from the sample population the question "Which social network do you use?"

Question	Social network	Respondents	Percentage (%)
Which social network do you use?	Facebook	192	60
	Twitter	49	15.31
	2go	69	21.56
	Any other	10	3.13

Table 2, presented the response we got to the question "How many social network accounts do you have from the entire social network combined?"

Question	Options	Respondents	Percentage (%)
How many social network accounts do you have from the entire social network combined?	1-3 accounts	220	68.75
	4-6 accounts	85	26.56
	7 and above	15	4.69

Table 3 indicated the reasons why virtually all our respondents had more than one social network account.

Question	Options	Respondents	Percentage (%)
Why do you have more than one social network account?	Access medium	77	24.06
	Distribution of contacts	220	68.75
	Access restriction	23	7.19

Table 4 shows a cross-section of the responses we got to the question on "How often do you use your social network account?"

Question	Options	Respondents	Percentage (%)
How often do you use your social website account(s)?	Daily	242	75.62
	Weekly	42	13.13
	Monthly	21	6.56
	Once in two months or longer	15	4.69

Table 5 is a representation of the values that we gathered in response to the question "What is your opinion on this? Is social network a curse or a blessing?"

Question	Opinion	Respondents	Percentage (%)
What is your opinion on this? Is social network a curse or a blessing?	Social network is a blessing	90	28.13
	Social network is a curse	25	7.81
	Social network is neither a curse nor a blessing	205	64.06

Table 6 contains values that were gathered from the response to the question "Which social network will you rank the best?"

Question	Social networks	Respondents	Percentage (%)
Which social network will you rank the best?	Facebook	160	50
	Twitter	70	21.88
	2go	80	25
	Any other	10	3.12

4 Results and Discussions

From the data that was presented in Table 1 above, 192 of the respondents representing 60% of the sample population indicated that they use Facebook, 49 respondents representing 15.31% said they used Twitter, 69 respondents representing 21.56% said they use 2go and 10 respondents representing 3.13 said they use other social networks like hi5, Naijapals, Eskimi and Gnaija.

From Table 2, 220 of the respondents, representing 68.75% of the sample population opined that they owned from 1 to 3 social network accounts, 85 respondents representing 26.56% indicated that they owned between 4 to 6 social network accounts while 15 respondents representing 4.69% indicated that they owned more than 7 social network accounts.

A look at Table 3 showed that 77 respondents representing 24.06% of the sample population indicated that access medium was the major reason that motivated them to owe more than one social network account, 220 respondents representing 68.75% opined that the reason why they have more than one account is because of the distribution of their contacts who are using other social networks, 23 respondents representing 7.19% cited access restriction that they encountered at one time or the other as the motivating factor that made them to create and use different social network accounts.

From Table 4, 242 of the respondents representing 75.62% of the entire sample population said they used their social network account daily, 42 of the respondents representing 13.13% said they use their account once a week, 21 respondents representing 6.56% said they use their social network account(s) once in a month while 15 respondents representing 4.69% indicated that they use their social network account(s) once in two months less frequently.

Table 5 showed that 90 of the respondents representing 28.13% of the sample population indicated that Social network is in their opinion a blessing, 25 respondents representing 7.81% agreed that Social network is a curse while 205 of the respondents representing 64.06% were of the opinion that Social network is neither a curse nor a blessing.

Table 6 showed that out of the sample population of 320 respondents, 160 respondents representing 50% said they rank Facebook as their best social network, 70 respondents representing 21.88% ranked Twitter as their best social network, 80 respondents representing

25% ranked 2go as their best social network while a total of 10 respondents representing 3.12% ranked any other Social network like Naijapals, Eskimi or Gnaija as their best in rank.

From the afore presented results, we were able to observed that all the respondents had more than one social network account for various reasons ranging from access medium, distribution of contacts to access restriction. Some of the respondents opined that they were having difficulty using some of their internet-enabled mobile phones to access some of their social network accounts like twitter. They complained that using their phones, access speed to twitter was very slow.

5 Conclusion and Recommendations

Arising from the findings of this work, is the fact that though a minimal size of the population (7.81%) considered social networks as a curse, it is staggering to realize that an enormous size of the sample population (64.06%) considered social network to be neither a curse nor a blessing. We were also able to discover that a colossal size of the sample population (75.62%) make use of their social network account(s) on daily basis. We were also able to observe that 68.75% of the sample population which is quite large owned at least 1 or more social network account. Facebook turned out to be the social network of choice from our investigation as 60% of the sample population make use of it and 50% also ranked it as their best social network.

