International Journal of Computing and ICT Research

Contents Volume 4, Issue 1, June 2010.

ISSN 1818-1139 (PRINT), ISSN 1996-1065 (ONLINE)

Table of Contents

Journal Editorial Office:
The International Journal of Computing and ICT Research
Makerere University
P.O. Box 7062,
Kampala, Uganda.
Tel: +256 414 540628
Fax: +256 414 540620
Email: ijcir@ijcir.org
Website: www.ijcir.org

International Journal of Computing and ICT Research

Volume 4, Issue 1, June 2010.

The International Journal of Computing and ICT Research
Makerere University
P.O. Box 7062,
Kampala, Uganda.
Tel: +256 414 540628
Fax: +256 414 540628
Email: ijcir@ijcir.org
Website: www.ijcir.org

Table of Contents

Book Reviews

Every issue of the journal will carry one or more book reviews. This is a call for reviewers of books. The book reviewed must be of interest to the readers of the journal. That is to say, the book must be within the areas the journal covers. The reviews must be no more than 500 words. Send your review electronically to the book review editor at: book-review-editor@ijcir.org

International Journal of Computing and ICT Research

The IJCIR is an independent biannual publication of Makerere University. In addition to publishing original work from international scholars from across the globe, the Journal strives to publish African original work of the highest quality that embraces basic information communication technology (ICT) that will not only offer significant contributions to scientific research and development but also take into account local development contexts. The Journal publishes papers in computer science, computer engineering, software engineering, information systems, data communications and computer networks, ICT for sustainable development, and other related areas. Two issues are published per year: June and December. For more detailed topics please see: http://www.ijcir.org.

Submitted work should be original and unpublished current research in computing and ICT based on either theoretical or methodological aspects, as well as various applications in real world problems from science, technology, business or commerce.

Short and quality articles (not exceeding 20 single spaced type pages) including references are preferable. The selection of journal papers which involves a rigorous review process secures the most scholarly, critical, analytical, original, and informative papers. Papers are typically published in less than half a year from the time a final corrected version of the manuscript is received.

Authors should submit their manuscripts in Word or PDF to ijcir@ijcir.org. Manuscripts submitted will be admitted subject to adherence to the publication requirements in formatting and style. For more details on manuscript formatting and style please visit the journal website at: http://www.ijcir.org.

Building the African Infrastructure for Development: The Role of the African University

PROF. JOSEPH M. KIZZA[*]
Editor-in-Chief

IJCIR Reference Format:
Kizza, Joseph. M. Building the African Infrastructure for Development: The Role of the African University. International Journal of Computing and ICT Research, Vol. 4, No. 1, pp. 7-8. http://www.ijcir.org/volume4-number1/article1.pdf .

1. INTRODUCTION

In volume 3 Issue 1 of this journal, I wrote part I of “Building the African ICT Infrastructure for Development: The Role of the African University”. After receiving many emails requesting me to make this broader, I am returning to the same theme but I am making it broader by removing the ICT component and considering all university education disciplines in national building. In addition to this and making it more relevant for the rest of the African population and beyond, I will also discuss the general population’s expectations of their universities in contributing to and advancing the forces of national development.

I have pointed out in various articles how the African university had a late – almost the last spot in the race for anything universities do for national development. The reasons for this are many including the fact that most of these universities are very recent with less than 50 years in business except a few. Even these few that have relatively a long history of educating Africa’s young minds, their missions were not genuinely, at least at the start, for developing African nations other than educating low level and half-baked Africans to help reduce the labor costs of the colonial masters who were finding it increasingly expensive to ship Europeans to Africa to do mere clerical jobs. To solve this problem, they started training “workshops” calling them technical or business colleges. Upon independence, most of these “workshops” were turned into national “universities”, but with no clear role in national development. These national “universities” were catering for children of the new African political elites. Cast into new roles of national administrators with little to no preparations, the new African elites did not formulate development agendas for these universities. So many of the universities continue to float with no development agenda only teaching students for personal prosperity, thus leading to the mass migration of the educated Africans to Europe and North America.

Through the seventies and eighties, most African universities were still without development agendas and were still doing business as usual. Meanwhile, governments strapped with lack of money saw no need of putting more scarce resources into big white elephants. By mid-eighties, even the UN and IMF were calling for a limit on funding African universities. But as I have pointed out in my previous writings, the wind of change has started blowing across the continent, especially for African universities. There is a new African quest, mostly fueled by an unprecedented indigenous interest, for relevant education, development driven based on technological acquisition.

To take advantage of this new African quest, African leading universities and institutions should set themselves new development agendas, based on the new technological advances and the an unprecedented interest in these technologies by young people; these agendas may include:

[*] Author’s Address: Joseph M. Kizza, Department of Computer Science and Engineering, The University of Tennessee-Chattanooga, Chattanooga, TN 37403, USA, *Joseph-kizza@utc.edu*.

International Journal of Computing and ICT Research, ISSN 1818-1139 (Print), ISSN 1996-1065 (Online), Vol.4, No.1 pp. 7-8, June 2010.

- building research and development capabilities and capacity that will create environments necessary for the development of infrastructures capable of solving local problems and challenges;
- developing curricula that put emphasis on:
  - educating graduates who are creators, not necessarily seekers, of jobs that meet national development needs,
  - identifying local problems and challenges that contribute to development and urgently need solutions,
  - identifying or developing relevant solutions and best practices, to solve these local problems and deal with the challenges,
  - finding local and global resources to build the needed research and development capacity,
  - building the tools needed to solve the identified problems where such tools are needed,
  - building the culture needed to promote the use of these tools and best practices to solve emerging local problems and challenges,
  - strengthening the newly developed research capacity through continuous improvement like the setting up of African Research Centers and Academies, and
  - Establishing a reward system to nationally recognize those people who excel in finding solutions and building tools that can be used to solve national and international problems and challenges.
- Encouraging researchers to put research interests before any other interests; that means sacrificing personal financial gains to academic pursuit.

However, none of these can be achieved without the governments showing interest and leadership through founding scientists and national research projects. Several African countries are already creating National Research Councils and Foundations and most important founding them. Some countries have also started funding graduate programs that are of national interests so that students doing graduate work can get scholarship funding. This is seed money for future research scientists.

All these activities, if implemented, will highlight the efforts African universities must make to advance basic and applied research agendas essential for building the critical mass of required capacity for national building in particular and for the development of Africa in general.

Feige-Fiat-Shamir ZKP Scheme Revisited

JOSEPH M. KIZZA[*]
Department of Computer Science and Engineering
The University of Tennessee, Chattanooga

Abstract
In networks and entity groupings that have sensitive resources, user identification is a crucial requirement for secure access, communication and transactions involving those resources. However, there are networks and entity groupings that require entity authentication while preserving the privacy of the entity being authenticated. There are several zero-knowledge protocols (ZKP) including the Fiege-Fiat-Shamir that authenticate an entity anonymously. We present a revised Feige-Fiat-Shamir ZKP scheme for the Airborne Networks (ANs) that reduces the ping-pong effect in the scheme and speeds up the growth of the Verifier trust of the Prover, thus making the authentication process faster and more efficient.

Key Words: Mission critical, time, authenticity, anonymity, zero knowledge, authentication.

IJCIR Reference Format:
Kizza, Joseph. M. Fiege-Fiat-Shamir Revisited. Journal of Computing and ICT Research, Vol. 4, No. 1, pp. 9-19. http://www.ijcir.org/volume4-number1/article2.pdf.

1. INTRODUCTION

In agile networks and other entity groupings that are mission driven, time sensitive, ad-hoc and self-organizing like in the Airborne Networks (ANs), authenticity, anonymity and accountability are essential and crucial and probably more so than in other similar networks that are less mission critical and time sensitive. In these kinds of networks, standard cryptographic authentication protocols like PKI cannot work effectively.

An Airborne Network is a self-forming, self-organizing, and self-generating, mission-critical and time sensitive network of airborne entities as nodes joining and leaving the network as they enter and exit specific regions. The network consists of dedicated tactical links, wideband air-to-air links, and ad-hoc networks constructed by the Joint Tactical Radio System (JTRS) networking services (Wikepedia [2009]). In addition, the JTRS is a software-defined radio that normally works with many existing military and civilian radios with the help of an integrated encryption and Wideband Networking Software that also provides system performance analysis and fault diagnostics automatically, reducing the demand for human intervention and network maintenance (Austin Mohr, [2007]).

There several efficient proofs including classical formulations of NP, interactive proof systems, computationally-sound proof systems, and probabilistic checkable proofs that can be good candidates for the ANs. However, the most suitable are proofs in the interactive proof systems. In particular, the zero-knowledge proof system (ZKP defined as Odel Goldreich [1993]: *For a language L a zero-knowledge proof system is a pair (P, V) of interactive machines, so that V is probabilistic polynomial-time, satisfying*

- Completeness:*For every x Є L the verifier V always accepts after interacting with the prove r P on common input x .*

[*] Author's Address: Joseph M. Kizza, Department of Computer Science and Engineering, The University of Tennessee-Chattanooga, Chattanooga, TN 37403, USA,*Joseph-kizza@utc.edu*.

International Journal of Computing and ICT Research, ISSN 1818-1139 (Print), ISSN 1996-1065 (Online), Vol.4, No.1 pp. 9-19, June 2010.

- Soundness:*For every x not in L and every potential prover P*, the verifier V rejects with probability*
at least ½ after interacting with P on common input x .*

The *Prover* P is a machine that is seeking authentication that must be done by the Verifier V upon presentation of evidence *by* the *Prover* to the Verifier that does not give away the identity of the *Prover*. Based on the evidence provided by the *Prover*, the verifier may get satisfied and authenticate the *Prover* without knowing the identity of the *Prover*. Unlike the Public Key Infrastructure (PKI), a framework for creating a secure method for exchanging information based on public key cryptography. The key role for the PKI is the certificate authority (CA), which issues digital certificates that authenticate the identity of entities over a public communication system as the Internet. ZKP does not involve this CA acting as a third party.

In ZKP, the *Prover* presents to the *Verifier* a publically generated and known part of the token. Upon receiving the public part of the *Prover*'s token, the Verifier then may require the *Prover* to produce a *response*, to a Verifier's randomly generated *challenge* based on the *Prover*'s public part of the token. On receiving the *Prover'*s response, the *Verifier* then validates the response using no more than the publicly known information. Two possible outcomes are either "yes" or "no". If a "yes" answer is produced, the authentication process is successfully over and the token is now *spent,* meaning, it has served its purpose and it is done. Any other authentication needed by this entity requires a new token to be generated. If the outcome is a "no" a new round of authentication may be required. This may go on for a number of back and forth ping-point exchanges until success. A successful ZKP authentication leads to the *Prover* remaining anonymous to the verifier.

Several scholars (Park Choonsik [1992], Dev Anshul and Suman Ray [2005], M. J. Fisher [2005], Hannu A. Aronnsson [2000]) have written about the problems of ZKP protocols including their inefficiency in exchanging tokens during the *challenge-response* sessions. Such problems tend to get worse as the network sizes grow.

In this paper we propose a new approach to the Feige-Fiat-Shamir ZKP scheme that aims to reduce the number of *challenge-response* ping-pong exchanges and thus create a speed-up in the building of trust and increasing the effectiveness of the scheme.

The rest of the paper is organized as follows. We will introduce the Feige-Fiat-Shamir ZKP Scheme in Section 2. Then we will explain the new improvements to the Feige-Fiat-Shamir Protocol scheme in Section 3. Security and trust analysis will be given in Section 4. Problems with Parallel Execution of Zero-Knowledge Proofs are discussed in Section 5. Finally we conclude and discuss possible extension in Section 6. References are in Section 7.

2. RELATED WORK

Several interesting zero knowledge proofs are of note here starting with Hannu Aronsson,s (Wikipedia [2009]) work which explains zero knowledge proofs starting with the basics including a summary of all the major zero knowledge studies. Li Lu et al [2006] discuss zero knowledge authentication in P2P systems. However, they use a modified ZKPI scheme that uses a key exchange but with no third party. Austin Mohr [2007] gives an in depth survey of zero knowledge proofs ranging from Graph Isomorphism, Graph 3-colorability, All Languages in NP and Fiat-Shamir protocol. None of these works attempts to extend the speed of authentication as ours attempts to do.

3. FEIGE-FIAT-SHAMIR PROTOCOL

The Feige-Fiat-Shamir Identification Scheme is a classical, practical and widely used modular arithmetic ZKP scheme developed by Uriel Feige, Amos Fiat and Adi Shamir in 1988. Following the principle of all zero-knowledge proofs, the Feige-Fiat-Shamir Identification Scheme involves two entities, the *Prover*, and the *Verifier*. The *Prove*r possesses a secret token and is seeking authentication and must prove to another entity, the *Verifier*, who must authenticate the *Prover* based upon the secret token the *Prover* has, through a series of challenges without getting to know the P*rover*'s secret token.
Procedure

The Feige-Fiat-Shamir process involves the *Prover* choosing two large Blum prime integers *p* and *q* where each is of the type 4g+3 and *gcd*(g, 3) =1. Also the *Prover* chooses two security integers *k* and *t*. Then computing the product *n* = *pq*. The protocol then uses this n in the modular arithmetic that follows.
The congruence relation
Two integers *a* and*b* are said to be *congruentmodulon*, if their difference *a* – *b* is an integer multiple of *n*. That is both numbers have the same remainder when divided by n. This is then expressed as:

$$a \equiv b \pmod{n}.$$

A good example are integers a = 38 and b = 14. Then 38 ≡ 14 (mod 12) shows that (a, b) form a congruence class.

Using this *n*, choose or create secret vector *s* = {$s_1, \cdots, s_k$} with *gcd*(s_i,*n*) = 1, and c = { $c_{i=1,\, k\,|}c_i$Є (0, 1)}. *n* is then made public. Now compute the vector *v* = { v_1, v_2, …v_k |$v_i \equiv s_i^2 \pmod{n}$} where ≡ is a congruency relation between v_i and s_i^2, meaning that v_i and s_i^2 have the same remainder upon division by n.

The vector *v* then is sent to the *Verifier*. The difficulty the *Verifier* may encounter in recovering the vector *s* as it involves the computation of the modular square root without knowing the modulus' factorization. The Feige-Fiat-Shamir procedure goes as follows [7].

1. *Prover* chooses a random integer *r*, a random sign b Є {-1, 1}and computes $x \equiv (-1)^{ci,\ i=1,\ k} . r^2$ (mod n). *Prover* sends this number to Verifier.
2. Verifier chooses numbers $a_1, \cdots, a_k$ where a_i equals 0 or 1. *Verifier* sends these numbers to *Prover.*
3. *Prover* computes $y \equiv rs_1^{a_1}s_2^{a_2}\cdots s_k^{a_k} \pmod{n}$. *Prover* sends this number to *Verifier.*
4. *Verifier* checks that $y^2 \equiv \pm xv_1^{a_1}v_2^{a_2}\cdots v_k^{a_k} \pmod{n}.$

This procedure is repeated with different *r* and a_i values until *Verifier* is satisfied that *Prover* does indeed possess the modular square roots (s_i) of his v_i numbers.

4. THE REVISED FEIGE-FIAT-SHAMIR PROTOCOL

The Ping-Pong Problem

While the Feige-Fiat-Shamir Identification Scheme is the most celebrated, classical, practical and widely used modular arithmetic ZKP scheme, it suffers from the *ping-pong problem.* The Ping Pong problem in the ZKP solutions is caused by repeated, sometimes uncontrolled, challenge-response exchanges between the *Verifier* and the *Prover*, as the *Verifier* tries to get as much information as possible from the *Prover* in order to complete the authentication process in the shortest time possible but in the most sure way and as the *Prover* tries to provide the needed information for the authentication process without revealing the *Prove*r's identity. The ping-pong problem is a resource guzzler. Given that the AN environment is time critical, the authentication process needs to be comprehensive, precise and take a short time. But in the Feige-Fiat-Shamir this cannot be accomplished because, there is no sure way of making the process short. In some cases, the authentication process may be short but not always. We propose a procedure that speeds up this process and it builds the trust quickly. The scheme still involves two entities, the *Prover*, who possesses a secret token and is seeking authentication and must prove to another entity, the *Verifier*, who must authenticate the *Prover* based upon the secret token the *Prover* has, through a limited series of challenges without getting to know the *Prover*'s secret token.

Procedure

The revised Feige-Fiat-Shamir protocol still involves the *Prover* choosing two large Blum prime integers *p* and *q* where each is of the type 4g+3 and *gcd*(g, 3) = 1. Also the *Prover* chooses two security integers *k* and *t*. The *Prover* then computes *n* = *pq*. Using this *n*, the *Prover* then chooses or creates a secret vector *s* = {$s_1, \cdots, s_k$} with gcd(s_i,*n*) = 1. *n* is then made public. Further the *Prover* still computes the vector *v* = {v_1, v_2 …vk |$v_i \equiv s_i^2 \pmod{n}$}. The vector *v* is then sent to the *Verifier*. Like in the original Feige-Fiat-Shamir protocol, the Holy Grail of the protocol is the difficulty the

Verifier encounters in recovering the vector *s* as this involves the computation of the modular square root without knowing the modulus' factorization. The revised Feige-Fiat-Shamir protocol then goes as follows.

1 *Prover* chooses a random integer *r*, a random sign *b* in set {-1, 1}and computes $x \equiv b.\ r^2$ *(mod n). Prover* sends this number to *Verifier*.

2. Each time the *Verifier* chooses a challenge, there are ${}^{k}C_{j=1,\,k}$ possible ways to choose the vector *a* = $\{ a_1, \cdots, a_k \}$ where a_i equals 0 or 1. These choices are represented by the 0-1 matrix M = $\{(a_{ij}) = (0,1)|\ (i, j) = 1, k\}$. From these rows of M, the *Verifier* randomly selects a number of rows forming a sub-matrix D = $\{(a_{ij}) = (0, 1)\ |i=1, k, j=1, f.\}$ of M to concurrently send to the *Prover* as the challenge.

3. Instead of the *Prover* computing only one number y, the *Prover* uses the received matrix D to compute a vector

   y=$\{ y_1,\ y_2,\ \ldots\ y_f\ |\ y_i \equiv r\ \pi\ s_i^{a}{}_{ij}$ (mod n), i=1..k and j=1, f}.

   The *Prover* then sends this vector *y* to the *Verifier.*

4. *Verifier* checks that each of the vector components of *y* satisfies ${}_{yj}^{2} \equiv \pm\ x\ \pi\ v_i^{a}{}_{ij}$ (mod n), i=1..k and j=1, f}.

This procedure may be repeated with different *r* and different sub-matrices D = $\{(a_{ij}|\ i=1, k, j=1, f.\}$ of M until the *Verifier* is satisfied that the *Prover* does indeed possess the modular square roots (s_i) of his v_i numbers.

An Example:

1. Suppose either the *Prover* or a trusted center T selects the primes p = 139, q = 347, and publishes n = pq = 48233.
2. The *Prover* chooses Integers k = 3 and t = 1 as the needed security parameters.
   Then the *Prover* does the following:
   - Selects 3 random integers s_1=87, s_2= 21649, s_3 = 523, and 3 bits b_1 = 1, b_2 = 0, b_3 = 1.
   - Computes v_1 = 7569, v_2 = 10310, and v_3 = 32364.
   - The *Prover*'s public key then is (7569, 10310, 32364, 48233) and the *Prover*'s private key is (87, 21649, 523).
3. The *Prover* chooses integers r = 3209, b = 1, and computes x = 24052, and sends this to Verifier.
4. Since k was chosen as 3, the *Verifie*r has the following possible matrix
   M = {0 0 0, 0 0 1, 0 1 0, 0 1 1, 1 0 0, 1 0 1, 1 1 0, 1 1 1 }
   of choices of challenges.
5. Suppose the *Verifier* chooses a sub-matrix
   D= { 0 1 0, 0 1 1, 1 1 1}
   and sends it to the *Prover*.
6. The *Prover* must compute a vector y = { y_1 , y_2 , y_3 } = {16121, 5788, 36823}
7. The *Verifier* computes (y_1^2 , y_2^2 , y_3^2) = (259886641, 33500944, 1355933329). Also computes ((24052*[10310], 24052*[10310*32364], 24052*[7569*10310*32364])
8. To accept the *Prover*'s identity the following pairs of numbers must be in the same congruency classes mod 48233:
   a. (259886641 and 24052*10310)
   b. (3350094 and 24052*10310*32364)
   c. (1355933329 and 24052*7569*10310*32364)

5. SECURITY AND TRUST ANALYSIS

Using the scheme we have outlined above one achieves tremendous savings first in time speed up and rapid build up of the trust and also in the security which is not compromised. Based on the Feige-Fiat-Shamir protocol on which this scheme is built, the *Prover* does not give any useful information to the *Verifier* during the whole process. If there is any interception of the communication, the interceptor can learn no more information than what the P*rover* gives out. The knowledge of the *Prover*'s secret cannot leak because it is not communicated to the *Verifier.* The new scheme adds nothing that would change this fact. Therefore the security of the scheme is assured.

The major contribution of this scheme is a quick build up of the *Verifier* trust and confidence for the *Prover*. We can calculate this trust build up as follows. Suppose the security integers chosen by the *Prover* are k and 1. This means that the Verifier has k! ways of choosing a 0-1 vector of length k. This is what we referred to in the protocol as matrix M. Suppose further that the Verifier decided to send several of these vectors at a go. The *Verifier* can decide to send to the *Prover* a sub-matrix D of M consisting of these choices, the *Prover* then sends back the vector $y = \{y_1 , y_2 \ldots y_f\}$. At each parallel burst resulting in matrix D of f rows, with k bits each, which the Prover returns correct, the *Verifie*r's trust/confidentiality grows as $\{1 – ((1/2)^f)^k\}$. So for t bursts of parallelism, the contribution to trust increases by $\{1- (((1/2^f)^k)^t\}$. This is a good speed up which makes the authentication process take less time.

6. PROBLEMS WITH PARALLEL EXECUTION OF ZERO-KNOWLEDGE PROOFS

Parallel executions of zero-knowledge in Feige-Fiat-Shamir protocol have been proposed and they are certainly attractive and they reduce the number of ping pong messages between *Prover* and *Verifier* to only 1 1/2. However, it has also been proven that they may not be fully zero knowledge (Joe Kilian, Eriz Petrank and Ransom Richardson [2001], M. Konidala Divyan [2003]). However, there have also been concurrent zero knowledge techniques that preserve zero knowledge (Li Lu, Jinsong Han, Yunhao Liu, Lei hu, Jinpeng Huai Lionel Ni and Jian Ma [2006]). Our approach consists of bursts of parallelism while maintaining serial execution of the Feige-Fiat-Shamir, hence maintaining zero knowledge. Note that the difference between the serial and full parallel versions of the protocol is that in the latter, the *Verifier* gets to know all of the x_i's before choosing the b_i's. This does not happen in our approach. The Verifier chooses matrix D with no knowledge of all the x_i's. We generate bursts of parallelism consisting of matrices D with no more that f < k. The matrices D can be calculated several times depending on the number of bursts of parallelism that can occur during an entity authentication. This number, however, cannot be more that t.

7. SIMULATION AND RESULTS

The full simulation to support this paper was planned to be carried out in two phases as follows:

(1) In phase one we planned to generate and test the C code developed by Daniele Raffo [2002] at LIX, Ecole Polytechnique, France. This code was modified and run in two modes, the single processor mode and the multi-processor distributed environment. In the single processor mode, we made several runs of the modified code and in the distributed environment, we developed the handshake protocols for the exchange of information between the Prover and the Verifier processors in a client-server model.

(2) In phase two, we plan to develop new C++ code for the revised Feige-Fiat-Shamir zero-knowledge protocol discussed in this paper. Next we will develop the handshake protocol for the new FFS. We ill then develop the test databed. With the test bed we will do:

- Distributed testing
- Speed up protocol development
- Testing using UAVs as needed and where possible.
- Analysis of results

In phase one, we have ran the modified C code on a trial basis and Figure 3 shows the outputs of those runs for T =10 and K =10. The results in Figure 3 show the full range of outputs which included modulus n, both the computed public and private keys after each of the ten iterations, the challenge from the Verifier, the response from the Prover, the verification by the Verifier and the acceptance by the Verifier. Since the growth of the output data was astronomical, we decided not to continue with this kind of experimentation.

Figure 3 (below): Row output from the Modified C Code.

```
Publishing modulus:
179769292056060085716483151220741222201029658454479408595548508404308134756702271009835
01843992713434673272870106881260075258096741070121083873322026654079847592167290680288
24258931358191508503013441231414124988924910363256333882578222976294474137538761493485
43391157235192405410661330286251829642799867610529
Computing keys
```

```
Public key:
13256255557264271676024090692164773830765799713043117227528632926510949761102233108196
70413057761792102446546320619998748411283056671496121877666821840103407959409519981908
78611212440363356690228646676543478072735080886180579618611185316085836814910668700772
178596560234925155243849909292527807550786877325598
13630403996302298141597863520177809111947610288203571012081079651181218746884402523762
20058072988193501083406566024325204606396729189849440291576507536446421239343452602583
27761305898784680879130656098014757732014784847792044698460542621432342880193923989712
919728007258096777490561336107137968867636283902048
91524625548709623598418881393288380896783392652190265032824063636517630562184208441303
75214315104013861149166043737298368977761673750514279370537015098821581567292055666783
81788937355133260675570024672415472418635228778601597110306827080098068875239606914108
692051693886750585316577378090227868777128594742 04
10852062878736044524314651638729447161297468389151454417802470349123506768218846068339
11090569231214982176846381546963135532020974113012816754717906695444111705386327157287
40220422386313382819937149948836131324128486088451484832130008634654758421957003736829
421218280063884645322699022818175881111555620622870
17394490629576510437597664352437135834914159329103498549131612574992273407611080476852
40070190865568825483418296403012259228105299377238410890844699832836567519277521855183
48206923304195027873271778735162035470605419467891818866408142508253820293651028149625
047926425499421469277319174658471647502125928532510
11192529250098233222560673627420816678837136040240815033214924870733065091217240716506
00836011004285414163587152789603446254793658690879244688162843792920636924413875355941
97753738090593907545516297554607535208626264617259399720566423147202578117585748144902
387479301022375529173683061506082526232204371185397
92822503344974732701231405311799192202978414254399253894641868595667210911014724422953
21878856186443399071038058578165851453560517385105019683059129891552161417771424498696
31872425552904497948391365064318696072866608208562762985912544545726265027644174116532
424772828443919214377133475010569155874638710755 07
76931730949259744103100800308564752542843555547705107776671639827301410839566750531691
52468498678481836164149403102781116890658043996620446432123302772274904580602048853758
37350747078469588651376415860835222218173266622068879398827422477356863499098915128259
356773093601532881536492171802679014109897289359 60
17109148207572442309009686117360022096200899570941288416101391003975383768152279674908
89675787141095611460464349046975878733196601462758601938116944554369826743793313913529
01132735936739840420010040771266522528130151911240828912866528466536723715546441664009
937573375045955972460224604447946948697851210255 84
54516656676446923506005618677267170596564581804575722672296464343354322039612834722878
42598411338783085874221915532096464489190810333414438291603980280329575946055220270198
06460974471618666362227087465044490552882058611657174179550983513384320904827797158689
537747787992311139996551112922389758085375239245 24
Private key:
15090651724267505309971848528182817639762883484063720504346210872054567712535887261764
89265163983867716116255306927666719477521261840399065391330144079770376099761751215442
82687798173836378706311506665888654639606166137472813102465213217334575444498611594443
601103317781106636911139835814853151103961218939133
12194695208480035384868695688957628159499601416962764459987609475311425548571694122189
31365647753497958459354506658130861780634363463660655122330567364616594193237206603357
68596576290810297389822595126022597737722063931686360491382793095922723028253192119896
767408290847272964868484796815942952909768991176838
15619200158546778457984510695972153067936715835277119391422623661283202164783846408379
16336747828474279324350783269220108689219839878918813072043990466030737399672906376065
03164678179518816642292522021767149970747002768545690951029354992973819220887304803952
261707336114172928800409692135487768743212955435166
```

```
262616321802500395276480805170513908064592564637896230244108659471378843026563925409494
300227638212338344727673832534073921289135729238007599271939634071646991229139373587496
353024807251173969339243496512031149359004192311877793629404155686210185425658165813
02156111293234815117318936031296070289412465381448
1115208873490861085400118058754335475763565536525193109657853390410041912314933108575
0161689156502327143652757848522471652741143560384839660254931268353605866312961795144021
71445792624944250260483971133471457120018694272953900102559028592506402594758017022705
409113177059788585979700768217349295828073892456104305409802177013508817477109810583389171947221068200199857140532129616008774214727249542084096302884491905294986044615113920067695400446078315256472700669357499834053843725
2767441661098866046034760861558682955053462937500835058349521398944892675431837895176036941162551971473550080587989115712433648396977555
12688048269240852856198759049205712364821231577104130321619098154241708195085827674163
80832937987428769899033236150556212721776722483300841934474488643115822858320598644458
69276458231405997136394987211967912986614047232992950838418542896590241758204040896430
2097212289790786935526921534696643554183552013124211293682550910430514535546604977802521685608998726360402116515432838140409021493108920828842437646076567506154422619070607560474175277643193330157138602685665678771521266105
46852339217807288022127853424796948792724336507164222694916480946104388172674846491531
096561148659130946473477303795819122557420978423911219504989159304145804447904961229020560947647075917794745157481575664457355960220487
813240338259576653921987724440975264863705717286172208157103413695196039316076755204285653374196275646365405746176477367421986717999839672254561657083513262383331523251026116864694639635376416585562606028125018079094674525966457423698969402991813166828200639023406606582801940676118130300251139098434855327309
395359505992903105215139157468031852231707045936130256625673325627583966473350875992821807689689402501086769056633388278648578959356081199014886090277554002831330022231419900749205277003448738458216286098718567909392354774
Witness                                                                                :
100894464009841049715216943115241675119414603317469451694560179205814464013278091739274547631997804822499806246345969357676565836311881943836146127126270346321257076328123130112367302118118424573183118805902123632347050642989532098727171794810063859213630048849323533068447522197721951395940291447402660685747
Challenge   : 1001001110
Response                                                                               :
7810173275356886115905966317186787418242627066881777507829842487368944771924046568396932489913456343487198548542240535084373605548162504832332491553866493744768880279715678781300927802226020260659284716471898158165417801569824660704643132625629316340689690919360148727479600709380214702228401577777633888289 7
Verification:
100894464009841049715216943115241675119414603317469451694560179205814464013278091739274547631997804822499806246345969357676565836311881943836146127126270346321257076328123130112367302118118424573183118805902123632347050642989532098727171794810063859213630048849323533068447522197721951395940291447402660685747
Authentication successful!
```

Next we restructured and expanded this code to convert it into C++ so that we could run both the Prover and the Verifier codes as threads. Several runs were made with varying sizes of K, T and time tamps. Figure 4 shows selected outputs of these runs except the varying time stamps for each change in T and K. We are showing a selected number of runs of varying sizes of Ts and Ks using a single core thread environment:

Figure 4 (below): Selected Runs with Varying Sizes of Ts and Ks Using Threads

T = 10, 100, 500, 1000, 2000, 5000.

K = 10, 20, 50, 70, 100, 500

Sample Runs:

1. T=5 and K = 4

```
Feige-Fiat-Shamir ZKP implementation
Iteration 0: 06.12.2009 22:24:27
Authentication successful.
Iteration 0 finished at: 06.12.2009 22:24:27

Iteration 1: 06.12.2009 22:24:27
Authentication successful.
Iteration 1 finished at: 06.12.2009 22:24:28

Iteration 2: 06.12.2009 22:24:28
Authentication successful.
Iteration 2 finished at: 06.12.2009 22:24:28

Iteration 3: 06.12.2009 22:24:28
Authentication successful.
Iteration 3 finished at: 06.12.2009 22:24:28
```

2. T=10 & K = 8

```
Feige-Fiat-Shamir ZKP implementation
Iteration 0: 06.12.2009 23:31:07
Authentication successful.
Iteration 0 finished at: 06.12.2009 23:31:07

Iteration 1: 06.12.2009 23:31:07
Authentication successful.
Iteration 1 finished at: 06.12.2009 23:31:07

Iteration 2: 06.12.2009 23:31:07
Authentication successful.
Iteration 2 finished at: 06.12.2009 23:31:07

Iteration 3: 06.12.2009 23:31:07
Authentication successful.
Iteration 3 finished at: 06.12.2009 23:31:07

Iteration 4: 06.12.2009 23:31:07
Authentication successful.
Iteration 4 finished at: 06.12.2009 23:31:07

Iteration 5: 06.12.2009 23:31:07
Authentication successful.
Iteration 5 finished at: 06.12.2009 23:31:07

Iteration 6: 06.12.2009 23:31:07
Authentication successful.
Iteration 6 finished at: 06.12.2009 23:31:07

Iteration 7: 06.12.2009 23:31:07
Authentication successful.
Iteration 7 finished at: 06.12.2009 23:31:07
```

K	Seconds
10	1
50	3
100	3
500	10
1000	34
2000	119
3000	296
4000	509
5000	807

Table 1: Changing values of K, T =20 and the time stamps.

To learn more of these changing timestamps, we extended this algorithm so that it can work in the multi thread and truly distributed environment of a client-server model by developing communication protocols and handshake necessary in a networked environment. Under this environment, the Verifier runs as the server and the Prover as the client. In this Client-Server model, we tested the algorithm on differing sizes of both K and T. As we did this, the time stamp was taken at the start and end of each exchange between the client and the server until the Verifier accepted the Prover.

In Table 1 and corresponding Figure 5 we show results of runs in this distributed client-server environment with varying sizes of K.

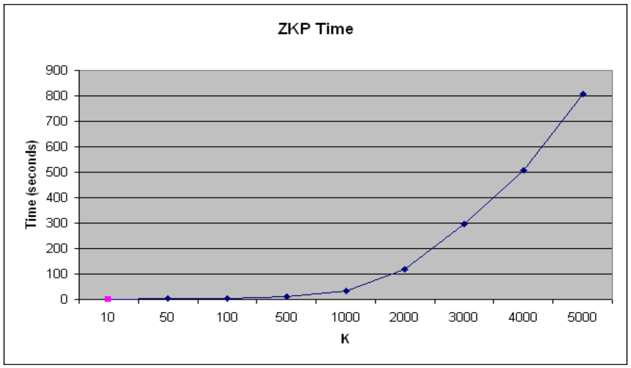


Figure 5: Growth of Computation Time Against the Size of the Primes K.

From Figure 5 above, there is compelling evidence that the larger the size of the integer strings, the longer it takes for the authentication of the entity.

9. ZKP COMPARED TO PKI

We have not compared ZPK with suitable PKI yet but this will be our next step.

10. FUTURE WORKS

As we pointed out earlier, this work has so far dealt with the original Feige-Fiat-Shamir. The simulation of the Feige-Fiat-Shamir discussed in full is to be tackled in the planned phase II of this work. This will be the starting point for our future work. In particular, we will generate new code C++ code for the revised Feige-Fiat-Shamir zero-knowledge protocol. Next we will develop the handshake protocol for the new FFS. We ill next develop the test databed. With the test bed we will do:

- Distributed testing
- Speed up protocol development
- Testing using UAVs as needed and where possible.
- Analysis of results

- Major testing

The purpose of this work was to revisit and revise Feige-Fiat-Shamir's original ZKP scheme in order to remove the ping-pong effect and make it faster to use. To meet this goal, after we get results in phase II, we will compare the duration of authentications in the distributed client-server model for the authentication of the Prover by the Verifier in both phase I and II. The differences we get in this comparison will demonstrate the time savings when our revised Fiege-Fiat-Shamir algorithm is used.

Zero Knowledge Protocols are designed to work between two parties, the Prover and the Verifier. Through verification rounds the Prover attempts to convince the Verifier he possesses a secret. Over time the Verifier may trust the Prover has a secret and allow the Prover to communication with the Verifier.
The trust the Verifier has for the Prover does not transfer to other nodes of the network. Further work, as a continuation of this project, is needed to look into how the Prover earns the trust of the entire network once accepted by the Verifier.

11. CONCLUSION

In this paper, we have produced a revised Fiege-Fiat-Shamir protocol scheme in which the Verifier instead of choosing one 0-1 vector as a challenge to the *Prover* now chooses a sub-matrix whose rows are individual challenge vectors. Increasing the number of challenge vectors sent to the Prover at once speeds up the growth of the Verifier's trust of the *Prover* making the whole authentication process a lot faster and more efficient. We have also developed test programs to run the algorithm in a multi thread environment. Further we have developed the necessary protocols to run the algorithm in a client-server model which gives it a real distributed environment. As we did this we took timestamps of each run and computed time growth computation with the increasing size of the primes used. Looking at the times graph raises more and interesting questions that require extending this study. Such improvements may include finding more efficient and economical ways to move matrix D from the *Verifier* to the *Prover*. In our next attempt, we will focus on ways to move this matrix more economically. We want to investigate ways to either decompose the matrix or find some other lossless compression that will cut down on the amount of data passed.
There are several other issues that are also attracting our interest. Some of these include:

- Since ANs are P2P networks, does authentication of an entity by another network entity lead to global network authentication of that entity? If not, how do we handle subsequent authentication of that entity?
- If an entity leaves the network constellation and comes back in a very short time, does this mean a new authentication? Do we need to generate a session identification code to reduce on the number of authentication requests?

12. REFERENCES

AIRBORNE NETWORKING.http://en.wikipedia.org/wiki/Airborne_Networking

AUSTIN MOHR. " A Survey of Zero-Knowledge Proofs with Applications to Cryptography". http://austinmohr.com/work/files/zkp.pdf

CHOONSIK, PARK. A *Roubust Identification Protocol Without a Highly Reliable Trusted Center*. Singapore ICCS/ISITA 1992, IEEE, 1992.

DANIELE RAFFO, 2002: Master of Science in Computer Science, specialization in Networking - with honors. "Digital Certificates and the Feige-Fiat-Shamir zero-knowledge protocol".Université Paris-Est Marne-la-Vallée.

DEV ANSHUL AND SUMAN RAY.*A ZKP-based Identification Scheme for Base Nodes in Wireless Sensor Networks*. ACM SAC '05, March 13-17, 2005.

FISHER, M. J.*Zero Knowledge Interactive Proofs,* http://zoo.cs.yale.edu/classes/cs467/2005s/course/lectures/ln_week10.pdf

HANNU A. ARONSSON. "Zero Knowledge Protocols and Small Systems".http://www.tml.tkk.fi/Opinnot/Tik-110.501/1995/zeroknowledge.html *http://www.iacr.org/archive/eurocrypt2000/1807/18070424-new.pdf*

IVAN DAMGºARD.*Efficient Concurrent Zero-Knowledge in the Auxiliary String Model*

JOE KILIAN, EREZ PETRANK AND RANSOM RICHARDSON.*On Concurrent and Resettable Zero-KnowledgeProofs for NP.,*http://arxiv.org/abs/cs.CR/0107004

KONIDALA M. DIVYAN .*ComparativeStudy on Zero-KnowledgeIdentificationProtocols* http://caislab.icu.ac.kr/Lecture/data/2003/spring/ice514/project/f02_divyan.ppt.

Li Lu, Jinsong Han, Yunhao Liu, Lei hu, Jinpeng Huai Lionel Ni and Jian Ma. “Pseudo Trust: Zero-knowledge Authentication in Anonymous P2Ps”. *IEEE Transactions on Parallel and Distributed Systems.* Vol. 19, No. 10, October 2006.

Oded Goldreich.*A Taxonomy of Proof Systems (part 1).* http://delivery.acm.org/10.1145/170000/165000/p2-hemaspaandra.pdf?key1=165000&key2=0808024421&coll=GUIDE&dl=GUIDE&CFID=39183453&CFTOKEN=53850464

RETRIEVED FROM "http://en.wikipedia.org/wiki/Feige-Fiat-Shamir_Identification_Scheme".

SHAFI GOLDWASSER AND YAEL TAUMAN KALAI.*On the (In)security of the Fiat-Shamir Paradigm*. Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science (FOCS’93).

WADE TRAPPE, LAWRENCE C. WASHINGTON, *Introduction to Cryptography with Coding Theory* (Prentice-Hall, Inc., 2003), pp. 231–233.

Improving Load Balance and Query Throughput of Distributed IR Systems

A. ABUSUKHON[†]
School of Computing and Technology
University of Sunderland, UK

M. TALIB
Department of Computer Science
University of Botswana

Abstract

As the number of queries grows over time it becomes necessary that Information Retrieval (IR) system provides high query processing rate i.e. high query throughput. In IR systems, there are three types of data partitioning, namely term-based, document-based, and hybrid partitioning. In document-based and hybrid partitioning, query is sent to all nodes and thus high level of parallelism is achieved but low query throughput. In term-based partitioning, a given query is divided into sub-queries and each sub-query is directed to the relevant node. This provides high query throughput and concurrency but poor parallelism and load balance. In this paper, the Moderate Distributed IR System (MDIRS) is proposed to improve the query throughput and load balance of hybrid partitioning. MDIRS inherits the advantage of document-based partitioning i.e. it provides moderate level of parallelism and the advantage of term-based partitioning. In other words, it provides moderate level of query throughput and load balance. Results from this paper showed that the MDIRS improved the query throughput and the total query response time of hybrid partitioning by 64% over the baseline system.