Social network can serve as a blessing or as a curse - it all depends on how you make use of them. In the past, social networking services were viewed as a distraction and offered no educational benefit. Blocking these social networks was a form of protection for students against wasting time, bullying, and invasions of privacy. In an educational setting, Facebook, for example, is seen by many instructors and educators as a frivolous, time-wasting distraction from schoolwork, and it is not uncommon to be banned in junior or high school computer labs. In the light of the aforementioned dilemma, one question that comes to mind is, “if we succeed to ban users from using these sites in public places, can we still ban them from gaining access to them in the privacy of their homes?” It is in an attempt to answer that fundamental question that we are recommending a review of those decisions to ban social networks. Instead of putting a ban on them, students and other would-be users should be properly educated on the proper use of these sites. Adequate enlightenment on some safety measures to adopt while using these sites should be enshrined in the regular school curriculum and other institutional manuals that will educate the user on the proper use of these social networks.

The number of users of social networks is growing by the day. It is often said that evil thrives in the absence of good. Against that backdrop, we are also recommending the development of more programs that will be beneficial to users in these social networks. This will help to provide a profitable diversion that will help the user to engage in more meaningful ventures in the social networks.

It is also our sincere recommendation that security apparatus should be incorporated into all social networks to deter unwholesome behaviors and keep social misfits away from using social networks as a platform for carrying out their unscrupulous activities.

On a final note, social network users should never agree to meet online acquaintances in solitary places alone. The perils that such imprudent meetings can produce might far outweigh the perceived gains from such encounters.

It is hoped that as the aforementioned recommendations are embraced and implemented, we will be able to minimize the perils associated with social network usage while maximizing the full potential as inherent in social networks for the overall good of our world.

Acknowledgments

This research would not have been possible without the help of students at Auchi Polytechnic, Auchi, who mostly gladly accepted our questionnaires and responded to them timely. Our gratitude also goes to all our colleagues, friends and family members for their solidarity while we carried out this research. We are indeed grateful to all.

REFERENCES

[1]. Afia, E., Social Networks: Are They A Blessing Or A Curse? 2013 Retrieved from http://afiaenglish.wordpress.com/2013/03/14/social-networksare-they-a-blessing-or-a-curse-written-by-afia-english/ on June 12, 2014.

[2]. Oyamienlen, G., Plan To Conquer Election Vises In July 14th In Edo State And Beyond - Phase One. 2012 Retrieved from https://www.facebook.com/notes/justice-oyamienlen-godfrey/plan-to-conquer-election-vises-in-july-14th-in-edo-state-and-beyond-phase-one-by/459052010788526 on May 3, 2014

[3]. Akinwale, A., Alleged Killers of Cynthia Osokogu Arraigned for Murder. ThisDayLive. 2013 Retrieved from http://www.thisdaylive.com/articles/alleged-killers-of-cynthia-osokogu-arraigned-for-murder/138927 on May 12, 2014.

[4]. The Associated Press May 1, 2013. Number of active users at facebook over the years. Retrieved from http://news.yahoo.com/number-active-users-facebook-over-230449748.html on November 27, 2013.

[5]. Hempel, J., "Linkedin: How It's Changing Business". 2013 Fortune. pp. 69–74.

[6]. Craig S., How Many People Use the Top Social Media, Apps and Services. 2013 Retrieved from http://expandedramblings.com/index.php/resource-how-many-people-use-the-top-social-media/ on January 3, 2014.

[7]. Douglas, B., Nicole, B. , Michael, F. and Caroline, V., Social Networking and Its Effects on Companies and Their Employees. 2011 Retrieved from

http://www.neumann.edu/academics/divisions/business/journal/Review2011/SocialNetworking.pdf on March 15, 2014.

[8]. Wilson, J., Social networking: the business case. [Electronic Version] Engineering & Technology 2009 (4)10 54-56.

[9]. Auchi Polytechnic, Student Handbook of Information, Published by The Information and Public Relations Unit 2011 p.4

[10]. Melissa, S., Demographic Breakdown Shows Who Uses Social Media Most. 2013 Accessed from http://socialnewsdaily.com/12711/demographic-breakdown-shows-who-uses-social-media-most/ on April 17, 2014.