Categories and Subject Descriptors: H.1.1 [Systems and Information Theory] Information Theory - Value Information, H.3.3 [Information Search and Retrieval] Information Filtering - Retrieval Model – Search Process C.2.4 [Distributed Systems] Distributed Applications, Network Operating Systems
General Terms: Algorithm, Performance, Verification
Additional Keywords: Term Partitioning, Hybrid Partitioning, Hybrid Queries, Throughput, Load balance

IJCIR Reference Format:
A. Abusukhon, and M. Talib. Improving Load Balance and Query Throughput of Distributed IR Systems. International Journal of Computing and ICT Research, Vol. 4, No. 1, pp. 20-29. http://www.ijcir.org/volume4-number1/article3.pdf.

1. INTRODUCTION

The number of pages (documents) available online is increasing rapidly. Gulli and Signorini [2005] estimated the current size of the web. They mentioned that Google claims to index more than 8 billion pages, MSN claims about 5 billion pages and Yahoo at least 4 billion pages. They estimated the indexable

[†] Authors' Address: A. Abusukhon, School of Computing and Technology, University of Sunderland, UK ce4aab@student.sunderland.ac.uk; M. Talib, Department of Computer Science, University of Botswana talib@mopipi.ub.bw

International Journal of Computing and ICT Research, ISSN 1818-1139 (Print), ISSN 1996-1065 (Online), Vol.4, No.1, pp. 23 - 29, June, 2010

web to be at least 11.5 billion pages. Besides the huge document collection, we have a large number of information requests (queries) that are submitted by clients. *Sullivan*[10] reported that the number of searches per day performed by Google is 250 million.

In order to the users to effectively retrieve documents that are relevant to their needs, the IR systems must provide effective, efficient, and concurrent access to large document collections. The indices of documents must be built to perform timely information retrieval. Baeza and Ribeiro [1999] defined the index of a text as - index is a data structure built over the text to speed up the search. The most popular indices are inverted files and suffix arrays. In this research, the inverted file structure is used because of being more efficient than suffix arrays structure. Inverted files are composed of two parts - distinct tokens and the inverted lists. The inverted list consists of a number of pairs and each pair consists of document identifier in which the term appears with its frequency in that document. Other inverted file structures may contain all positions in the document at which a unique term appears, Moffat et al. [2006].

This example explains how to construct the inverted file.
Suppose that we have the following documents and terms:

Table 1: Inverted File - Example

Document identifier	**Terms appear in**
D1	A, B, C,A
D2	D, E, F, A
D3	C,D, B,B

In this case, the inverted file is constructed as:

A: 1:2, 2:1	B: 1:1, 3:2	C: 1:1, 3:1
D: 2:1, 3:1	E: 2:1	

The inverted list 1:2, 2:1 means term A appears two times in document D1 and one time in D2. The list “1:2, 2:1” is called the inverted list.

Usually inverted files are very huge and need to be accessed at very high speed. The solution to this problem is to split the index among N nodes so that each node searches part of the distributed index.

Badue et al. [2001] evaluated distributed query performance on a real machine. They compared the local index (document partitioning) with the global index (term partitioning). They concluded that the local index provided high parallelism while the global index provided high concurrency. In local index a given query is sent to all nodes means that all nodes execute the same query. In global index partitioning, not all nodes necessarily participating in performing a single query meaning that more than one query are executed concurrently. In other words, in global index partitioning, query terms are sent only to the nodes that store their inverted list and thus allowing high concurrency.

Related Work

In general, there are three types of index partitioning namely, term-based, document-based and hybrid partitioning. In document-based partitioning, the document collection is divided equally into sub-collections then the sub-collections are distributed over nodes and then each node generates an index for that sub-collection. In this case, the documents of each sub-collection and the index reside on the same node. In term-based partitioning, all unique terms in the data collection and their full inverted lists are stored in a global index and then the terms of the global index are distributed equally among nodes using an appropriate mapping algorithm. In this paper the lexicographical mapping is used. In lexicographical mapping, each node stores a set of terms that start with a certain set of letters. For example node 1 may store all terms that start with letters A through F, and so on).

Xi et al. [2002] proposed a hybrid partitioning scheme that partitions the inverted lists into a number of chunks that are equal in size and allocated to different nodes. The main aim of hybrid partitioning is to balance the load among all the nodes. They measured the load balance and concluded that hybrid partitioning performed better than document-based and term-based partitioning when the chunk size was small. Their results showed that for hybrid partitioning the smaller the chunk size the better the performance.

Badue et al.[2001] compared local index and global index partitioning. They concluded that the global index provided high concurrency while the local index provided high parallelism. The local index achieved better load balance than the global index and the global index performed less disks access than the local index. They used the global index to direct queries to their relevant nodes. Firstly they distributed the global index over the nodes such that all terms starting with a certain set of letters reside on one node other terms starting with different letters may reside on different nodes and so on. Secondly they directed queries to their relevant nodes by dividing query into sub-queries and send each sub-query to its relevant node.

This work differs from Xi et. al. [2002]. In their work it is difficult to direct queries to the relevant nodes because they divided each inverted list into chunks and then chunks were distributed randomly among nodes. Thus, the broker, when receives a query, it sends the query to all nodes because it has no information about the location of each term (i.e. no supper index was created). This results in low query throughput. Here, MDIRS is proposed to tackle this problem and make it easy to direct queries to their relevant nodes while the inverted lists are divided into chunks and chunks are distributed among nodes. This makes it easy to perform concurrent search as shown in Sec 3.

The main aim of this research is to investigate the effect of hybrid queries, as proposed in this paper, on query throughput, load balance, and the total query response time.

Moffat et. al. [2006] examined different methods to balance the load for term-distributed parallel architecture and proposed different techniques in order to reduce the query costs. They investigated different approaches to balance the load for a pipelined distributed retrieval system. In pipelined system, query evaluation is executed like this - suppose that we have N nodes and a query consists of three terms t1, t2, and t3 that reside on three nodes n1, n2, and n3. The query evaluation begins at n1 which retrieves the inverted list of term t1 sends it to node n2 which retrieves the inverted list of t2 and sends it with the posing list of t1 to n3 and so on. The disadvantage of this system is the load imbalance caused by a number of terms with heavily workload. They calculated the work load as $Q_t \times B_t$ where Q_t is the number of appearances of term (t) in a query batch and B_t is the inverted list length in bytes. To solve this problem they proposed to replicate those terms among nodes.

Cambazoglu et al. [2006] compared term-based and document-based partitioning with respect to query response time and query throughput. They found that document-based partitioning outperformed term-based partitioning when queries were performed sequentially. In addition, they concluded that term-based outperformed document-based partitioning when queries were performed concurrently.

The following differences are found between their work and our work:

1. We propose hybrid queries and show how they can be directed to their relevant nodes, Sec. 2.
2. We focus our work on improving the query throughput of hybrid partitioning by proposing the MDIRS. They focused their work on term-based and document-based partitioning.

System Architecture

Our system architecture consists of six nodes connected to a broker through 100 Mbps Ethernet switch. Nodes have CPU 2.80GHz and RAM 256MB.

2. RESEARCH METHODOLOGY

We perform a set of real experiments in a distributed IR system using the WT10G collection from TREC-9. First, we build the global index as follows:

1. The broker distributes the document collection among nodes document by document in round robin fashion.
2. Each node filters the document it receives from stop words and HTML symbols and then builds the inverted file in memory until a memory threshold from there the in-memory data is flushed to on-disk file [Heinz and Zobel 2003, Jaruskulchai and Kruengkrai 2002, Zobel and Moffat 2006].
3. Each node merges its on-disk files in one file.
4. Broker merges all inverted files from all nodes into one file called the global index.

In the above algorithm steps 2, 3 and 4 are performed in parallel.

After building the global index, the next step is to partition it across nodes. In term-based partitioning we distribute the global index such that all terms starting with the letters A through D reside on one node in order to allow queries to be directed to their relevant nodes.

Research Hypotheses

MDIRS relays on the following hypotheses. Hypothesis H1 states that "A h*ybrid query improves the query throughput and load balance and thus reduces the average query response time*". We define the hybrid query Hq as fusing more than one query into one query with no duplicated terms. A hybrid query is then divided into sub-queries or streams where each query stream is directed to the relevant cluster of nodes (Fig. 2 Sec. 3). Hypothesis H1 is formulated as follows –

Suppose that we have µ queries in the query buffer Qb and each query q consists of m terms t then we have:

$q_1 = t_{11}, t_{21}, \ldots, t_{m1}$
$q_2 = t_{12}, t_{22}, \ldots, t_{m2}$
.
.
$q_n = t_{1n}, t_{2n}, \ldots, t_{mn}$

where t_{mn} means term m of query n, then any hybrid query Hq may be any combination of the set T= $\{t_{11}, t_{21} \ldots , t_{mn}\}$ provided that all terms (t) in Hq are unique. Note that a hybrid query contains terms that belong to multiple queries.

Hypothesis H2 states that "*Directing query terms to the relevant cluster of nodes improve the searching time and thus reduce the average query response time of hybrid partitioning*".

In MDIRS, we divide the nodes into clusters where each cluster consists of two nodes. Each cluster of nodes stores all terms starting with a certain set of letters. For example, cluster 1 stores all terms starting with the letters A through D. The terms of the term-based index are distributed among a certain cluster of nodes such that each inverted list is divided into nearly two equal parts p1 and p2 and then p1 and p2 are distributed among the nodes of a certain cluster in round robin fashion. For example, p1 resides on node 1 of cluster 1 while p2 resides on node 2 of the same cluster.

In MDIRS hybrid queries are generated by merging a set of queries (5, 10, 25, or 50 queries) into one query then splitting this query into 3 streams where each stream contains all terms that start with a certain set of letters then streams are directed to the relevant cluster of nodes (Fig. 2 Sec 3).

So the advantages of hybrid queries are:

1. A hybrid query reduces the communication time between the broker and the nodes. Suppose we have m queries in Qb then the broker needs to send m message to all nodes. However, when hybrid query is used it is divided into n streams where n equals the number of nodes in the system and then each stream is sent to the relevant cluster of nodes. Note that n is less than m.
2. Hybrid query smoothens the skewness of the term frequency distribution of a set of queries. Jeong and Omiecinski [1995] concluded that partitioning by term resulted in load imbalance because some terms were more frequently requested in a query. Thus, nodes where these terms, associated with their inverted lists, were stored would be heavily utilized. Marin and Costa [2007] stated that load balance is sensitive to queries that include high frequency terms that refer to inverted lists of different sizes. Moffat et al. [stated that the distribution of inverted lists can be based on term frequency. They calculated the workload as $L = Qt \times Bt$, where Qt is the number of appearance of term t and Bt is the inverted list length in bytes. They stated that load imbalance was there because of some terms with heavy workload. Our observation is that the most frequent terms of a set of queries with long inverted lists may cause the load imbalance because the nodes that store the relevant inverted lists will be heavily loaded. As a solution to this problem we propose hybrid queries. Hybrid queries reduce the Qt

value to (1) by omitting duplicated terms therefore achieving better load balance because each term t generate workload equal 1× Bt thence nodes are no longer heavily loaded.

3. THE MODERATE DISTRIBUTED IR SYSTEM [MDIRS]

In Sec 3.1 we compare the result (the total query response time) from the MDIRS with that from hybrid partitioning proposed by Xi et al. [2002]. In 3.2 we measure the total query response time when using term-partitioning scheme.

MDIRS works as below:

1. We divide the nodes into clusters such that each cluster consists of two nodes. For example, C1 consists of node 1 & node 2, C2 consists of node 3 & node 4, and C3 consists of node 5 & node 6.

2. We distribute the global index among nodes as follows: Suppose that the size of the inverted list of a given term X equals S_p and the number of nodes in each cluster C equals N_c we distribute the global index among nodes such that the inverted list of a given term X is divided into k chunks where the chunk size equals

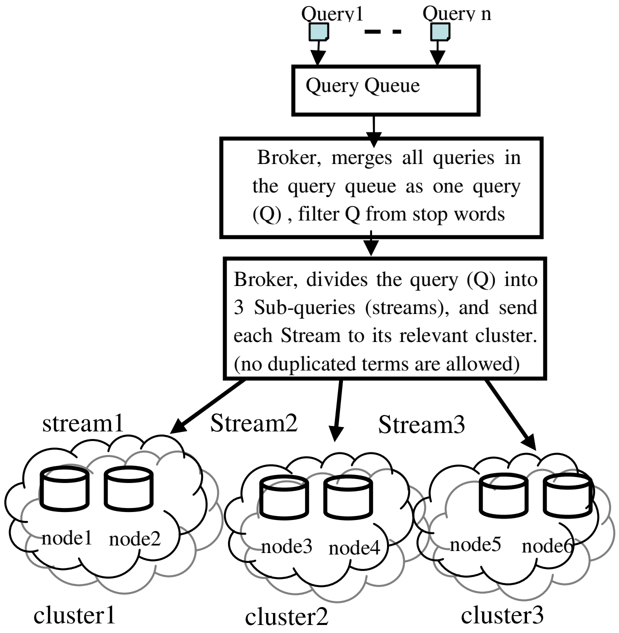
$$S_p / N_c$$

We choose the chunk size to be S_p / N_c in order to store nearly equal size of data on nodes and to make the size of each chunk as small as possible. This was because Xi et. al. [2002] concluded that hybrid partitioning performed better than document-base and term-based partitioning when chunk size was small. This was because retrieving small chunks achieved better I/O load balance. On the other hand, if they have six nodes in their system and choose the chunk size = $S_p/6$ then the inverted list of term X will be distributed among six nodes. This implies that it is difficult to direct queries to their relevant nodes because all terms with part of their inverted list may exist on all nodes and thus lead to low query throughput. To tackle this problem MDIRS assigns a set of terms that start with a certain letter(s) to a certain cluster in order to facilitate directing hybrid queries to their relevant clusters as shown in the following Table 2.

Table2: MDIRS-Term Partitioning

Cluster no.	**Node no.**	**Letters (streams)**
1	1,2	A, B, C, D, E, F, G, H, I
2	3,4	J, K, L, M, N, O, P, Q, R
3	5,6	S, T, U, V, W, X, Y, Z, Others

Fig. 2 System Architecture, MDIRS


Query1
Query n
Query Queue
Broker, merges all queries in the query queue as one query (Q) , filter Q from stop words
Broker, divides the query (Q) into 3 Sub-queries (streams), and send each Stream to its relevant cluster. (no duplicated terms are allowed)
stream1
Stream2
Stream3
node1
node2
node3
node4
node5
node6
cluster1
cluster2
cluster3

3. We performed 50 queries extracted from TREC-9 (451-500) as a single query Q. We filtered Q from stop words and all non-digits and non-character symbols. We prohibited any duplicated terms from appearing more than once (i.e. all terms in the hybrid query are unique).
4. We divided the hybrid query Q into 3 streams because we have three clusters of nodes. Each stream consists of all terms that start with a certain set of letters. This was done in order to facilitate directing hybrid query to the relevant cluster of nodes.
5. The terms in each stream were sorted in alphabetical order and then terms were directed to one cluster. For example, stream 1 which stores all terms that start with the letters A through I is directed to cluster 1. Fig. 2 shows the system architecture and three data streams directed to the relevant clusters of nodes.

3.1 Evaluation of MDIRS

In this section we compared MDIRS and hybrid partitioning as described by Xi et. al.[2002] with respect to the total query response time. We calculated the query response time as the time elapsed between the time the broker sends a query over nodes to the time the broker receives all inverted lists from all nodes. We focused our research on improving the retrieval time, by directing queries to the relevant cluster of nodes, rather than document weighting and sorting time.

We carried out two experiments using the WT10g. In the first experiment, we distributed the global index across nodes as described by Xi et. al.[2002]. We divided the inverted list of a given term into small chunks (k = S_p / 6). Each chunk is sent to a certain node in round robin fashion and then we ran 50 queries sequentially. Our results showed that the total query response time was 130,233 milliseconds.

In the second experiment, we used the MDIRS. We distributed terms as shown in table 2. We ran the same 50 queries and we set μ (the number of queries used to generate the hybrid query) to 50. The total query response time was 52,469 milliseconds.

This implies that the total query response time is dropped by 0.6 or 60%. Alternatively, we can say that MDIRS improved the system throughput of Xi et. al. [2002] by 60%. This was because our algorithm split the inverted lists into chunks as Xi et. al.[2002] did but it was also able to direct hybrid queries to their relevant nodes.

3.2 Improving the Total Query Response Time of Term-based partitioning Using Hybrid Queries

In this experiment, we distributed the global index among nodes as shown in table 3 below:

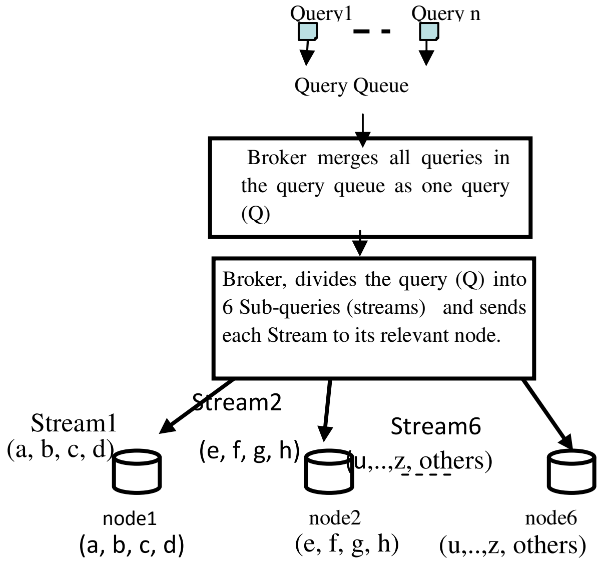
Table3: Term Partitioning

Node no.	Letters
1	A, B, C, D
2	E, F, G, H
3	I, J, K, L
4	M, N, O, P
5	Q, R, S, T
6	U, V, W, X, Y, Z, Others

As shown in Fig.3, we have six streams and each stream is directed to one node. The differences between this experiment and the experiment performed in Sec. 3.1 are given below:

1. The terms of the global index are partitioned among six nodes instead of three clusters.
2. In this experiment, nodes store full inverted lists while in the experiment performed in Sec 3.1 each node stores part of the full inverted list.

Fig. 3 System Architecture, Term Partitioning


Query1
Query n
Query Queue
Broker merges all queries in the query queue as one query (Q)
Broker, divides the query (Q) into 6 Sub-queries (streams) and sends each Stream to its relevant node.
Stream1
(a, b, c, d)
Stream2
(e, f, g, h)
Stream6
(u,..,z, others)
node1
(a, b, c, d)
node2
(e, f, g, h)
node6
(u,..,z, others)

3. In this experiment, we have six streams where each stream is directed to a different node. In other words, one node is responsible for retrieving the inverted list of a given term from disk. In the experiment performed in Sec 3.1, we create three streams, because we have three clusters of nodes, where each stream is directed to a certain cluster of nodes. In other words, two nodes participated in retrieving the full inverted list of a certain term.

We ran 50 queries and set μ to 50. The total query response time was 55,172 milliseconds. In section 3.1, we found that the total query response time of MDIRS was 52 seconds. In other words, MDIRS performs slightly better than the term-based partitioning when hybrid queries are used in both systems.

4. STUDY THE EFFECT OF INCREASING μ VALUE ON THE TOTAL QUERY RESPONSE TIME

In the previous section, we showed that hybrid query is composed of μ queries where μ = 2, 3, .. , or n queries extracted from the query buffer. In Sec 3.1 and 3.2, we set μ to 50 queries. In this section, we investigate the effect of varying μ value on the total query response time.

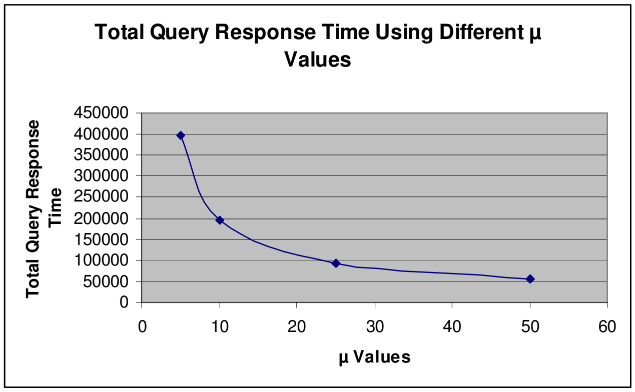
We distributed the terms of the global index as shown in Table 3 and ran a set of real experiments in order to investigate the effect of different values 5, 10, 25, and 50 of μ on the total query response time. The results are shown in Table 4 and Fig. 4.

Table4: Total Query Response Time using different μ values

μ Value (throughput factor)	**Total query response time (milliseconds)**
5	397385
10	196623
25	91579
50	55812

Table 4 and Fig.4 show that the total query response time is decreased when μ value is increased.

Fig. 4 Total Query Response Time



The above results prove research hypothesis H1.

5. STUDY THE EFFECT OF INCREASING μ VALUE ON LOAD BALANCE

In this section, we measured the load balance in terms of node utilization for different values of μ (1, 5, 10, 25, or 50 queries).

Node utilization is defined as the total amount of time the node is serving requests from the IR server divided by the total amount of time of the entire experiment, Xi et. al.[2002]. Node utilization is shown in Table 5a. The results showed that the relation between the load balance and µ is proportional relation, as described in Table 5a and Fig. 5a.

Table 5a: Node Utilization

Node label	µ =1	µ=5	µ=10	µ=25	µ=50
1	0.1606	0.0701	0.2153	0.5575	0.9137
2	0.2023	0.0969	0.2548	0.5889	0.9556
3	0.2263	0.1217	0.2937	0.6166	0.9894
4	0.2309	0.1283	0.3097	0.6271	0.9900
5	0.4326	0.1756	0.3541	0.6309	0.9936
6	0.5488	0.1839	0.3542	0.6323	0.9966

We monitored the load balance for each node in the system. We calculated the node utilization difference ΔU, where ΔU= MaxU – MinU, for each value of µ. For example when µ =1, MaxU = 0.5488 and MinU = 0.1606 thus ΔU = 0.5488 - 0.1606 or ΔU= 0.388 as described in Table 5b. Fig. 5a is drawn with the help of Table 5b.

Note that large value of ΔU means poor load balance. In general µ is increased as ΔU is decreased. In other words, we achieve better load balance (node utilization) as µ is increased.

Fig. 5a Load Balance (Node Utilization)

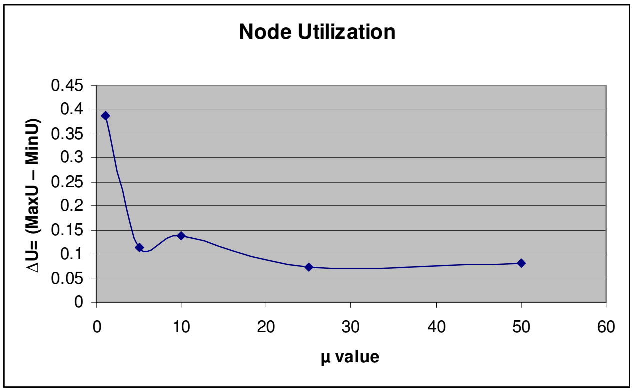


Table 5b: ΔU

µ value	ΔU= (MaxU – MinU)
1	0.388
5	0.113
10	0.138
25	0.074
50	0.082

6. CONCLUSIONS

MDIRS improved the total query response time and query throughput by 60% over hybrid partitioning. This was because MDIRS improved the searching time when queries were directed to the relevant clusters of nodes. This result proved research hypotheses H1 and H2. In addition, the results from this research showed that the relation between μ and the total query response time is reverse relation, and that the relation between μ and the node utilization is proportional relation.

7. REFERENCES

BADUE, C., BAEZA-YATES, R., RIBEIRO-NETO, B., and ZIVIANI, N., Distributed query processing using partitioned inverted files. *Proceedings.Eighth International Symposium* 2001, 10-20

BAEZA-YATES, R., and RIBEIRO-NETO, B., *Modern information retrieval* (ACM press, Addison-Wesley, New York, 1999).

CAMBAZOGLU, B.B., CATAL, A., AND AYKANAT, C., Effect of inverted index partitioning schemes on performance of query processing in parallel text retrieval systems, *ISCIS 2006, LNCS 4263*, c_Springer-Verlag Berlin Heidelberg 2006, 717–725

GULLI, A., AND SIGNORINI, A., The indexable web is more than 11.5 billion pages**,** *The 14th international conference on World Wide Web ACM*, New York, USA, 2005, 902-903.

HEINZ, S., AND ZOBEL, J., Efficient single-pass index construction for text databases. *Journal of the American Society for Information Science and Technology*, 2003.

JARUSKULCHAI, C., AND KRUENGKRAI, C., Building inverted files through efficient dynamic hashing. 2002.

JEONG, B.S., AND OMIECINSKI, E. (1995) Inverted File Partitioning Schemes in Multiple Disk Systems. *IEEE Transactions on Parallel and Distributed Systems*, 6(2), pp. 142-153. IEEE Press, USA.

MARIN, M., AND COSTA, G.V. (2007) High-Performance Distributed Inverted Files. In *Proceedings of the 16th ACM Conference on Information and Knowledge Management* CIKM'07. Lisbon, Portugal, 6-9 November 2007, pp. 935-938, ACM: New York, USA.

MOFFAT, A., WEBBER, W., AND ZOBEL, J., Load balancing for term-distributed parallel retrieval,Proceedings of the 29th annual international ACM SIGIR conference on Research and development in information retrieval, ACM, New York, USA, 2006, 348-355.

SULLIVAN, D., Searches per day. search engine *Watch*,http://searchenginewatch.com/reports/article.php/2156461, 2003.

XI, W., SOMIL, O., LUO, M., AND FOX, E., Hybrid partition inverted files for large-scale digital libraries, 2002.

ZOBEL, J., AND MOFFAT, A., Inverted files for text search engines, ACM, New York, USA, 2006.

Experiments for Accelerating IEEE 802.11i on Cyclone II FPGA

Chakib Alaoui, Ph.D[‡].
Taif University, KSA

Abstract

This paper presents hardware solutions for accelerating IEEE 802.11i. Several experiments were applied on the low-cost Cyclone II FPGA by using various architectures with different number of threads. The FPGA offloads the process of AES encryption from the master CPU. In addition, it offers the possibility of using several threads to run the AES encryption. Different optimizations have been applied on the hardware architecture of AES and on the basic unit of AES, in order to satisfy different constraints in terms of latency, area occupation and speed. Their performances are compared to AES software implemented on a NIOS II processor. A strong focus is devoted for the achievement of high throughput, which is required to support security requirements for the high bandwidth applications.

Categories and Subject Descriptors: B.2.4 [**Algorithms**], B.6.1 [**Memory Used as Logic**], B.7.1 [**Algorithms Implemented in Hardware**], C.1.4 [**Parallel Architectures**].
General Terms: IEEE 802.11i, AES, Cipher, WEP, FPGA. CYCLONE II

IJCIR Reference Format:
Chakib Alaoui, Experiments for Accelerating IEEE 802.11i on Cyclone II FPGA. International Journal of Computing and ICT Research, Vol. 4, No. 1, pp. 30 - 42. http://www.ijcir.org/volume4-number1/article 4.pdf.

1. INTRODUCTION

ENCRYPTION is a fundamental building block for data and telecommunication networks security. It makes electronic commerce, payment systems and transactions over networks possible. It is also a tool for privacy, trust, access control and corporate security, as defined by NIST [2001].

Effective implementations of cryptographic algorithms are essential for the realization of many real time communication systems. Performance has always been one of the most critical issues of a cryptographic function. It determines its effectiveness. It is evaluated by many metrics like latency, size and power consumption. Cryptographic computations are intensive and therefore they influence the performance of the whole system.

Wi-Fi (IEEE 802.11) is a common example of wireless communication. Schools, hospitals and public buildings are the major applications fields. However, the major drawback of current wireless LAN technology is the weak security measures in the standard 802.11 protocols (Wired Equivalent Privacy - WEP) as described by Graham S. J. [2003].

The solutions for WLAN security are delivered in two stages:

[‡] Author's Address: Chakib Alaoui, Faculty of Computers and Information Systems. Taif University. Taif – Al-Haweiah – P.O. Box 888 – Zip Code 21974 – Kingdom of Saudi Arabia – www.tu.edu.sa.

International Journal of Computing and ICT Research, ISSN 1818-1139 (Print), ISSN 1996-1065 (Online), Vol.4, No.1, pp. 30 - 42, June, 2010

- The first is the Wi-Fi Protected Access (WPA), which has been designed to allow software upgrade for existing WLAN systems.
- The second is the standard IEEE 802.11i, which provides the best available security, but requires hardware support as described by Graham S. J. [2003].

The AES (Advanced Encryption Standard) protocol requires complex algorithms for encryption/decryption processes, which makes them computationally extensive (AES requires about 350 lines of code, WEP implement RC4 algorithm that require 50 lines of code). At backbone communication channels or heavily loaded servers, it is possible to lose processing speed. This drops the efficiency of the overall system while running cryptography algorithms.

Moreover, the 802.11i standard specifies that AES should have its own coprocessor in order to speed up the encryption/decryption process (Morioka et al. [2002]). This implies that older existing wireless hardware cannot be upgraded via firmware to support IEEE 802.11i.

IEEE 802.11i (also known as WPA2) is an enhancement of the 802.11 standard specifying security mechanisms of wireless networks. The draft standard was ratified on June 24, 2004, and supersedes the previous security specifications. In addition to the introduction of key management and establishment, it defines encryption and authentication improvement (Morioka et al. [2002]). AES is a mandatory implementation of 802.11i. It was designed by D. Whiting, N. Ferguson and R. Housley. AES may be implemented in sizes of 128 bits, 192 bits or 256 bits, but 802.11i supports 128 bit AES only.

There are several AES implementation on FPGA's (Field Programmable Gate Arrays) available on the literature as was described by Alireza et al. [2004], Chodowiec et al. [2001], Chiueh et al. [2000], Dandalis et al. [2000], Elbirt et al. [2000], Elbirt A. J. et al. [2001], Gaj et al. [2000], Fisher V. et al. [2001], Ichikawa et al. [2000] and McLoone et al. [2001].

Its ASIC (Application Specific Integrated Circuit) counterpart was also widely studied by Lin et al. [2001], Lutz et al. [2002], Mayer et al. [2002], Morioka et al.[2002] and Morioka et al. [2000]. These implementations feature high speed and high costs suitable for high end applications only. Early AES designs featured pipelined architectures and limited resource utilization. These designs were described by Dandalis et al. [2000], Elbirt et al. [2000], Gaj et al. [2000] and Ichikawa et al. [2000]. Later FPGA and ASIC implementations showed better optimization, using dedicated on-chip memories implementing S-Boxes, as described in Alireza et al. [2004], Chiueh et al. [2000], Edney et al. [2003], Hodjat A. et al. [2004], Lin et al. [2001], Kimmo et al. [2003] and Verbauwhede I. et al. [2003].

The goal of this work is to design and evaluate an embedded coprocessor based on the NIOS II processor. It implements an efficient, cost-effective solution and optimized WiFi NIC (Network Interface Card). Different optimizations will be applied on the hardware architecture in order to satisfy different constrains in terms of latency, area occupation and security. This design uses Cyclone II FPGA (Field Programmable Gate Array) using Quartus foundation series.

2. IEEE 802.11i NETWORK INTERFACE CARD ARCHITECTURE

2.1 Network Interface Card components in IEEE 802.11

There are essentially four parts in a Wi-Fi LAN card shown in figure 1:

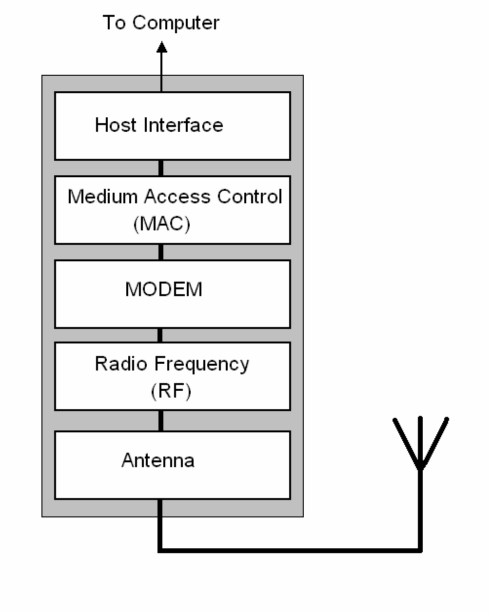


Figure1: NIC components in IEEE 802.11

1. Radio Frequency (RF) deals with the transmission and reception of the signal through the antenna.
2. MODEM extracts data from the received signal
3. Medium Access Control (MAC) is the heart of IEEE802.11 protocol. It has many functions like encryption/decryption of data, retransmission of lost data and data acknowledgement.
4. Host Interface is used to connect all the above to a computer like the USB or PCI bus.

Since IEEE 802.11i protocol is an enhancement to the MAC in terms of security, a closer look at the MAC components of IEEE802.11 is needed. Refer to figure 2.

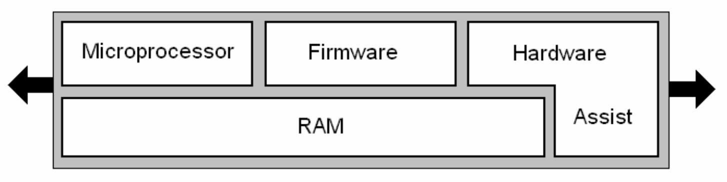


Figure 2: MAC Components Graham S. J. [2003]

MAC is made of a microprocessor who handles all the formatting and timing operations to control the protocol, the firmware is software that implements most functions and finally a hardware assist that speeds up the process of encryption/decryption of WEP. The hardware assist implemented in the existing NIC causes a critical problem for IEEE 802.11i; it cannot support AES.

2.2 WIFI Adapter Card IEEE 802.11i

2.2.1 WIFI Adapter Card IEEE 802.11i Block Diagram

The earlier NIC is static hardware and therefore its configuration could not be changed. The new design overcomes this issue and gives more flexibility for the longer term. FPGAs provide hardware reconfiguration possibility, i.e. flexible interconnect and short development time. They are very suitable as

hardware accelerators for AES. Another great improvement of the new WiFi adapter card is the network processor. It controls and processes all the network tasks so that the host CPU can be used for non-network related tasks such as video/audio processing. In this case, all networking tasks should be dropped into the FPGA (Encryption, Firewall, TCP|IP stack…). For evaluation purposes, NIOS II CPU from Altera Corporation was used as network processor.
Figure 3 shows a block diagram of the WiFi adapter card 802.11i

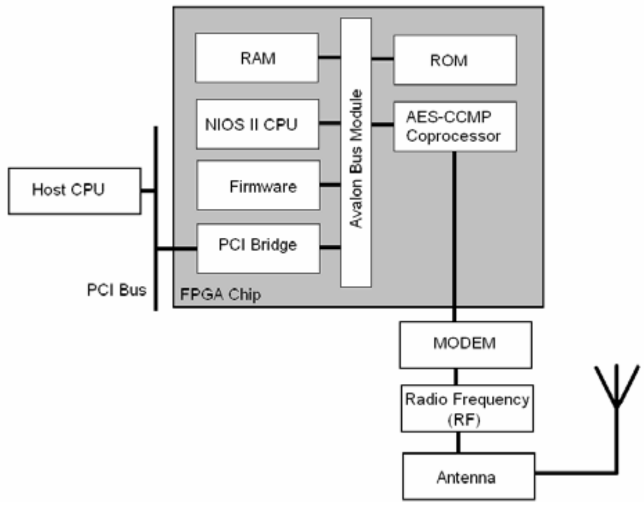


Figure 3: WiFi Adapter Card IEEE 802.11i

Avalon bus is an Altera's interface bus, used in NIOS II CPU. RAM contains unencrypted or decrypted data ready to be processed by AES coprocessor. The ROM contains all instructions necessary for the FPGA to work. During the boot-up phase, instructions are fetched from ROM since FPGA is volatile. PCI Bridge provides transparency between the host CPU and the NIOS II network processor. MODEM and Radio Frequency are off-chip.

2.2.2 The Choice of Network Processor

It was shown by Evangelos et al. [2001] that performance improvements made to general purpose processors do not translate necessarily into improved network performance, because these processors are not optimized for network data processing. Recent processors incorporates several innovations in their architecture, like larger caches, out of order executions, deep pipelines, and super-scale executions, all of which cannot necessarily be exploited by networking code. It was also concluded by the same author, that, even if the processor speed increases by Moore's law, network system speed increases in much lower pace. So it is necessary to develop an efficient co-processor dedicated for network tasks.

3. AES DESIGN AND IMPLEMENTATION

3.1 Key Scheduling by using Rijndael Algorithm

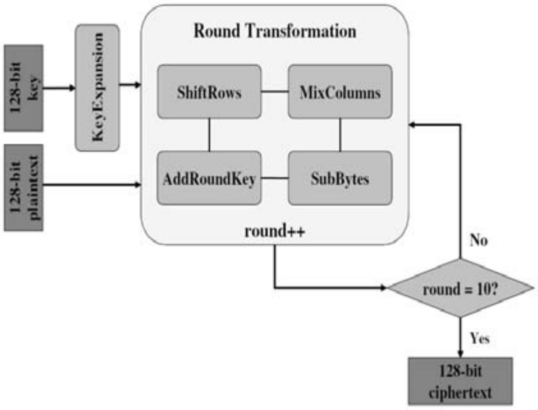


Figure 4: Algorithmic View of AES 128 from Zambreno et al. [2004]

The initial 128-bit key is fed into the KeyExpansion function which produces separate keys for each of the 10 required rounds. These rounds combine their scheduled keys with a two dimensional representation of the input using various transformations:

- **SubBytes( )** calculates a non-linear function independently on each byte of the state. The substitution used by this transformation can be more simply represented as a lookup table which is referred to as an "S-box".
- **MixColumns( )** separately modifies each column of the state in what is essentially a matrix multiplication operation. Fortunately, in the 8-bit finite mathematical field relied on by this class of block ciphers, multipliers can be replaced with simpler fixed-length shifts and XOR operations.
- **ShiftRows( )** cyclically shifts the bytes in the last three rows of the state. As this function requires no computational hardware it can be implemented on an FPGA as simple wiring.
- **AddRoundKey( )** adds the round key to the state using a bitwise XOR operation.

Key scheduling expands a 128-bit cipher key into a 170 Byte key. It utilizes operations like word rotation, word substitution, and exclusive OR with round constant. Figure 5, from A. SATOH [2001], shows a more detailed AES key scheduling architecture.

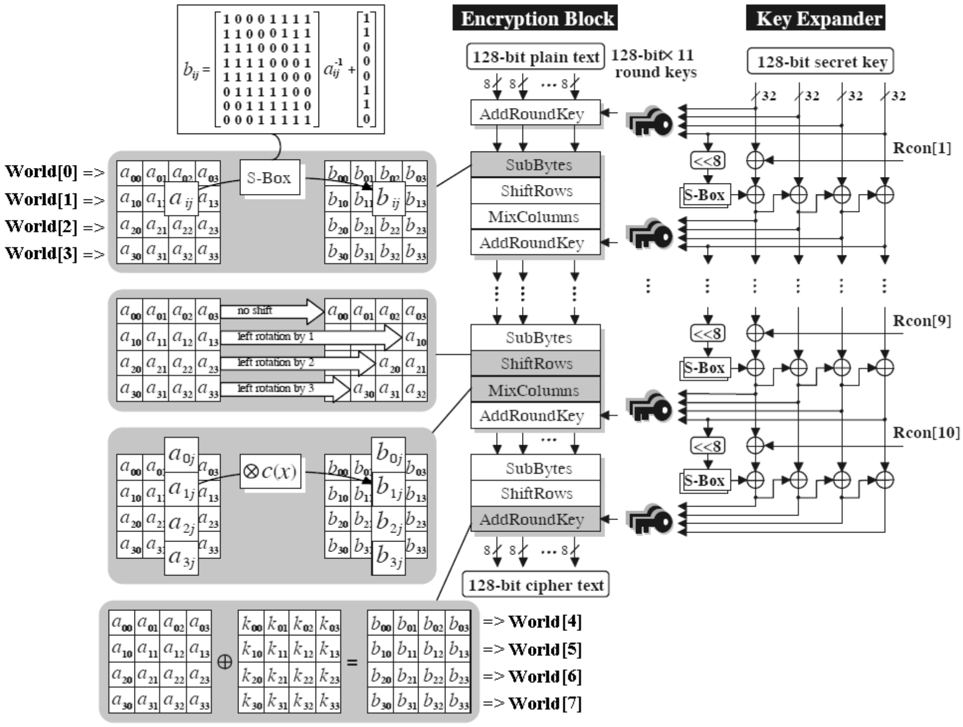


Figure 5: Detailed Key Scheduling Architecture.

The key expander in Figure 5 generates 11 sets of 128-bit round keys from one 128-bit secret key by using a 4-byte S-Box. These round keys can be prepared on the fly in parallel with the encryption process. In the decryption process, these sets of keys are used in reverse order.

First, the 128 bit cipher is divided into 4 sub-keys Word[0] to Word[3]. Then the shown operations are done to produce four new sub-keys Word[4] to Word[7]. Then this cycle is repeated 10 times in order to produce 160 Bytes. In total, a key of 176 Bytes is obtained.

In order to produce the new four sub-keys, the previous values of sub-keys are needed. So with this architecture, parallel execution is not possible.

In order to exploit the nature of parallelism offered by the FPGA hardware, an improved architecture is proposed using redundant computations. Refer to figure 6.

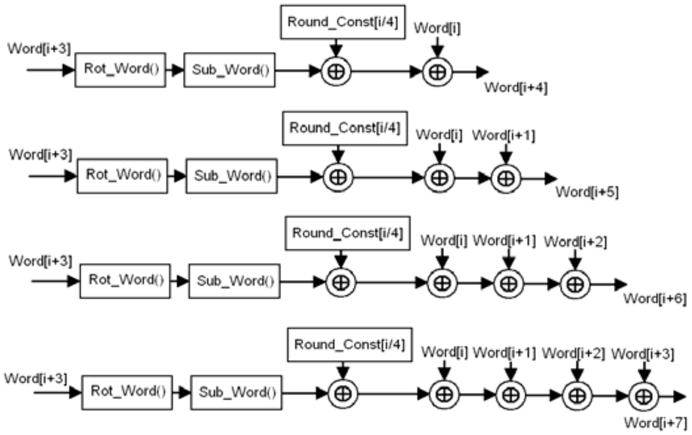


Figure 6: Modified Key Scheduling Architecture

3.2 AES Hardware Architecture

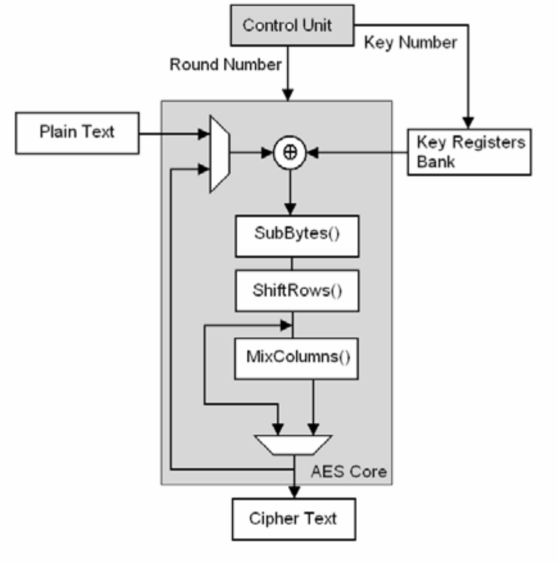


Figure 7: AES( ) Architecture

Figure 7 shows the AES() architecture, it is made of:
Control Unit: controls the components of the core (key registers bank and AES core). It also organizes the data flow by loading the specific data at the right round. After 10 rounds, the control unit will force the AES core to stop and output the cipher text.
Key registers bank: outputs the round keys. These sub-keys were computed offline.
AES Core: performs all the AES( ) modules described before.

3.3 Round Component Optimizations

Four different hardware/software optimizations have been developed. The first is based on the basic AES( ) unit which implements one round and executes ten times. This optimization employs the minimum hardware. The second optimization uses two AES( ) units and executes 5 times. The third implementation uses five AES( ) unites and executes them two times. Finally, the fourth implementation uses ten AES( ) units and executes them only one time. This last optimization uses the maximum hardware. Figure 8 shows the four different AES implementations.

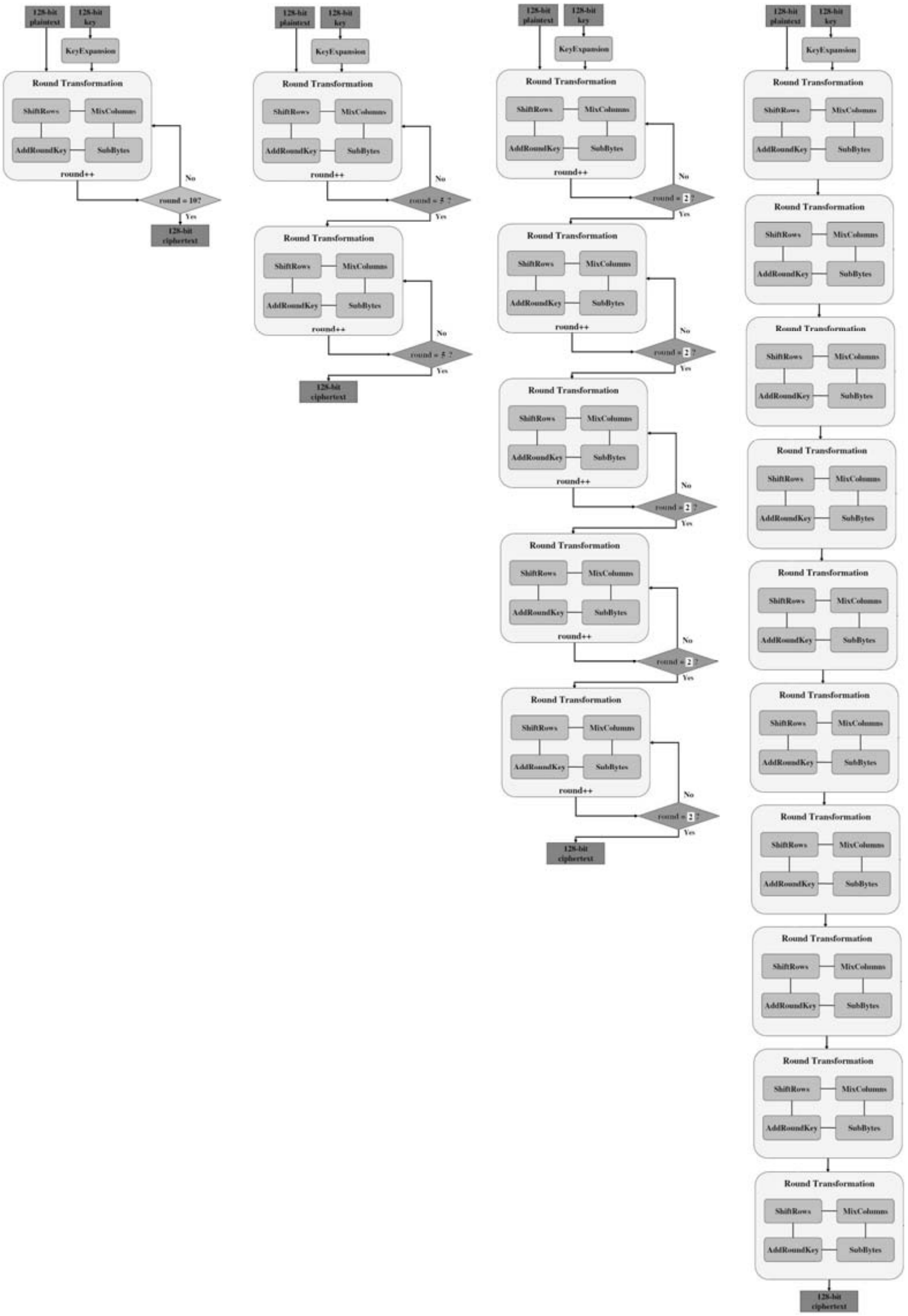


Figure 8: Four Different AES Implementations: 1 AES() x 10 exec., 2 AES x 5 exec., 5 AES x 2 exec. and 10 AES x 1 exec.

4. AES TESTING AND EVALUATION

The code has been synthesized using Altera's Quartus 6.1 development system. And Altera's Cyclone II chip was chosen for the implementation of the ciphers, because of its good performance among Altera's family and low cost.

4.1 AES Modules Synthesis

Table 1 shows the synthesis of the main components of AES, which are MixColumns() ver1, MixColumns() ver2, ShiftRows(), SubBytes() and SubBytes that implements RAM.

TABLE1: SYNTHESIS OF THE MAIN COMPONENTS OF AES

Total	MixColumns() ver1	MixColumns() ver2	SubBytes()	SybBytes() RAM
Logic Elements	**212**	**196**	**196**	**0**
Registers	**0**	**0**	**0**	**0**
Memory bits	**0**	**0**	**0**	**2048**
Cell Delay (ns)	**4.275**	**4.446**	**5.777**	**4.292**
Interconnect Delay (ns)	**11.263**	**11.394**	**9.090**	**7.955**
Worst Case tpd (ns)	**15.538**	**15.840**	**14.867**	**14.04**

There are two choices SubBytes() look-up table in the target device:
RAM: The values of the S-Box are loaded at the embedded RAM at configuration time.
Logic: S-Box can also be converted into logical representations and therefore implemented with logic elements. This option consumes chip area.

Data from table1 shows that the implementation of SubBytes() with embedded RAM gives significant improvements in the area/delay performance. Each 8 bits require 2048 bit of RAM, so in order to process 128 bits, 32768 bits for a 16x16 S-Box.

4.2 AES Cores Synthesis

Table 2 shows the synthesis results of AES key scheduling in Cyclone II

TABLE2: SYNTHESIS RESULTS OF AN AES KEY SCHEDULING WITH CYCLONE II

Implementation	Total
Logic Elements	**1102**
Registers	**269**
Clock Frequency (MHz)	**167.81**
Clock Cycles per Block	**11**
Period (ns)	**5.96**
Throughput (Mbits/s)	**1952.7**

Table 3 shows the synthesis results of AES without exploring the embedded RAM in Cyclone II

TABLE 3: SYNTHESIS RESULTS OF AN AES WITHOUT EXPLOITING EMBEDDED RAM IN CYCLONE II

Implementations	1 AES( ), 10 Iterations	2 AES( ), 5 Iterations	5 AES( ), 2 Iterations	10 AES(), 1 Iteration
Logic Elements	**4190**	**7385**	**17991**	**35624**
Registers	**270**	**151**	**134**	**132**
Memory Bits	**0**	**0**	**0**	**0**
Clock Frequency (MHz)	**61.69**	**56.30**	**21.67**	**10.47**
Clock Cycles per block	**12**	**7**	**4**	**3**
Period (ns)	**16.69**	**17.762**	**46.157**	**95.51**
Throughput Mbits/sec	**658.07**	**1029.48**	**693.44**	**446.72**
Throughput/Area (Mbps/TLE)	**0.157**	**0.139**	**0.038**	**0.012**

Table 3 shows that having 2 AES( ) units and executing them 5 times yields the highest throughput of **1029.48** Mbits/sec.

In order to exploit the RAM blocks that exist in FPGA, the four implementations were re-synthesized by allowing the tool to use the embedded RAM. This reduces the total logic elements used in the four implementations. Table 4 shows the synthesis results of AES that exploits the embedded RAM in Cyclone II

TABLE4: SYNTHESIS RESULTS OF AN AES EXPLOITING EMBEDDED RAM IN CYCLONE II

Implementations	1 AES( ), 10 Iterations	2 AES( ), 5 Iterations	5 AES( ), 2 Iterations	10 AES(), 1 Iteration
Logic Elements	**828**	**4156**	**14754**	**32322**
Registers	**270**	**151**	**134**	**134**
Memory Bits	**32768**	**32768**	**32768**	**32768**
Clock Frequency (MHz)	**62.83**	**61.32**	**23.01**	**11.17**
Clock Cycles per block	**12**	**7**	**4**	**3**
Period (ns)	**15.92**	**16.32**	**43.457**	**89.526**
Throughput Mbits/sec	**670.19**	**1121.28**	**736.32**	**476.58**

Since each S-Box needs 2K bits, 32768 bits are needed for 16 S-Boxes. Also, 16 blocks of RAM is exactly 32768 memory bits. Inferring S-Box as RAM blocks saves chip area in FPGA and improves the speed of the overall architecture.

5. AES ACCELERATOR: ARCHITECTURE, IMPLEMENTATION & RESULTS

5.1 Hardware Encryption of AES

AES computes the message authentication code and performs encryption in a single pass. That is encryption and authentication work in parallel.

Figure 7 shows the AES algorithm used in the 802.11i security protocol. It is responsible for the authentication that produces a 64-bit long MIC (Message Integrity Check). **IV** in the Initialization Vector, it contains the source address, the length of packet during the session and other fields. PN: Packet Number.

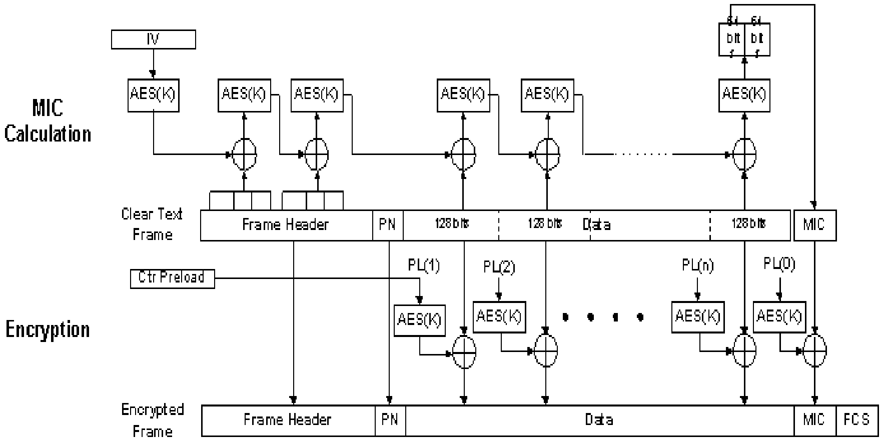


Figure 9: AES Algorithm from McLoone et al. [2001]

5.2. AES Implementation Results

In order to implement the AES core, the design that meets the lowest area with the highest throughput must be selected. The lowest area achieves a throughput of 670.19 Mbps (1 AES( ), 10 executions), while the second design (2 AES( ), 5 executions) achieves 1121.28 Mbps. Therefore these two different designs have been used to implement AES algorithm.
Figure 10 shows the performance and the cost comparison of these 2 implementations.

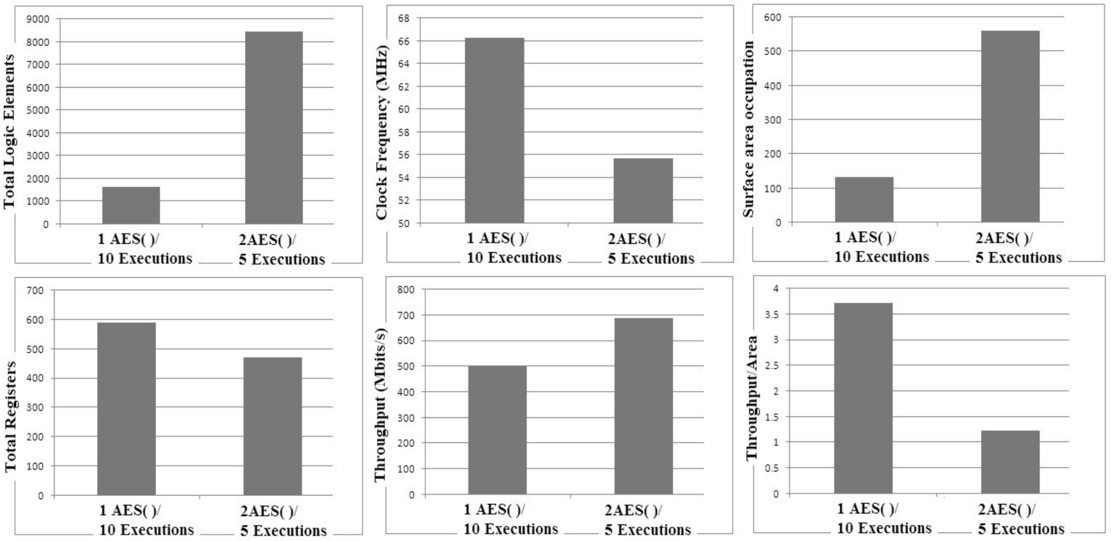


Figure 10: Performance and Cost Comparison of AES Implementations

6. CONCLUSION

In this paper a top-down methodology for implementing cryptographic block ciphers on FPGA was proposed and evaluated. Cyclone II series FPGA and NIOS II CPU make a low-cost and compact solution that adds high-speed features. Various architectures of AES units were implemented with strong emphasis on high speed performance. FPGA technology has matured to the point where high throughput can be easily obtained. The most interesting result achieved in this paper is a data rate of 688.16 Mbits/sec by using the standard and low cost Cyclon II FPGA chip of Altera. This encryption rate meets the performance requirements of the emerging cryptographic applications such as the high speed standard IEEE 802.11n which supports a data rate of 600 Mbps as supported by Evangelos et al. [2001]

7. REFERENCES

AKASHI SATOH, SUMIO MORIOKA, KOHJI TAKANO, AND SEIJI MUNETOH. A Compact Rijndael Hardware Architecture with S-Box Optimization. *Proc. ASIACRYPT 2001*, LNCS 2248, 2001, pp. 239–254.

ALIREZA HODJAT AND INGRID VERBAUWHEDE. 2004. A 21.54 Gbit/s Fully Pipelined AES Processor on FPGA. *IEEE Symposium on Field Programmable Custom Computing Machines, April 2004.*

ALIZERA HODJAT AND INGRID VERBAUWHEDE. 2004. Minimum area Cost for a 30 to 70 Gbits/s AES Processor. *Proceedings of IEEE Computer Society Annual Symposium on VLSI, Pages 83-88, February 2004*

CHODOWIEC P., GAJ K., BELLOWS P. AND SCHOTT B. 2001. Experimental Testing of the Gigabit IPSec-Compliant Implementations of Rijndael and Triple DES Using SLAAC-1V FPGA Accelerator Board. *Information Security Conference (ISC 2001), Malaga, Spain, 2001*

DANDALIS A., PRASANNA V.K. AND ROLIM J.D. 2000. A Comparative Study of Performance of AES Final Candidates Using FPGAs. *Cryptographic Hardware and Embedded Systems Workshop (CHES 2000), Worcester, Massachusetts, 2000*

ELBIRT A.J., YIP W., CHETWYND B. AND PAAR C. 2000. An FPGA Implementation and Performance Evaluation of the AES Block Cipher Candidate Algorithm Finalists. *Third Advanced Encryption Standard (AES3) Candidate Conference, New York, 2000*

ELBIRT A.J., YIP W., CHETWYND B. AND PAAR C. 2001. An FPGA-based performance evaluation of the AES block cipher candidate algorithm finalists, *IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Volume: 9 Issue: 4, August 2001*

EVANGELOS P. MARKATOS. 2001. Speeding up TCP/IP: Faster Processors are not enough. *The 21st IEEE International Performance, Computing and Communication Conference, 2001*

FISCHER V. AND DRUTAROVSKY M. 2001. Two Methods of Rijndael Implementation in Reconfigurable Hardware. *Cryptographic Hardware and Embedded Systems (CHES 2001), Paris, France, 2001*

GAJ K. AND CHODOWIEC P. 2000. Comparison of the Hardware Performance of the AES Candidates Using Reconfigurable Hardware. *Third Advanced Encryption Standard (AES3) Candidate Conference, New York, 2000*

ICHIKAWA T. AND MATSUI T. 2000. Hardware Evaluation of the AES Finalists. *Third Advanced Encryption Standard (AES3) Candidate Conference, New York, 2000*

J. ZAMBRENO, D. NGUYEN AND A. N. CHOUDHARY, “Exploring area/delay tradeoffs in an AES FPGA implementation,” *FPL 2004, LNCS3203, pp. 575-585, 2004.*

JARVINEN K.U., TOMMISKA M.T. AND SKYTTA J.O. 2003. A Fully Pipelined Memoryless 17.8 Gbps AES-128 Encryptor, *International Symposium on Field-Programmable Gate Arrays, Monterey, CA, 2003*

JON EDNEY, WILLIAM A. AND ARBAUGH. 2003. Real 802.11 Security: Wi-Fi Protected Access and 802.11i. *ISBN 0-321-13620-9, Chap9, July 15, 2003*

KIMMO U. JARVINEN, MATTI TOMMISKA AND SKYTTA J.O. 2003. A Fully Pipelined Memoryless 17.8 Gbps AES-128 Encryptor. *Proceedings of the ACM/SIGDA International Symposium on Field Programmable Gate Arrays, February 23-25 2003, Monterey, CA.*

LIN T.F., SU C.P., HUANG C.T. AND WU C.W. 2001. A High-Throughput Low-Cost AES Cipher Chip. *IEEE Asia-Pacific Conference on ASIC, 2002*

LUTZ A.K., TREICHLER J., G¨URKAYNAK F.K., KAESLIN H., BASLER G., ERNI A., REICHMUTH S., ROMMENS P., OETIKER S. AND FICHTNER W. 2002. 2Gbit/s Hardware Realizations of RIJNDAEL and ERPENT: A Comparative Analysis. *Cryptographic Hardware and Embedded Systems (CHES 2002), San Francisco Bay, CA, 2002*

MAYER U., OELSNER C. AND KOHLER T. 2002. Evaluation of Different Rijndael Implementations for High-end Servers. *IEEE International Symposium on Circuits and Systems (ISCAS 2002), 2002*

MCLOONE M. AND MCCANNY J.V. 2001. High Performance Single-Chip FPGA Rijndael Algorithm Implementations. *Cryptographic Hardware and Embedded Systems (CHES 2001), Paris, France, 2001*

MCLOONE M. AND MCCANNY J.V. 2001. Single-Chip FPGA Implementation of the Advanced Encryption Standard Algorithm. *Field Programmable Logic and Applications (FPL 2001), Belfast, Northern Ireland, UK, 2001*

MCLOONE W. AND MCCANNY J.V. 2001. FPGA Implementation Utilizing Look-up Tables. *IEEE Workshop on Signal Processing Systems, 2001*

MORIOKA S. AND SATOH A. 2000. A 10 Gbps Full-AES Crypto Design with Twisted-BDD S-Box Architecture. *IEEE International Conference on Computer Design: VLSI in Computers and Processors, 2000* National Institute of Standards and Technology (U.S.). 2001. Advanced Encryption Standard. Available at: http://csrc.nist.gov/publication/drafts/dfips-AES.pdf

MORIOKA S. AND SATOH A. 2002. An Optimized S-Box Circuit Architecture for Low Power AES Design. *Cryptographic Hardware and Embedded Systems (CHES 2002), San Francisco Bay, CA, 2002*

SIMON JAMES GRAHAM. 2003. Hardware-Based Secure WLAN Solution. *The University of Auckland, Part IV, September 15, 2003*

TZI-CKER CHIUEH AND PRASHANT PRADHAN. 2000. Cache Memory Design for Network Processors. *Proceedings of the Sixth International Symposium on High-Performance Computer Architecture, Pages 409-418, 2000*

VERBAUWHEDE I., SCHAUMONT P. AND KUO H. 2003. Design and Performance Testing of a 2.29-GB/s Rijndael Processor. *IEEE Journal of Solid-State Circuits, Volume: 38 Issue:3, March 2003*

A Consideration of Propagation Loss Models for GSM during Harmattan in N’djamena (Chad)

D.D. DAJAB AND NALDONGAR PARFAIT[*]
Department of Electrical and Computer Engineering,

AHMADU BELLO
University, Zaria, Nigeria.

Abstract

The paper discusses the influence of propagation environment in a GSM mobile network. It considers the measurement and prediction results for a special case of propagation, that is, the harmattan, in a live network. The harmattan precipitation intensity may be so great that visibility at ground level is reduced to less than a hundred meters by dust clusters. In this paper, the path loss during harmattan in N’djamena (Chad) is computed from the received signal strength at various distances for three major roads. The Hata and Free-space models were applied, and compared with received signal measurement data. The results indicate that measurement data and the Hata prediction model agree closely while the free space model generally underestimates the path loss phenomena. The significance here is that various forms of precipitation such as rain, snow, cloud and fog absorb and scatter electromagnetic energy leading to attenuation in its signal strength. The study indicates that harmattan precipitates do inflict attenuation significantly.

Categories and Subject Descriptors: C.4 [**Performance of Systems**]: Modeling Techniques; D4.8 [**Performance**]: Measurements; Modeling and Prediction; I6.4[**Simulation and Modeling**]:Model Validation and Analysis
General Terms: Harmattan, Propagation, Signal Strength, Pathloss
Additional Key Words: Global System for Mobile –Telephony (GSM),

IJCIR Reference Format:

D.D. Dajab and Naldongar Parfait. A Consideration of Propagation Loss Models for GSM during Harmattan in N’djamena (Chad). International Journal of Computing and ICT Research, Vol. 4, No. 1, pp. 43 - 48. http://www.ijcir.org/volume4-number1/article5.pdf.

1. INTRODUCTION

[*] Authors Address: D.D. Dajab and Naldongar Parfait, Department of Electrical and Computer Engineering, Ahmadu Bello University, Zaria, Nigeria.Email: dddajab@abu.edu.ng , pnaldongarmbete@yahoo.com

International Journal of Computing and ICT Research, ISSN 1818-1139 (Print), ISSN 1996-1065 (Online), Vol.4, No.1, pp. 43 – 48, June, 2010

In the savannah region, the atmosphere is affected by harmattan. In his work Dajab,[2005], defined the harmattan as a weather condition in the tropics in which dust particles (precipitates) are blown up into the air by winds defined as air in horizontal motion relative to the earth surface and pushed southwards from the Sahara desert by the northeast winds. It has been observed that Harmattan intensity may be so great that visibility at ground level is reduced to less than a hundred meters by the dust clusters. Harmattan occurs in Chad during the dry season that is, between the months of November and March.

2. REVIEW OF RELATED LITERATURE

Harmattan dust with its micro size particles and harmattan dust clusters resemble that of fog and the space they cover can be considered, according to Neyman, [1981] as a dielectric since the clusters consist predominantly of quartz layer which non-coherently scatters and disturbs propagation of RF signals. The result is that the incoming radio signal which enters the receiver circuitry varies in magnitude. These variations are attributed to changes in propagation conditions. In extreme cases it can lead to complete cancellation of a signal at the receiving point. These signals variation can occur fast or slow and the speed at which they take place is known as "rate of fading" [Shittu, 2006]. The reception of microwaves depends on the propagation environment between a transmitter and a receiver. Propagation models can be used extensively in network planning, particularly for conducting feasibility studies and during initial deployment. They are also very useful for performing interference studies and optimization of radio resources [Mishra, 2004].Attenuation is less pronounced at frequencies around 3GHz, however, to a communications system designer, attenuation due to precipitation and atmospheric gases at frequencies above 1GHz is very important[Eyo et al, 2003].

3. METHODOLOGY

Pavlos et al. [2007] provides that Measurement reports over the GSM network are transmitted periodically (480ms) from the Mobile Terminal (MT) to the Base Transceiver Station (BTS) on the Stand Alone Common Channel (SACCH) assigned to each communication, according to which the measured Received signal Level (RXLEVs) from the serving BTS and from a neighbor BTS (in situations requiring handover) are submitted. In this paper, RXLEV data or signal strength data have been collected for a year from the Chadian Celtel GSM network in Djamena. These were collected experimentally by Naldongar, [2007] using vendor Transmission Evaluation and Monitoring System (TEMS) and drive testing equipment for certain urban routes . The losses in signal strength that do occur during transmission from the Transmitting antenna T_X to the Receiving antenna RX are given by the path loss, while the receive power is the result of the path loss phenomenon. It is anticipated that propagation loss models would provide physical explanations for results obtained from measurements. These were conducted within the period of harmattan. The models used in the work are considered below.

3.1 Free Space Model

The path loss may be obtained from the effective isotropic radiated power (EIRP) using the expression [Godara, 2002]:

$$L_p = \text{EIRP} - S_R \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \qquad (1)$$

Where S_R is the measured received signal strength also in dBm and $EIRP$ is the Effective Isotropic Radiated Power also in dBm

L_p denotes the loss associated with propagation of electromagnetic waves from the transmitter to the receiver, called the free-space path loss and is given by:

$$L_P = \left[\frac{\lambda}{4\pi d}\right]^2 \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad (2)$$

$$P_P = 20Log\left[\frac{\lambda}{4\pi d}\right] + P_T + G_T + G_R(dBm) \quad \ldots \quad \ldots \quad (3)$$

$$L_P = 20Log\left[\frac{4\pi d}{\lambda}\right](d\,B) \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad (4)$$

3.2 COST- 231 Hata Model

This is a popular model for predicting the path loss of mobile wireless systems of not more than 10km between the transmitter and the receiver. The model was described by Hata for the prediction of path loss and land mobile radio of not more than 1500MHz.It was later modified by the COST-231 project to include predictions of path loss up to 2000MHz and the provision of correction factors for urban, suburban and rural areas. The basic equation for path loss model in dB for urban areas is [Okumura, 1968; Hata, 1980]:

$$L_P = A + B\log(d) + C \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad (5)$$

$$A = 46.3 + 33.9\log(f_c) - 13.82\log(h_b) - a(h_m) \quad \ldots \quad \ldots \quad (6)$$

$$B = 44.9 - 6.55\log(h_b) \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad (7)$$

$$a(h_m) = 3.2[\log(11.75h_m)]^2 - 4.97 \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad (8)$$

4. RESULTS AND DISCUSSIONS

The suite of measurements performed in the environment in which the radio (GSM) system is deployed is necessary for the validation of radio wave propagation tools or predicted results. When characterizing path loss in outdoor radio channels, the free space and Hata models are a common approach. In this paper measurements carried out were used as the basis for comparison between propagation loss predictions with these two selected models as represented in Figs 1 to 3.Comparing the loss predictions indicate a mean difference of 20dB between the two models consistently. Fig 1 shows that the Hata model below 1.5km slightly underestimates while above 2km also slightly overestimates the path loss scenario. As evident from Figs 2 & 3 whereas the Hata model closely predicts the path loss compared with measurement, the free-space model significantly underestimates the path loss along the streets considered in the experiment.

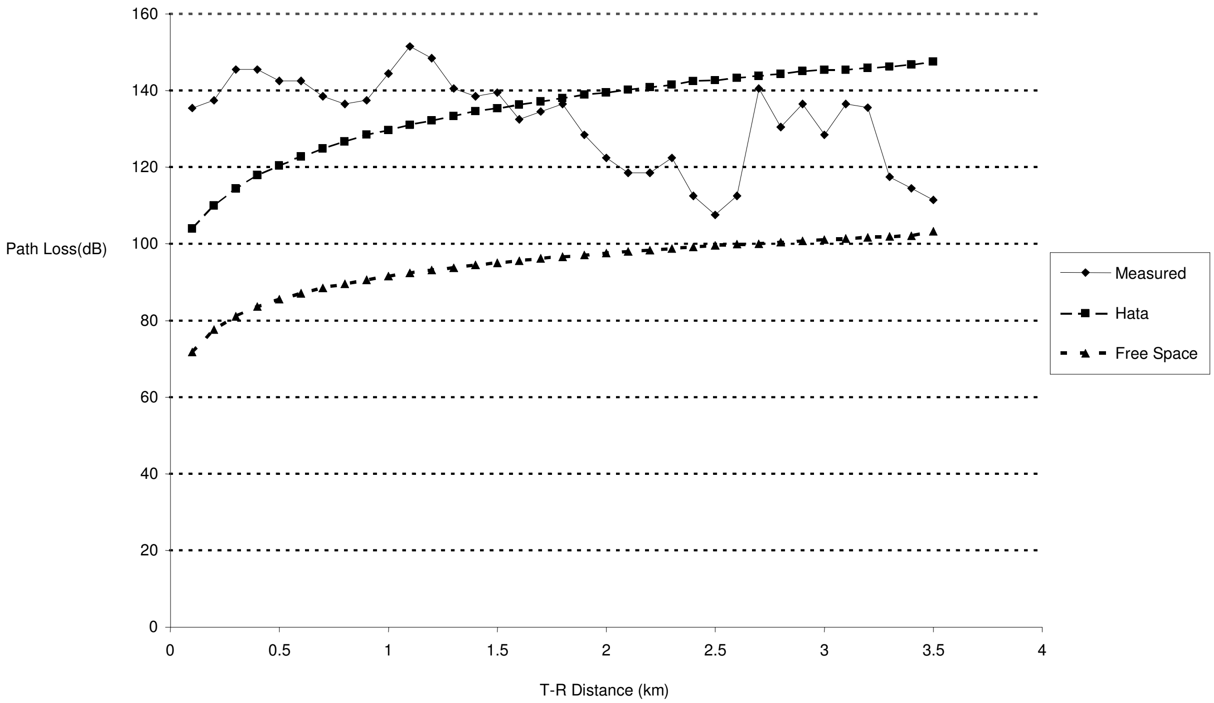


Figure 1: PATH LOSS VARIATION ON MOURSAL ROAD FOR MARCH, 2006

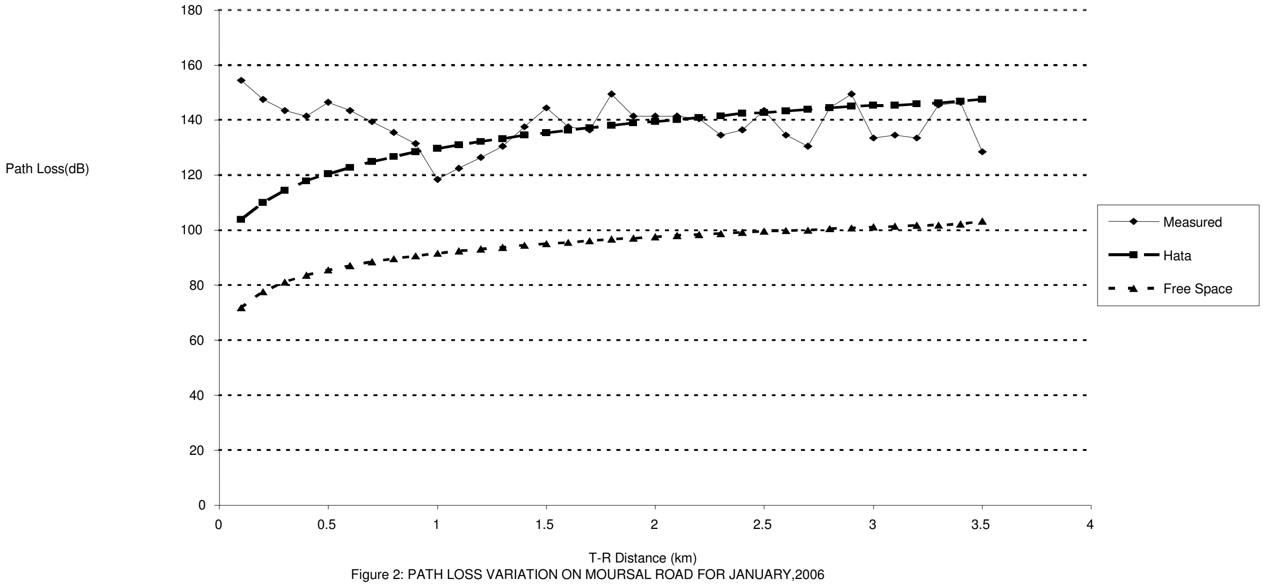


Figure 2: PATH LOSS VARIATION ON MOURSAL ROAD FOR JANUARY,2006

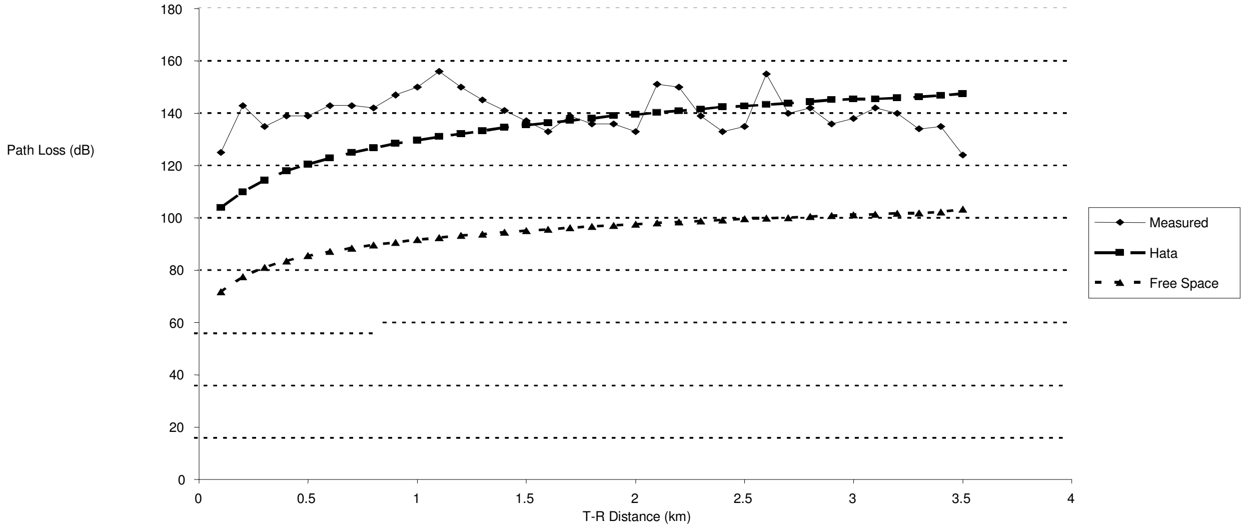


Figure 3: PATH LOSS VARIATION ON CHAGOUA ROAD FOR NOVEMBER,2006

The significant differences in the predictions can be explained by reasons of the many phenomena affecting propagation such as interference from neighbor base stations, difference in fading and shadowing patterns of the received power as a function of distance along the streets considered. Path loss in real propagation environments such as considered here increase depending upon obstructions in the environment, such as terrain, buildings, foliage and precipitations like the harmattan dust clusters which is the predominant factor of all these. In their work, Yu-Huei et al ,[2003] observed concerning field measured results that the effect of the precipitations is that the changes and fluctuations obvious in the measurement results indicate that the radio coverage field strength is poor and the path loss fluctuates constantly reflecting that. It can also be due to varying and environmental factors at the various base stations and the increase of dust particles in the air which constitute an obstacle between transmitter and receiver. This results in a lower signal level at the distant end than anticipated due to path loss and the Fresnel zone is literally blocked, even if the other antenna (Mobile) in the distance can also literally be “seen”. It is, however, still possible to get a signal under these conditions because in the access part, GSM networks operate in what is called the Radio Frequency (RF) part of the spectrum which exhibit multipath effect as against the Microwave Frequency (MF) obtained in the backhaul and transmission parts of the network which are Line-Of-Sight (LOS) dependent.

5. CONCLUSION

There are two major motivations for performing measurements: i) propagation surveys for the purpose of radio system development and deployment and ii) model validation for propagation prediction tools. In the foregoing study, the later motivation has been carried out, even as it is found that atmospheric particles density do affect GSM signal strength especially during harmattan period in N’djamena. Taking into account the micro size of particles in the harmattan dust, and on the other hand, it’s quite high density resembling that of fog, the particles covering the atmosphere may be considered as a dielectric thereby inducing some electrostatic conditions. The effect on signal propagation demands that in regions with these conditions higher gain antennas need to be deployed in addition to the introduction of precisely defined local correction factors for consistent quality of service in and out of season.

6. ACKNOWLEDGEMENTS

We wish to acknowledge the cooperation of Celtel Network of Chad Republic for assisting with test equipment and provision of enabling environment for the study as well as Ahmadu Bello University,Zaria Nigeria, where the research was defended in partial fulfillment for the award of a Masters degree in Electrical Engineering

8. REFERENCES

DAJAB, D.D. 2005. Characterisation and Modelling of 900MHz Indoor Wireless communication channels in the savannah region. PhD Dissertation, Electrical Eng. Dept. Ahmadu Bello University, Zaria. 45-52; 144-152.

EYO,O.E., MENKITI.A.I., UDO.S.O. 2003. Microwave Signal Attenuation in Harmattan Weather Along Calabar-Akampkpa Line-Of-Sight Link. Turk Journal of Physics,Vol.27, 153-160.

GODARA, L.C. 2002. Handbook of Antennas in Wireless Communication. CRC press LLC.

HATA, M. 1980. Empirical Formula for Propagation Loss in Land Mobile Radio Service, IEEE Transactions on Vehicular Technology, Vol. VT-29, No3, 317-325.

MISHRA, A.R. 2004. Fundamentals of Cellular Network planning and optimization. John Wiley and sons Ltd.

NALDONGAR, P. 2007. An assessment of the Impact of Harmattan Particles on Microwave Propagation in the Savannah Region, M.Sc thesis, Electrical Engineering Department, Ahmadu Bello University, Zaria.,(unpublished).

NEYMAN, A.B. 1981. Study of short wave reception in Zaria.PhD dissertation, Electrical Engr Dept. Ahmadu Bello University,Zaria. 1-2; 62-63

OKUMURA, Y., OHMORI, E., and KAWANO, T. 1968. Field Strength and its Variability in VHF and UHF Land Mobile Radio Services. A Review of the Electrical Communications Laboratory, Vol 16, 825-873.

PAVLOS, F., SOFOKLIS, K ., and GEORGE, K . 2007. Enhanced Handover Performance in Cellular Systems based on Position Location of the Mobile Terminals. Seminar paper, Telecommunications Laboratory, National Technical University of Athens. 2-3.

SHITTU, W. A., 2006. Cellular Mobile Radio propagation characteristics. M.Sc thesis, Electrical Engineering, Ahmadu Bello University, Zaria.

YU-HUEI, T., WEN-SHYANG, H., and CE-KUEN, S. 2006. The Influence of Propagation Environment in a Live GSM Network. Research Paper, Department of Electrical Engineering, National Kaohsiung University of Applied Sciences, Kaohsiung, R.O.C.3-5.

Internet Utilization: A Case of Connected Rural and Urban Secondary Schools in Kenya

GEORGE KIBET KIPTALAM[*]*
Aga Khan University, Nairobi Campus, Kenya

ANTHONY JOACHIM RODRIGUES
School of Computing & Informatics, Chiromo Campus, University of Nairobi, Kenya

Abstract

This paper looks at the utilization of the Internet among teachers and students in connected rural and urban secondary schools in Kenya. A conceptual framework composed of variables which can explain Internet utilization in Kenyan secondary schools is established and measured. Instruments based on this framework were used in the survey and covered 11 schools with school principals, teachers and students as respondents. Findings show that use of the Internet and its integration in teaching and learning in secondary education is increasing with its use more pervasive among students and teachers as a means of communication and for information searching. Internet access rates for teachers and students have been observed to be much higher in educational institutions that have made effective ICT investments in education, translating into better utilization of ICT related technologies. Strategies are suggested on how to utilize the Internet to improve educational outcomes, and recommendations given on issues that touch on ICT access and infrastructure; human resources and training; policy environment; financing and ICT investment; curriculum development and locally relevant content.

Categories and Subject Descriptors: K.3.0 [Computing Milieux]: Computers and Education
Keywords: Internet utilization, access, secondary schools

IJCIR Reference Format:

Kiptalam, G.K and Rodrigues, A.J. Internet Utilization: A Case of Connected Rural and Urban Secondary Schools in Kenya. International Journal of Computing and ICT Research, Vol. 4, No.1, pp. 49 - 63. http://www.ijcir.org/volume4-number1/article6.pdf

1. INTRODUCTION

There is lack of cross-country evidence on the utilization of Internet in different sectors of the economy in African countries. In some cases the evidence is non-existent due to recent developments, the rapid revolution of ICTs and methodological challenges that include a deficiency of assessment variables and models of causality. Attempts to measure or assess the utilization and impacts of ICT in Africa have

[*]Author's Address: George Kibet Kiptalam, Aga Khan University, Nairobi Campus, Kenya (george.kiptalam@aku.edu)
Anthony Joachim Rodrigues, School of Computing & Informatics, Chiromo Campus, University of Nairobi, Kenya (tonyr@uonbi.ac.ke)

International Journal of Computing and ICT Research, ISSN 1818-1139 (Print), ISSN 1996-1065 (Online), Vol.4, No.1, pp. 50 – 63, June, 2010

been hampered by insufficient empirical data to indicate any impact of ICT on sector productivity. Most of the research and projects have tended to focus on information infrastructure issues, while few have been undertaken to measure the extent of Internet utilization as well as ICTs in Africa, particularly in education [Kenya SchoolNet, 2003].

In this paper, the concept Internet "utilization" is preferred as it considers the actual use of the Internet as compared to the availability of resources. Utilization of the Internet depends on the capacity to use the available services. Such capacity may be measured in terms of the number of years in experience one has using computers, the number of computer applications one has mastery over, as well as general levels of education and intelligence.

The conceptual framework was adapted from the National Research Council [National Research Council, 1998] and is based on the utilization of the Internet rather than its penetration and the resultant impacts. This adapted framework uses modified indicators and sub-indicators that have been derived from an e-readiness assessment tool originally developed by the Centre for International Development (CID) at Harvard University, and which was modified for use in assessing the e-readiness of higher education institutions in Kenya [Kashorda et al., 2007]. The tool organizes the assessment of numerous factors that determine the Networked Readiness of a community in the developing world. It makes use of the Networked Readiness Index (NRI) that measures not only the regulatory and national infrastructure but also usage by government, businesses and individuals. The indicators and sub-indicators are categorized into four domains: accessibility; usage; individual and society; and policy and strategy. The resulting framework is in the form of Internet supply and demand, in which impacts of the Internet can best be understood by measuring the extent of Internet usage. Indicators are then offered as tools to help measure the direct and indirect usage of Internet.

The use of ICT in education has the potential to enhance the quality of teaching and learning, the research productivity of the faculty and students, and the management and effectiveness of institutions [Kashorda et al., 2007]. However opportunities for realizing the benefits of using ICT in education face a number of challenges in the developing countries. Access to ICT facilities is a major challenge facing most African countries, with a ratio of one computer to 150 students against the ratio of 1:15 students in the developed countries. In Kenya, the ratio for universities and colleges is 1:45 while access at the primary school level is much more limited at 1:250 [Ministry of Education, Kenya, 2006]. The Education Management Information System (EMIS) survey of 2003/2004 indicated that over 70 per cent of the secondary schools in Kenya required functional telephones. Furthermore 90 per cent of such schools needed to establish Local Area Networks (LANs) in order to improve sharing of learning resources. As of 2008, there were 6,566 secondary schools in Kenya, of which 4,261 were publicly funded and the rest 2,305 privately funded with a total student enrolment of 1,382,211 and total teaching staff of 43,016 [Kenya National Bureau of Statistics , 2009].

With regard to the status of ICT in Kenyan secondary schools one of the earliest ICT projects in the education sector was implemented by the Aga Khan Foundation (AKF), which was responsible for introduction of computers in Kenya's secondary schools through the Computers in Education Project in Kenya (CEPAK) in 1983. The first phase began with the Aga Khan Academy receiving five computers and the necessary software from AKF [Makau & IDRC, 1990]. The second phase introduced computers to four public secondary schools in Nairobi. During the three year period of this second phase, the project was studied by an independent research team [Makau & IDRC, 1990]. This large-scale study on the use of computers in secondary schools in Kenya found that most computer-assisted lessons were observed to be in mathematics and the sciences. However, it was also found that in the majority of computer-assisted lessons teachers tended to be passive, thus leaving students to do whatever they chose. It found that some students regarded both formal and informal sessions on the computer as time for relaxation as opposed to serious learning. This approach to computer-assisted lessons was explained as being a result of the perception of the computer as an object of study; more exciting and potentially more rewarding than integration of the technology into the existing curriculum. The research also found that computer studies lessons were conducted in the computer laboratory, thus they seemed to have priority over computer-assisted lessons in other subjects. With regard to gender, female students were more disadvantaged than their male counterparts when exposure outside the school (i.e. at home or elsewhere) was considered. The proportion of males that claimed to come from a home which owned a computer was nearly twice that of females, while 21% more boys than girls claimed to have used a computer outside school. In mixed schools surveyed female students claimed to have received less in-school exposure than the males.

A large scale study by SchoolNet in which 69 secondary schools responded found that only 46 per cent of the sampled schools had computers, with availability of Internet and facsimile rare in these schools [Kenya SchoolNet, 2003]. The findings also indicated that email was yet to be recognised as a tool for collaboration among students and teachers, and only one school had a website while another two reported having networked all their computers to the Internet. It went on to affirm that in these schools, access to the Internet was severely limited and when available was only for administrative use. The study found that almost 40% of schools had less than 10 computers, and therefore inadequate for teaching and learning. More than 20 per cent had less than 5 computers, indicating that the computers were mostly for administrative use. Only a third of schools studied had dedicated computer laboratories. The study also found that some schools were making use of very old equipment and there was dependency on donations of computers as opposed to sourcing locally. Similar to findings of the CEPAK study, the SchoolNet Kenya study revealed a significant difference in the quality and use of the computers in schools, depending on the gender of students there. Girls' schools were found to have the lowest numbers of computers, almost a third of that of boys' schools. Furthermore, there were fewer computers located in a computer laboratory in girls' schools, indicating their use predominantly in administration in girls' schools. The study concluded that fewer girls were being exposed to computers than boys. Consequently, the research concluded that girls would be marginal players in the emerging information society.

Another study by Pádraig Wims and Mark Lawler studied the implementation of ICT projects in selected educational institutions with a view to making recommendations on how such projects can be deployed and supported. The findings were from two secondary schools – St. Patrick's High School and Singore Girls' Secondary School – and an agriculture training college, Baraka Agricultural College. The findings reported that half of Keiyo District's 32 secondary schools had at least some computer equipment installed, with over half of these schools offering computer lessons to their students [Wims & Lawler, 2007]. The average number of computers in the schools that offered computer lessons was 15, the highest recorded being 21, and the lowest at 10. The ratios of students to computers in the institution surveyed were: St. Patrick's, 25:1; Singore, 32:1 and Baraka, 4:1. In St. Patrick's, the computer laboratory had 16 working computers, with an average of 1.5 students per computer. Singore had a laboratory of 10 computers, and an average class size of 15, or a ratio of 1.5 students per computer. In Baraka Agricultural College, students had access to a computer laboratory of 12 computers. Only 12 students attended classes at any given time, allowing for a ratio of 1:1. Of the institutions studied, it was only Baraka Agricultural College that was served by a fixed line. Though the institutions had email addresses, it seemed this was only available for administrative use. And as regards website, it was St. Patrick's and Baraka that had websites, with the former appearing not to be updated regularly. Funding for the deployment of the ICT infrastructure was locally for the secondary schools, with considerable donor support for the training college. It was found that half of the students surveyed in St. Patrick's had used a computer before joining the school; however the figure for the girls at Singore was much lower at 30 per cent.

These studies used different conceptual models to understand the extent of ICT utilization, and in turn inform on the benefits and impacts of ICTs in Kenya. There is very limited information available on the experiences of African learners, teachers and school managers on the use of ICTs. Very limited information is available too, on the supply chain of the ICTs in schools – the nature and extent of government ministry involvement, the involvement of the parent and residential communities in which the schools are located and the role of the private sector. While noting the underlying common theme of understanding the dynamics of supply and demand to explain the benefits of ICTs in education, often overlooked is the usage of such technologies that are likely to play a major role in determining the benefits and impacts being studies.

2. METHODOLOGY

The study was a cross sectional descriptive survey using quantitative approaches to data collection, analyses and reporting. A survey design was used to guide the research process and participants were drawn from 11 secondary schools that were connected to the Internet, and were from rural and urban areas of Kenya. The study involved secondary schools from Nairobi and Rift Valley provinces.

The respondents were selected using the linear simple sampling approach and required the class register as sampling frame which was available in these schools.

Since there were no estimates available of the target population using the Internet in these schools, 50 per cent was used as recommended by Fisher [Fisher et.al, 1999].

The following equation was used to obtain the estimate (see equation 1 and 2).

$$n=Z^2pq/d^2 \qquad ...eq.1$$

Where:

n=the desired sample size (when population is greater than 10,000)
z=the standard normal deviate at the required confidence level, set at 1.96
p=the proportion in the target population estimated to have characteristics being measured. Since there is not available estimate, we will use 50 per cent (0.5)
q=1-p
d=the level of statistical set

$$n=1.96^2(0.5)(0.5)/(0.05)^2 \qquad ...eq.2$$

n=384

But since the entire population (N) is less than 10,000, the required sample size will be smaller. We got the final sample estimate (n_f) by using the following equation (see equation 3):

$$n_f=\frac{384}{1}+\frac{384}{1920}=385 \qquad ...eq.3$$

However a final sample of 752 (11.3%) students was randomly selected from the eleven schools with a student population of 6,681 to take into account the different categories of schools and Internet accessibility. Also selected for random sampling were 132 (28.2%) teachers respondents from of a total population of 468 teachers and all 11 (100%) principals from the 11 schools sampled. The response rates were 100% for principals (n=11), 74.2% for the teachers (n=98) and 91.9% for the students (n=691). There were 6,566 secondary schools (4,261 public and 2,305 private secondary schools), with student enrolment of 1,382,211 (635,698 girls and 746,513 boys) and 43,016 teachers employed (15,761 female teachers and 27,838 male teachers) as at 31 December 2008 [Kenya National Bureau of Statistics, 2009].

Table 1 Profile of the students and teachers

			Research Group	
			Frequency	**%**
Students	**Gender**	Female	469	67.9
		Male	222	32.1
	Form	Pre 1	16	2.3
		1	164	23.7
		2	167	24.2
		3	152	22.0
		4	143	20.7
		5	31	4.5
		6	18	2.6
	Area	Rural	280	40.5
		Urban	411	59.5
Teachers	**Gender**	Female	58	59.2
		Male	40	40.8
	Age	< 30 years	17	17.3
		30-40 years	57	58.2
		40-50 years	21	21.4
		50 years +	3	3.1
	Educational qualifications	Postgraduate	17	17.3
		Undergraduate	51	52
		Diploma	30	30.6
	Area	Rural	41	41.8
		Urban	57	58.2

Table 1 shows the profile of the students and teachers. Of the 11 schools sampled, 2 were girls' only; 6 boys' only and the remaining 3 mixed gender schools. Girls were the majority of the students sampled at 67.9% (469) with 32.1% (222) boys. Students from the rural based schools were 40.5% (280) compared to 59.5% (411) from urban based schools. Among the teachers in the research group 59.2% (58) were female and 40.8% (40) male. Majority of the teachers were in the 30-40 years age group with 58.2% (57) teachers. This was followed by 21.4% in the 40-50 years age group; 17.3% in the under 30 years age group and finally the least represented with 3.1% teachers in the 50 years + age group. Fifty two per cent teachers had an undergraduate degree as their highest educational qualification; followed by 30.6% with a diploma qualification and 17.3% with a postgraduate qualification.

Data was collected from the principals, teachers and students using an interviewer-administered standardized questionnaire measuring ICT indicators for each of the target populations in the secondary schools. The questionnaire used twelve indicators grouped into four domains as developed in the conceptual framework -accessibility; utilization; individuals and society; and policy and strategy. Information on the characteristics of the populations was collected. Other information collected included accessibility to ICT facilities, pattern of ICT and related facilities, level of skills in computer applications, and purposes and extent of use of the Internet.

3. FINDINGS

3.1 Accessibility

3.1.1 Internet Availability

Figure 1 shows that schools with access to the Internet for more than 40 hours in a month were 82% while another 18% reported less than 20 hours in a month of Internet access and this was attributed to non-networked computers in the school laboratories.

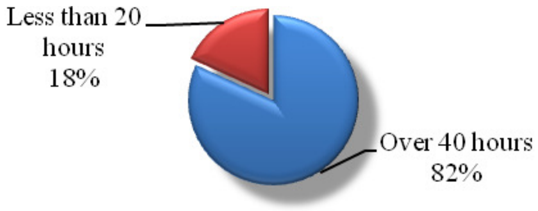


Figure 1 Hours in a month of Internet access among schools

Table 2 shows proportions of students with Internet accessibility at school. At school, 435 (63.7%) students had access to the Internet, with students from private schools having higher access rates compared to students from public schools as shown in Figure 2. However, there did not seem to be any significant difference when Internet access rates were compared between students from rural and urban based schools. However, when gender was considered, there were significant differences observed among girls from public and rural based schools who had lower access rates at 41.2% compared to boys from the same schools at 89.2%.

Table 2 Internet accessibility students at school (n=683)

Area	**Gender**	**Internet access**	**School category**		**Sub-Total**
			Private	**Public**	
Rural	**Male**	Yes	11 (73.3%)	58 (89.2%)	69 (86.3%)
		No	4 (26.7%)	7 (10.8%)	11 (13.8%)
		Sub-Total	**15 (100.0%)**	**65 (100.0%)**	**80 (100.0%)**
	Female	Yes	11 (73.3%)	75 (41.2%)	86 (43.7%)
		No	4 (26.7%)	107 (58.8%)	111(56.3%)
		Sub-Total	**15 (100.0%)**	**182 (100.0%)**	**197 (100.0%)**
Urban	**Male**	Yes	68 (100.0%)	36 (50.7%)	104 (74.8%)
		No	0 (0%)	35 (49.3%)	35 (25.2%)
		Sub-Total	**68 (100.0%)**	**71(100.0%)**	**139 (100.0%)**
	Female	Yes	57 (100.0%)	119 (56.7%)	176 (65.9%)
		No	0 (0.0%)	91 (43.3%)	91 (34.1%)
		Sub-Total	**57 (100.0%)**	**210 (100.0%)**	**267 (100.0%)**
		Total	**155 (22.7%)**	**528 (77.3%)**	**683 (100.0%0**
Internet access		**Yes**	435 (63.7%		
		No	248 (36.3%)		
Total			683 (100.0%)		
Internet access (Private schools)		**Yes**	147 (94.8%)		
		No	8 (5.2%)		
Total			155 (100.0%)		
Internet access (Public schools)		**Yes**	288 (67.3%)		
		No	240 (32.7%)		
Total			428		

(100.0%)

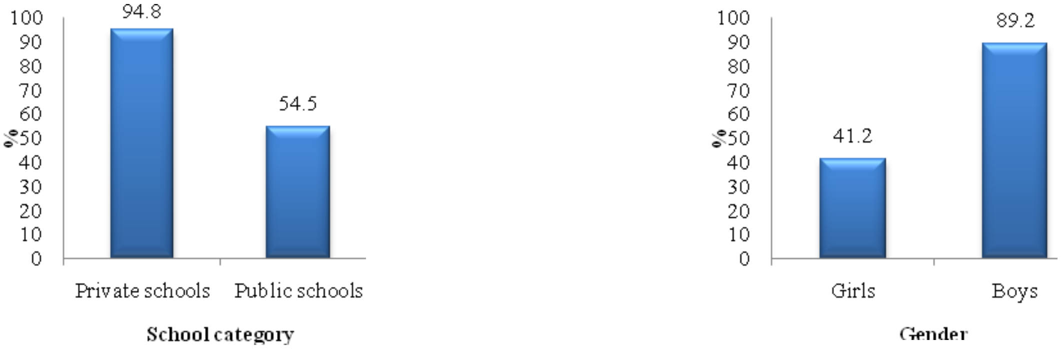


Figure 2 Students' Internet access rates

Similarly, Table 3 shows proportions of teachers with Internet access at school and home. Like the students, there did not seem to be any significant difference when Internet access rates were compared between teachers from rural and urban based schools. At schools, 96 (98%) teachers had access to the Internet while at home; only 23 (23.5%) teachers had access to the Internet access as shown in Figure 3. Teachers from urban-based schools had higher Internet access rates at home at 35.1%, compared to their counterparts from rural-based at only 8.8%.

Table 3 Internet accessibility for teachers at school and home (n=98)

	Area	**Gender**	**Internet access**	**School category**		**Sub-Total**
				Private	**Public**	
At school	**Rural**	**Male**	Yes	2 (100.0%)	11 (100.0%)	13 (100.0%)
			Sub-Total	**2 (100.0%)**	**11 (100.0%)**	**13 (100.0%)**
		Female	Yes	6 (100.0%)	21 (95.5%)	27 (96.4%)
			No	0 (0.0%)	1 (4.5%)	1 (3.6%)
			Sub-Total	**6 (100.0%)**	**22 (100.0%)**	**28 (100.0%)**
	Urban	**Male**	Yes	7 (100.0%)	19 (95.0%)	26 (96.3%)
			No	0 (0.0%)	1 (5.0%)	1 (3.7%)
			Sub-Total	**7 (100.0%)**	**20 (100.0%)**	**27 (100.0%)**
		Female	Yes	10 (100.0%)	20 (100.0%)	30 (100.0%)
			Sub-Total	**10 (100.0%)**	**20 (100.0%)**	**30 (100.0%)**
	At school		**Yes**	**96 (98.0%)**		
			No	**2 (2.0%)**		
			Total	**98 (100.0%)**		
At home	**Rural**	**Male**	Yes	0 (0.0%)	1 (10.0%)	1 (9.1%)
			No	2 (100.0%)	9 (90.00%)	11 (90.9%)
			Sub-Total	**2 (100.0%)**	**10 (100.0%)**	**12 (100.0%)**
		Female	Yes	2 (33.3%)	0 (0.0%)	2 (8.0%)

		No	4 (66.7%)	19 (100.0%)	23 (92.0%)
		Sub-Total	**6 (100.0%)**	**19 (100.0%)**	**25 (100.0%)**
Urban	**Male**	Yes	5 (71.4%)	4 (20.0%)	9 (33.3%)
		No	2 (28.6%)	16 (80.0%)	18 (66.7%)
		Sub-Total	**7 (100.0%)**	**20 (100.0%)**	**27 (100.0%)**
	Female	Yes	5 (50.0%)	6 (30.0%)	11 (36.7%)
		No	5 (50.0%)	14 (70.0%)	19 (63.3%)
		Sub-Total	**10 (100.0%)**	**20 (100.0%)**	**30 (100.0%)**
At home		**Yes**	**23 (23.5%)**		
		No	**71 (76.5%)**		
		Total	**98 (100.0%)**		
Rural schools		**Yes**	**3 (8.8%)**		
		No	**34 (91.2%)**		
		Total	**37 (100.0%)**		
Urban schools		**Yes**	**20 (35.1%)**		
		No	**37 (64.9%)**		
		Total	**57 (100.0%)**		

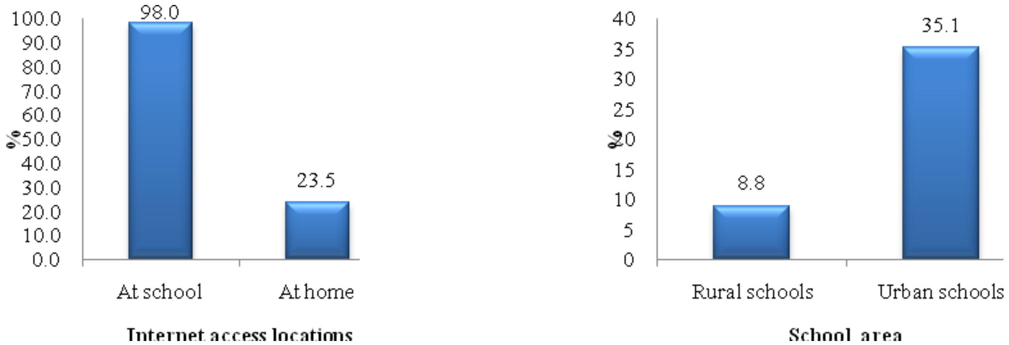


Figure 3 Teacher's Internet access rates

3.1.2 Internet Affordability and Financing

As can be seen from Table 4 all private schools and some public schools spent less than 5% of their annual expenditure on maintaining Internet connectivity, and schools which spent up to 20% of the school expenditure for the purpose were publicly funded. These schools were low cost and cited tuition fee as their main source of financing Internet connectivity.

Table 4 Proportion of costs on Internet connectivity on schools' annual total expenditure

Area	**Proportion of Internet costs / Annual total expenditure**	**Category**		**Sub-Total**
		Private	**Public**	
Rural	Less than 5%	1 (100.0%)	1 (25.0%)	2 (40.0%)
	5-10%	0 (0.0%)	1 (25.0%)	1 (20.0%)
	11-15%	0 (0.0%)	1 (25.0%)	1 (20.0%)
	16-20%	0 (0.0%)	1 (25.0%)	1 (20.0%)
	Sub-Total	**1 (100.0%)**	**4 (100.0%)**	**5 (100.0%)**
Urban	Less than 5%	2 (100.0%)	1 (25.0%)	3 (50.0%)
	5-10%	0 (0.0%)	1 (25.0%)	1 (16.7%)
	11-15%	0 (0.0%)	2 (50.0%)	2 (33.3%)
	Sub-Total	**2 (100.0%)**	**4 (100.0%)**	**6 (100.0%)**

The study also showed that all the schools relied on tuition fees paid by students to maintain Internet connectivity, and for some public schools this was a challenge as reflected in their spending proportions of the annual school expenditure due to the ceiling set on what they could collect from the students. As Table 5 illustrates, the schools were classified as low, medium or high cost based on the tuition fee collected.

Table 5 Classification of schools based on annual school fees charged

Classification of schools	**Annual school fees range**
Low cost	Less than Ksh. 50,000 (< USD 625)
Medium cost	Ksh. 50,000-150,000 (USD 625-1,875)
High cost	More than Ksh. 150,000 (USD 1,875 +)

However, private schools were able to install, equip and maintain better ICT facilities as compared to public schools due to the high fees they charged (which ranged from Ksh. 120,000-1,150,000 or US $ 1,500-14,375). Most of the public schools were reliant on donor support through non-governmental support initiatives such as Computers for Schools-Kenya (CfS-K) and NEPAD, with little or lack of financial support from the government to support the ICT initiatives in these schools.

3.2 Usage

3.2.1 Access to ICTs

All the schools' ICT facilities were available and accessible to both teachers and students. It was observed that private schools surveyed had purchased lap top computers for their teachers. Students to computer ratios were 5:1 in private schools and 20:1 in public schools, with average number of computers available for student use in both rural and urban based private schools being 60, and in both rural and urban based public schools being 40. These findings suggested that accessibility to ICT facilities at schools that are connected were much higher than those schools which are not connected to Internet [Ministry of Education, Science & Technology, 2005].

The findings of the study also suggested that there was a positive correlation between accessibilities proportions of teachers and students with access to computers as shown in Table 6 (a); and a negative correlation among schools based on their rural and urban settings, and access to the Internet as shown in Table 6 (b), and below.

Table 6(a) Pearson correlation coefficient between students' and teachers' access to computers among schools

		Proportion of student with access to computers	**Proportion of teachers with access to computers**
Proportion of students with access to computers	Pearson Correlation	1	0.623(*)
	Sig. (2-tailed)	0.000	0.040
	N	11	11
Proportion of teachers with access to computers	Pearson Correlation	0.623(*)	1
	Sig. (2-tailed)	0.040	0.000
	N	11	11

* Correlation is significant at the 0.05 level (2-tailed)

Table 6(b) Pearson correlation coefficient between schools' area setting and students' access to Internet

		Area setting	**Access to Internet**
Area setting	Pearson Correlation	1	-0.133(**)
	Sig. (2-tailed)	.	0.001
	N	691	683
Access to Internet	Pearson Correlation	-0.133(**)	1
	Sig. (2-tailed)	0.001	.
	N	683	683

** Correlation is significant at the 0.01 level (2-tailed)

As found in previous studies [Makau & IDRC, 1990] accessibility to ICT facilities by students is still predominantly in the school laboratories, though this study has shown that private schools are installing ICT facilities in school libraries, teachers' lounges, dormitories and even in the school health centres. Overall, more than 75% of the students had access to ICT facilities and this is a departure from the previous studies that indicated low rates of accessibility [Kenya SchoolNet, 2003].

3.2.2 Enhancing Education with ICTs

Responses from the school principals showed high levels of ICT integration in subjects taught at the schools. Using a weighted usage index, the study suggested that ICT and its related components have been integrated into subjects such as ICT, Sciences, English, Mathematics and Music for teaching and learning as shown in Table 7. The most popular subject taught using ICTs are the ICT related subjects in both rural and urban based schools. Teachers from urban based schools appeared to place more emphasis on the humanities as compared to teachers from rural based schools with more emphasis on the sciences.

Table 7 Ranking of teachers' ICT usage index in subjects among schools

Area	**Classes or subjects**	**Usage Index**	**Variance**
Rural	ICT subjects	4.00	0.00

	Sciences	2.40	0.80
	English	2.20	1.20
	Mathematics	2.00	0.00
	Social sciences	1.80	2.20
	Art	1.20	1.20
	Music	1.00	1.50
Urban	ICT subjects	3.83	0.167
	Music	2.83	2.17
	Art	2.50	0.70
	Sciences	2.00	0.40
	English	2.00	1.20
	Mathematics	2.00	0.40
	Social sciences	1.67	1.07

The same observation was made as regards the purposes of Internet usage among teachers, with 75-87.5% of teachers from both rural and urban based schools indicating that Internet was most used for finding and accessing information as shown in Table 8. Unlike their counterparts from the rural schools, 79.3% of teachers from urban schools used Internet for communication as compared to only 60% of teachers from rural schools. Internet use for teaching and learning for specific subjects was the least cited use among teachers from rural schools. The findings thus demonstrate that among teachers surveyed there were differences on use of ICT in specific subjects, and on use of Internet based on whether the school was rural or urban based.

Table 8 Ranking of teachers' purposive index in descending order

Area	Purpose of Internet usage	Purposive Index	Variance
Rural	Finding/accessing information	3.00	0.50
	Learning enrichment or learning new things	2.80	1.20
	Communicating with others	2.40	0.80
	Regular instruction and training for developing computer skills	2.40	1.30
	As teaching/learning tool for specific subjects	2.20	1.70
Urban	Finding/accessing information	3.50	0.30
	Communicating with others	3.17	0.97
	As teaching/learning tool for specific subjects	2.67	1.07
	Learning enrichment or learning new things	2.60	1.80
	Regular instruction and training for developing computer skills	2.50	1.10

3.2.3 Developing the ICT Workforce

Table 9 shows that 44% of the teachers had more than 6 years of using computer, with 11% stating they had less than 1 year using computers. However, there was gender disparity especially among female teachers with more than 4 years of computer usage who were 52% as compared to male teachers who were 70% of their populations. The study also found that 55% of the teachers did not receive any ICT training prior to joining the teaching profession, but nevertheless noted that half of them had had training in the past 3 years. This is supported by the view from the school principals that over 75% of their teachers could be regarded as having basic ICT literacy skills.

Table 9 Years of computer usage among teachers

Area	Gender	Years using computers	Area		Sub-Total
			Private	Public	
Rural	**Male**	< 1 yr	0 (0.0%)	1 (9.1%)	1 (7.7%)
		1-2 yrs	1 (50.0%)	1 (9.1%)	2 (15.4%)
		2-4 yrs	0 (0.0%)	1 (9.1%)	1 (7.7%)
		4-6 yrs	0 (0.0%)	5 (45.5%)	5 (38.5%)
		6 yrs +	1 (50.0%)	3 (27.3%)	4 (30.8%)
		Sub-Total	**2 (100.0%)**	**11 (100.0%)**	**13 (100.0%)**
	Female	< 1 yr	0 (0.0%)	4 (18.2%)	4 (14.3%)
		1-2 yrs	0 (0.0%)	7 (31.8%)	7 (25.0%)
		2-4 yrs	0 (0.0%)	5 (22.7%)	5 (17.9%)
		4-6 yrs	2 (33.3%)	2 (9.1%)	4 (14.3%)
		6 yrs +	4 (66.7%)	4 (18.2%)	8 (28.6%)
		Sub-Total	**6 (100.0%)**	**22 (100.0%)**	**28 (100.0%)**
Urban	**Male**	< 1 yr	0 (0.0%)	3 (15.0%)	3 (11.1%)
		1-2 yrs	0 (0.0%)	2 (10.0%)	2 (7.4%)
		2-4 yrs	0 (0. 0%)	3 (15.0%)	3 (11.1%)
		4-6 yrs	2 (28.6%)	1 (5.0%)	3 (11.1%)
		6 yrs +	5 (71.4%)	11 (55.0%)	16 (59.3%)
		Sub-Total	**7 (100.0%)**	**20 (100.0%)**	**27 (100.0%)**
	Female	< 1 yr	0 (0.0%)	3 (15.0%)	3 (10.0%)
		1-2 yrs	0 (0.0%)	2 (10.0%)	2 (6.7%)
		2-4 yrs	2 (20.0%)	5 (25.0%)	7 (23.3%)
		4-6 yrs	1 (10.0%)	2 (10.0%)	3 (10.0%)
		6 yrs +	7 (70.0%)	8 (40.0%)	15 (50.0%)
		Sub-Total	**10 (100.0%)**	**20 (100.0%)**	**30 100.0%)**

3.3 Individuals and Society

3.3.1 People and Organizations Online

Almost all the teachers (about 92%) in these connected schools had functional email addresses, with 64% of the students also indicating use of a functional email address as shown in Table 10. Interestingly 7.5% of the students said they had a personal webpage or blog, and references were made to social networking sites such as Facebook®. A high proportion of students (73%) said they owned a mobile phone, with 52% of these students using the mobile phones for accessing Internet and sending and receiving emails.

Table 10 Student's ownership-mobile phones, email addresses and personal websites

Area	Do you:	Do you own a mobile phone?		Do you have an email address?		Do you have a personal webpage	
		Frequency	Percent	Frequency	Percent	Frequency	Percent
Rural	**Yes**	203	72.4%	158	56.4%	24	8.6%

	No	77	27.6%	122	43.6%	256	91.4%
Urban	**Yes**	297	72.3%	286	69.6%	28	6.8%
	No	114	27.7%	125	30.4%	383	93.2%

3.3.2 Locally Relevant Content

The findings of the study suggest that there were low proportions of teachers (18.4%) with access to local web-based training programmes, and 24.5% of teachers with access to local web portals. This is attributed to the lack of locally relevant material online especially for ICT related courses and which is also reflected in the approved school curricula for ICT courses.

3.4 Policy, Strategy and Financing

3.4.1 ICT Strategy

About 64% of the schools had an ICT code of conduct to regulate use of computers and Internet among their users. But it was observed that not all the schools had adopted the national ICT strategy implemented by the Ministry of Education in 2002 so as to guide the process of ICT integration into education.

4. DISCUSSION AND CONCLUSION

The objective of the study was to help policy makers, decision makers and investors to make well informed decisions about public policy and investments in ICT as regards education at the secondary school level by understanding how the Internet and its related components (and by extension ICT in general) are utilized. The study has shown the extent to which the Internet is being utilized and has identified the factors that enhances or impedes its utilization at secondary schools, and which can be used to explain the integration of Internet into the teaching and learning.

The findings of the study has shown that use of Internet and its integration in the teaching and learning in secondary education is getting more widespread; and its use more pervasive students and teachers as a means of communication and for information searching being common. Access rates for teachers and students have been observed to be much higher in educational institutions that have made effective ICT investments in education, translating into better utilization of ICT related technologies with assumed positive impacts which another study can attempt to measure by better understanding the linkages between utilization of the Internet and its impacts in education.

The study also found that most of the schools are actually expending a substantial part of their annual budget on maintaining Internet connectivity, and this explains why it is estimated by the Ministry of Education that only 3% of the 6,566 secondary schools in Kenya have any form of Internet connectivity. But this could change with the enhancement of the competition regulatory framework as well as operationalization of the National Fibre Optic cable through the East African Submarine System (EASSY) project expected to boost Internet penetration and bring the cost of Internet connectivity down in the third quarter of 2009, with subsidized costs of USD 10 per megabyte being envisaged for educational, health and research institutions.

It was also found that there was a positive correlation between proportions of students and teachers accessing the schools' computers, and this was evident in girls only schools where it appeared that investments in ICT was low and resulting in gender disparity disadvantaging the girl child. This does not portend good news for the girls in the secondary schools, considering that there are 635,698 girls enrolled, constituting 46% of the country's 1,382,211 total student enrolment in secondary schools [Kenya National Bureau of Statistics , 2009]. Though the study focussed on schools with Internet connectivity, the proportion of teachers with access to computers and internet at schools and homes was respectively 98% and 53% of the teachers sampled, implying that the affordable bundle rates and increased access to the mobile wireless broadband services is having an impact. According to the Communications Commission of Kenya (CCK) there were 392,964 mobile broadband users as at 31 December 2008 [Communications Commission of Kenya, 2009]. Some of the schools sampled are addressing the issue of accessibility to computers by teachers and students through use of Wi-Fi in the school localities. This is also reflected at the proportion of teachers and students with email addresses which are at 92% and 64% respectively, with

72% of the students owning mobile phones. Related to this findings, it has always been assumed that the most common place for students to access the computers has been the computer laboratories, though it appears that some schools, especially privately sponsored schools are focussing on the libraries with the intention of extending traditional libraries services to support digital resources.

The study also found that majority of the teachers did not receive ICT training at the teachers' training colleges or universities where they trained, with 55% getting into the teaching profession with no experience of computers and its related technologies. But it is reassuring to note that 51% of the teachers indicated that they have undergone ICT training in the past 3 years, with some schools supporting the training programmes.

The study also investigated use of ICT and the Internet in schools, and like the study conducted in Malaysia on extent of ICT adoption among secondary school teachers [Lau & Sim, 2008] the findings suggest most of the teachers are positive with uses of the Internet, and appreciate the use of ICT in enhancing teaching and learning. The findings also showed that there is integration of ICT in classroom teaching.

The levels of ICT literacy skills were found to high in both students and teachers than was expected in the schools with Internet connectivity. The index levels that were computed for the expertise levels in the most commonly used software applications also supported this finding, and the same was noted for the purpose of Internet in the school work among students with weighted ratings of above 75%.

Thus it can be concluded that use of ICT and its related technologies is still at its early stages of its development and implementation. There is also use of inadequate and divergent curricula in secondary schools depending on the system of education and which was not responsive to the fast changing ICT landscape, for instance, like examining students in open source software like Ubuntu®. Though it is worth noting that in some instances there is evidence of development of e-content with the relevant local material content by the Kenya Institute of Education (KIE) in use for the Form 1s and 2s students.

5. REFERENCES

BUTUNYI, C., 2008. *News.* [Online] Available at: http://www.nation.co.ke/News/regional/-/1070/498064/-/6lotcv/-/index

COMMUNICATIONS COMMISSION OF KENYA, 2009. *Communications statistics report-Second Quarter 2008/2009*. Nairobi: CCK.

DALY, J.A., 2002. *Centre for International Development & Conflict Management*. [Online] Available at: http://www.cidcm.umd.edu/library/papers/jdaly/concept.htm

FARREL, G., 2007. *Survey of ICT in Education in Kenya*. Washington D.C.: infoDev/World Bank.

FISHER, A.A., LAING, J.E., STOECKEL, J.E. & TOWNSEND, J.W., 1999. *Handbook for Family Planning Operations Research Design (2nd Edition)*. New York: Population Council.

INTERNET WORLD STATS-USAGE AND POPULATION STATISTICS, 2009. *Internet Usage Statistics for Africa (Africa Internet Usage and Population Stats)*. [Online] Available at: http://www.internetworldstats.com/africa.htm

JENSEN, M., 2002. *African Internet-Status Report*.

KASHORDA, M., WAEMA, T., OMOSA, M. & KYALO, V., 2007. *E-Readiness Survey of Higher Education in Kenya*. Nairobi: Kenya Education Network (KENET).

KENYA NATIONAL BUREAU OF STATISTICS, 2009. *Economic Survey 2009*. Nairobi: The Government Printer.

KENYA SCHOOLNET, 2003. *Preparing a Workforce for the Evolving Information Economy: A Survey on ICT Access and Use in Kenya Secondary Schools*. Nairobi: Summit Strategies Limited.

LAU, B.T. & SIM, C.H., 2008. *Exploring the extent of ICT adoption among Secondary School Teachers in Malaysia*. International Journal of Computing and ICT Research, II(II), pp.19-36.

MAKAU, B.M. & IDRC, 1990. *Computers in Kenya's secondary schools : case study of an innovation in education*. Ontario: IDRC.

MINISTRY OF EDUCATION, KENYA, 2006. *National Information and Communication Technology (ICT) Strategy for Education and Training*. Nairobi: The Government Press.

MINISTRY OF EDUCATION, SCIENCE & TECHNOLOGY, 2005. *ICTs in Educations Options Paper*. Nairobi: MOEST.

NATIONAL RESEARCH COUNCIL, 1998. *Measuring the Impacts of Internet*. Washington, D.C.: National Academy Press.

NGAHU, C. & NDUATI, C., 2007. *Kenya ICT Policy*. [Online] Available at: www.epolafrica.org/ictkigali2007/resources/Kenya_ICT_policy_implementation-Ngahu_Nduati-en.ppt

NYABIAGE, J., 2009. *Smart Company*. [Online] Available at: http://www.nation.co.ke/magazines/smartcompany/-/1226/510682/-/stbxnqz/-/index.html

SHAKIFA, I., IRENE, B. & THOMAS, M., 2002. *Contextualising Education in Africa: The Role of ICTs*. [Online] Available at: http://www.idrc.ca/en/ev-71268-201-1-DO_TOPIC.html

UNCTAD, 2007. *Manual for the Production of Statistics on Information Technology*. Geneva: UNCTAD.

WIMS, P. & LAWLER, M., 2007. *Investing in ICTs in educational institutions in developing countries: An evaluation of their impact in Kenya*. [Online] Available at: http://ijedict.dec.uwi.edu/printarticle.php?id=241amp;layout=html&layout=html

WORLD SUMMIT ON INFORMATION SOCIETY, 2005. *Tunis: Agenda for the Information Society*. Geneva: WSIS.